

VYPOŘÁDÁNÍ PŘIPOMÍNEK K MATERIÁLU S NÁZVEM:

Návrh zákona o kybernetické bezpečnosti

Podle Jednacího řádu vlády byl materiál rozeslán do meziresortního připomínkového řízení dopisem ředitele Národního úřadu pro kybernetickou a informační bezpečnost dne 19. 6. 2023, s termínem dodání stanovisek do 26. 7. 2023. Vyhodnocení tohoto řízení je uvedeno v následující tabulce:

Resort		Připomínky	Vypořádání
1. Ministerstvo spravedlnosti	D	K § 15 odst. 2 Není zřejmé, z jakého důvodu nejsou bezpečnostní opatření pro poskytovatele regulované služby v režimu nižších povinností členěna na organizační a technická opatření ve smyslu § 14 odst. 1 návrhu zákona. Bezpečnostní opatření pro poskytovatele regulované služby v režimu vyšších povinností takto členěna jsou (viz návrh § 15 odst. 1). Doporučujeme v uvedeném smyslu návrh dopracovat.	Vysvětleno Účelem této rozdílnosti oproti vyhlášce v režimu vyšších povinností je udělat režim nižších povinností přehledný a přiměřeně náročný s ohledem na předpokládanou maturitu subjektů. Výčet bezpečnostních opatření včetně jejich obsahu, který je uvedený v prováděcích právních předpisech, nám dává smysl aktuálně na úrovni zákona rozdělovat pouze u režimu vyšších povinností. V režimu nižších povinností s ohledem na zobecnění povinností včetně jejich vzájemných prolnutí nám obdobné rozdělení, jako je nyní v režimu vyšších povinností, nepříjde opodstatněné. Navíc některé ustanovení prováděcích právních předpisů organizační a technické požadavky kombinují. Provedli jsme však korekci u § 15 odst. 2, aby bylo jasné že výčet bezp. opatření pro režim nižších povinností obsahuje povinnosti organizačního i technického charakteru. Připomínkové místo s vypořádáním souhlasí.
2. Ministerstvo spravedlnosti	D	K § 16 odst. 4 Upozorňujeme, že formulace povinnosti v uvedeném ustanovení není zcela přesná. Podle návrhu musí poskytovatel regulované služby začít	Akceptováno jinak Z § 16 odst. 1 a 2 vyplývá, že poskytovatelům regulované služby v jednotlivých režimech povinností

		plnit povinnost hlásit kybernetické bezpečnostní incidenty pro každou regulovanou službu nejpozději do 1 roku ode dne doručení písemného vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb. Splnění dané povinnosti však předpokládá vznik kybernetického bezpečnostního incidentu, k němuž však nemusí do jednoho roku nutně dojít. Doporučujeme proto přeformulovat dané ustanovení tak, aby z něj bylo patrné, že uplynutím dané doby vzniká poskytovateli regulované služby povinnost hlásit kybernetické bezpečnostní incidenty, a nikoliv, že je tuto povinnost v dané době povinen splnit.	vzniká povinnost v rámci stanoveného rozsahu hlásit kybernetické bezpečnostní incidenty již v okamžiku, kdy se stávají poskytovateli regulované služby. § 16 odst. 4 pouze určuje nejzazší okamžik, od něhož má poskytovatel regulované služby přistoupit k faktickému plnění této povinnosti. V případě, že ke kybernetickému bezpečnostnímu incidentu nedojde, poskytovatel regulované služby není povinen jej hlásit, platí tedy zásada, že kde není incident, není ani povinnost. Za účelem posílení právní jistoty povinných osob podle návrhu zákona jsme uvedenou odpověď na Vaši připomínku doplnili do důvodové zprávy. Připomínkové místo s vypořádáním souhlasí.
3. Ministerstvo spravedlnosti	Z	K § 29 odst. 4 Návrh předmětného ustanovení stanovuje, že poskytnutí informací podle § 29 není porušením mlčenlivosti podle jiného právního předpisu, přičemž však výslovně uvádí, že tímto ustanovením není dotčena povinnost mlčenlivosti advokáta podle právního předpisu upravujícího výkon advokacie. Požadujeme větu druhou uvedeného ustanovení doplnit tak, aby ustanovením § 29 nebyla dotčena ani povinnost mlčenlivosti soudců, notářů, exekutorů, soudních znalců, překladatelů a tlumočnicků. <u>Tato připomínka je zásadní</u>	Akceptováno jinak - nyní § 30 odst. 5 a 6 Dotčené ustanovení bylo na základě jiných připomínek přepracováno. Obdobně jako u sankčního zákona je prolomení mlčenlivosti v současné době koncipováno tak, že v jeho odst. 5 jsou vyjmenovány orgány, ve vztahu k nimž se mlčenlivost výslovně prolamuje (orgány činné v trestním řízení, Finanční analytický úřad, správce daně, orgány Celní správy České republiky). V případě potřeby získání jiných informací krytých povinností mlčenlivosti bude přistoupeno k podání žádosti o zproštění povinnosti mlčenlivosti. Dále byl doplněn odst. 6, který od prolomení povinnosti mlčenlivosti odlišuje prolomení bankovního tajemství. Výše uvedené změny byly zrcadlově promítnuty do doprovodného zákona v podobě změn zákonů upravujících činnost orgánů označených v odstavcích 5 a 6. Reakce připomínkového místa:

		Vítáme přepracování konstrukce předmětného ustanovení po vzoru sankčního zákona, kdy nový návrh výslovně uvádí orgány, ve vztahu k nimž se mlčenlivost výslovně prolamuje. Co se týče mlčenlivosti soudců a tzv. „justičních profesí“ (advokáti, notáři, atd.) tak máme připomínku za vypořádanou. Ve vztahu k návrhu nového § 30 odst. 5 písm. a) však upozorňujeme, že ačkoliv návrh vychází z obdobné úpravy v sankčním zákoně, na rozdíl od ní zachovává v případě orgánů činných v trestní řízení mlčenlivost pouze v případech, kdy by její prolomení „zmařilo účel trestního řízení“, nikoliv však v případech, kdy by došlo k „ohrožení trestního řízení“ [srov. § 14 odst. 3 písm. a) sankčního zákona]. Požadujeme proto vyjasnit, z jakého důvodu je ustanovení § 30 odst. 5 písm. a) omezeno pouze na případy, v nichž by poskytnutí informace mohlo zmařit trestní řízení, a proč naopak chybí omezení pro případy ohrožení trestního řízení (tak, jak je tomu například i u sankčního zákona, na který je ve vypořádání poukazováno). V důvodové zprávě k tomu není žádné odůvodnění. Pokud by pro uvedený rozdíl nebyl dán žádný věcný důvod, požadujeme, aby do ustanovení § 30 odst. 5 písm. a) byla za slovo „vztahuje,“ doplněna slova „ohrozilo nebo“, neboť tak bude dostatečně garantována ochrana informací z trestního řízení. Současně upozorňujeme, že Nejvyšší státní zastupitelství není typicky orgánem činným v trestním řízení a nebude poskytovat pouze informace z trestního řízení v postavení orgánu činného v trestním řízení, ale i jiné zájmové informace, kterými disponuje v rámci své činnosti. Ve vztahu k těmto jiným informacím není v odstavci 5 prolomení mlčenlivosti nijak upraveno. Odstavec 5 je proto třeba formulovat

		tak, aby odpovídal vymezení povinných subjektů v odstavci 2. Reakce NÚKIB: Vámi označený rozpor ve formulacích dotčených ustanovení sankčního zákona a návrhu zákona o kybernetické bezpečnosti vyplývá ze skutečnosti, že návrh zákona byl při zapracování zaslaných připomínek přeformulován také s ohledem na pojetí a formulace vlastní zákonu č. 141/1961 Sb., trestnímu řádu, coby základnímu právnímu předpisu pro vedení trestního řízení. Trestní řád v souvislosti s trestním řízením pracuje výhradně (v § 51 odst. 2, § 88 odst. 9, § 88a odst. 3) s formulací "zmaření účelu trestního řízení", ohrožení účelu trestního řízení v něm zmíněno není. Trestní řád obsahuje formulaci "podstatné ztížení dosažení účelu" (např. v § 71 odst. 1), ovšem pouze v souvislosti s trestním stíháním, tedy pojmem, který je proti trestnímu řízení významově užší. Uvedené vysvětlení s odkazem na trestní řád bylo doplněno rovněž do výkladu týkajícího se § 30 odst. 5 návrhu zákona v důvodové zprávě. Reakce připomínkového místa: Skutečnost, že návrh § 30 odst. 5 a 6 na rozdíl od některých jiných zákonů nezachovává mlčenlivost orgánů činných v trestním řízení v případech, kdy by poskytnutí informací mohlo ohrozit účel trestního řízení, lze s ohledem na odůvodnění NÚKIB z naší strany akceptovat. Považuje však za nutné, aby byla ve smyslu Vámi předestřené argumentace doplněna zvláštní část důvodové zprávy, aby bylo zřejmé, proč je konstrukce odlišná od úpravy v jiných předpisech. Pokud dojde k doplnění důvodové zprávy, pak

			můžeme vypořádání, resp. vysvětlení, v dané části akceptovat. Z Vašeho vyjádření však neplyne, zda bude nějak zvlášť upravena mlčenlivost Nejvyššího státního zastupitelství, jež nelze považovat za „klasický“ orgán činný v trestním řízení. Otázkou je, zda by se tak dané ustanovení mohlo, resp. mělo na NSZ aplikovat. Považujeme za vhodné uvedené vyjasnit (ať již v odůvodnění, nebo v textu návrhu). Reakce NÚKIB: Navrhujeme k části druhé této připomínky do DZ ještě doplnit následující text: <i>„Pro účely aplikace tohoto ustanovení vzhledem k jeho povaze a důvodům pro které je toto ustanovení součástí zákona o kybernetické bezpečnosti, považujeme i Nejvyšší státní zastupitelství za OČTR.“</i>. Připomínkové místo s vypořádáním souhlasí.
4. Ministerstvo spravedlnosti	D	K § 40 odst. 1 písm. d) Doporučujeme uvedené ustanovení zpřesnit tak, aby bylo patrné, komu může ředitel NÚKIB v době stavu kybernetického nebezpečí nařídít práci v pohotovostním režimu.	Akceptováno - nyní § 41 odst. 1 písm. e) Ustanovení týkající se stavu kybernetického nebezpečí byla upravena komplexně. Dotčené ustanovení bylo rovněž v návrhu upraveno a zpřesněno. Připomínkové místo s vypořádáním souhlasí.
5. Ministerstvo spravedlnosti	D	K § 41 odst. 3 písm. w) a hlavě VI Podle návrhu § 41 odst. 3 písm. w) NÚKIB „<i>ukládá správní sankce za nedodržení povinností stanovených tímto zákonem a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti</i>“. Název hlavy VI pak je „<i>Kontrola, nápravná opatření, přestupky a sankce</i>“. V této souvislosti upozorňujeme, že z návrhu není zcela zřejmé, co se rozumí „<i>správními sankcemi</i>“, resp. „<i>sankcemi</i>“ podle návrhu	Akceptováno - nyní § 44 odst. 3 písm. v) a hlava VI Sankcemi podle hlavy VI jsou skutečně myšlena pozastavení platnosti certifikace podle § 60 a pozastavení výkonu řídicí funkce podle § 61. Ustanovení § 41 odst. 3 písm. w) bude upraveno následujícím způsobem: „<i>ukládá správní tresty a další sankce za nedodržení ...</i>“. Správní tresty je termín z

		zákona. Pakliže by mělo být za tyto správní sankce považováno pozastavení platnosti certifikace podle návrhu § 60 nebo pozastavení výkonu řídicí funkce podle návrhu § 61, pak upozorňujeme na nutnost vyhodnotit, zda nemůže dojít ke kolizi s některou s návrhem zákona stanovených skutkových podstat přestupků ve smyslu zákazu dvojího trestání.	přestupkového zákona, dalšími sankcemi jsou myšleny právě sankce podle § 60 a § 61. Co se týče kolize ukládání sankcí podle § 60 a § 61 s ukládáním pokut za přestupky, jsme toho názoru, že ke kolizi (a tedy dvojímu trestání) nedochází. Instituty podle § 60 a § 61 mají jeden konkrétní specifický účel, a to je vymození splnění povinnosti uložené nápravným opatřením Úřadu. To plyne jednak z formulace odstavce 1 obou ustanovení (tedy že dočasné pozastavení se ukládá až do doby odstranění zjištěných nedostatků), jednak z odstavce 5, podle kterého Úřad po ověření, že příslušné povinnosti byly splněny, vydá osvědčení, které je podkladem pro ukončení pozastavení. Tzn. jde jen o dočasné řešení, jehož cílem je přinutit subjekt, aby plnil své povinnosti. Jakmile jsou povinnosti splněny, toto dočasné řešení pozbývá smyslu a následně i formální platnosti. Jde tak spíše o obdobu donucovací pokuty podle správního řádu, s tím rozdílem, že na rozdíl od donucovací pokuty jsou tyto sankce „vratné“ (tzn. certifikát je po splnění povinnosti obnoven, funkce je po splnění povinnosti vrácena). Jde tedy o odlišný institut než v případě správních trestů podle přestupkového zákona, kdy uložení pokuty za přestupek, případně uložení jiného trestu, je jednorázový, nevratný proces, primárně sloužící k potrestání pachatele, nikoli k vymození splnění uložené povinnosti. Nadto v případě § 61 jde pouze o návrh Úřadu na vydání soudního rozhodnutí, nikoli o uložení povinnosti samotné. V případě postupu podle § 61 je vedeno civilní soudní řízení s fyzickou osobou, tedy osobou odlišnou od té, které je ukládána pokuta za přestupek. Nedochází tedy ani k souběhu druhu

			řízení, příslušného orgánu, sankcionovaného subjektu a sankcionované povinnosti (povinná osoba dostává pokutu např. za nesplnění povinnosti zavést bezpečnostní opatření nebo za nesplnění povinnosti uložené reaktivním opatřením, fyzická osoba je zde sankcionována za neplnění povinnosti řádného výkonu své řídicí funkce a bránění splnění povinností právnickou osobou). Pro posílení právní jistoty adresátů normy bude do § 60 doplněn odst., který stanoví, že aplikací postupu podle § 60 není dotčeno ukládání pokut za přestupky podle § 58 návrhu zákona. V tomto smyslu bude doplněna i důvodová zpráva k zákonu. Připomínkové místo s vypořádáním souhlasí.
6. Ministerstvo spravedlnosti	Z	K § 42 odst. 1 písm. f) Podle uvedeného ustanovení může být provozovatelem Národního CERT pouze právnická osoba, která nebyla pravomocně odsouzena za spáchání trestného činu uvedeného v § 7 zákona o trestní odpovědnosti právnických osob a řízení proti nim (dále jen „zák. o trestní odpovědnosti práv. osob“). Jde o text převzatý ze současného znění § 18 odst. 2 písm. f) zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Stávající § 18 odst. 2 písm. f) však nezohledňuje novelizaci zák. o trestní odpovědnosti práv. osob, kterou došlo ke změně přístupu k vymezení okruhu trestných činů, které jsou přiřítelné právnické osobě. Zatímco původní znění zák. o trestní odpovědnosti práv. osob pracovalo v § 7 s pozitivním výčtem, po 1. 12. 2016 obsahuje § 7 negativní výčet. V § 7 zák. o trestní odpovědnosti práv. osob jsou tak po novele provedené zákonem č. 183/2016 Sb. vyjmenovány trestné činy, kterých se právnická osoba dopustit nemůže („<i>Trestnými činy se pro účely tohoto zákona rozumí zločiny nebo přečiny uvedené v trestním zákoníku, s výjimkou trestných činů...</i>“). Odkaz na § 7 zák.	Akceptováno - nyní § 45 odst. 4 písm. f) Ustanovení bylo změněno požadovaným způsobem: „Provozovatelem Národního CERT může být pouze právnická osoba, která nebyla pravomocně odsouzena za spáchání trestného činu, nebo na kterou se hledí, jako by nebyla odsouzena.“ V návaznosti na zaslanou připomínku a pro potřebu uvést v soulad požadavky na bezúhonnost provozovatele Národního CERT a žadatele o registraci členství v Komunitě kompetencí pro kybernetickou bezpečnost došlo rovněž ke změně formulace § 51 odst. 1 písm. c): „Žadatel má základní způsobilost, pokud nebyl v posledních 5 letech před podáním žádosti pravomocně odsouzen pro trestný čin, jehož skutková podstata souvisí s předmětem podnikání žadatele, nebo pro trestný čin hospodářský, trestný čin proti majetku, trestný čin obecně nebezpečný, trestný

		o trestní odpovědnosti práv. osob je tak v kontextu uvedeného ustanovení matoucí a zcela nadbytečný. Právnická osoba může být odsouzená pouze za trestné činy neuvedené v ustanovení § 7. Požadujeme proto vypuštění odkazu na § 7 zák. o trestní odpovědnosti práv. osob a přeformulování textu písm. f) na: <i>„f) která nebyla pravomocně odsouzena za spáchání trestného činu“.</i> Dále upozorňujeme, že z návrhu není zřejmé, zda se má či nemá při posuzování splnění dané podmínky přihlížet rovněž k zahlazeným odsouzením. Výkladu, podle něhož se k zahlazeným odsouzením nepřihlíží, by nasvědčovala skutečnost, že se předpokládá prokazování výpisem z Rejstříku trestů, jelikož návrh výslovně nezakládá oprávnění vyžádat si opis z Rejstříku trestů. Naopak textace návrhu § 48 odst. 1 písm. c) nasvědčuje opaku. Požadujeme proto dále do návrhu doplnit text, z něhož bude patrné, že relevantní pro posouzení splnění podmínky bezúhonnosti jsou pouze odsouzení, pokud se na odsouzenou právnickou osobu nehledí, jako by nebyla odsouzena. <u>Tato připomínka je zásadní</u>	čin proti České republice, cizímu státu a mezinárodní organizaci, trestný čin proti pořádku ve věcech veřejných, nebo pokud se na žadatele ve vztahu k těmto pravomocným odsouzením hledí, jako by nebyl odsouzen.“. Reakce připomínkového místa: Dáváme ke zvážení, zda by nebylo vhodné ustanovení přeformulovat následovně: „Provozovatelem Národního CERT může být pouze právnická osoba, která nebyla pravomocně odsouzena za spáchání trestného činu, pokud se na ní nehledí, jako by nebyla odsouzena.“. Reakce NÚKIB: Změna akceptována a připomínka je vypořádána.
7. Ministerstvo spravedlnosti	D	K § 42 odst. 1 písm. g) Upozorňujeme, že není zřejmé, co se rozumí „<i>zahraniční osobou podle jiného předpisu</i>“, když není zřejmé, o jaký jiný předpis se má jednat. Doporučujeme proto slova „<i>podle jiného právního předpisu</i>“ z návrhu vypustit s tím, že lze v daném případě použít obecné pravidlo stanovené v § 26 odst. 1 zákona č. 91/2012 Sb., o mezinárodním právu soukromém.	Akceptováno jinak - nyní § 45 odst. 4 písm. g) Na základě připomínky došlo ke změně textu příslušného ustanovení na „nemá sídlo mimo území České republiky“. Připomínkové místo s vypořádáním souhlasí.
8. Ministerstvo spravedlnosti	D	K § 42 odst. 1 písm. h) Doporučujeme zvážit přeformulování dané podmínky, podle které může být provozovatelem Národního CERT pouze právnická osoba, která „<i>nebyla založena nebo zřízena výlučně za účelem dosažení zisku</i>“. Právnické osoby zpravidla nejsou zakládány explicitně a výlučně za účelem dosažení či dosahování zisku, typicky spíše za účelem podnikání. Navržená podmínka je	Akceptováno - nyní § 45 odst. 4 písm. h) Připomínkové místo s vypořádáním souhlasí.

		subjektivní a formálně neověřitelná. Navíc lze pravidlo jednoduše obejít tím, že právnická osoba bude mít i jiný účel, např. správu vlastního majetku. Dále je nejasný význam části věty za středníkem, ve které má být upravena výjimka z pravidla (či určité vyjasnění). Část věty za středníkem se netýká účelu, ale činností, které právnická osoba může vykonávat; činnost a účel jsou však různé věci. Současně věta obsahuje další podmínku, a sice, že „<i>činnost nenaruší plnění povinností uvedených v odstavci 3</i>“. V tom lze v kontextu účelu návrhu zákona spatřovat podstatnější podmínku než limitaci účelu. Lze proto doporučit namísto regulace účelu např. stanovit, že provozovatelem Národního CERT může být pouze právnická osoba, „<i>která nevykonává v oblasti kybernetické bezpečnosti činnosti neupravené tímto zákonem, který by mohly narušit plnění povinností uvedených v odstavci 3</i>“. Doporučujeme proto upřesnit textaci návrhu ustanovení.	
9. Ministerstvo spravedlnosti	Z	K § 42 odst. 2 V ustanovení § 42 odst. 2 absentuje způsob prokázání splnění podmínky podle § 42 odst. 1 písm. f). Důvodová zpráva k tomu nic neuvádí. Požadujeme proto do návrhu doplnit způsob prokazování podmínky podle písm. f). Zároveň požadujeme vyjasnit, zda a jak bude uvedené prokazováno ve vztahu k cizozemským odsouzením. <u>Tato připomínka je zásadní</u>	Akceptováno – nyní § 45 odst. 5 Ustanovení bylo změněno požadovaným způsobem: "Zájemce prokazuje splnění podmínek předložením a) čestného prohlášení v případě odstavce 4 písm. a) až d), g) a h) z jehož obsahu musí být zřejmé, že uchazeč splňuje příslušné předpoklady; b) výpisu z evidence Rejstříku trestů v případě odstavce 4 písm. f), který nesmí být starší než 3 měsíce, a c) potvrzení příslušných orgánů Finanční správy České republiky, Celní správy České republiky, České správy sociálního zabezpečení a příslušné pojišťovny v případě odstavce 4 písm. e) bod 4, která nesmí být starší než 30 dnů." Pokud jde o prokazování ve vztahu k cizozemským odsouzením, vycházíme z předpokladu, že podle § 4

		odst. 1 zákona č. 269/1994 Sb., o Rejstříku trestů, ve znění pozdějších předpisů, se do rejstříku trestů zaznamenávají mj. údaje o odsouzení cizozemským soudem, jestliže o uznání rozhodnutí takového soudu rozhodl soud podle zvláštního právního předpisu a uznané rozhodnutí bylo cizozemským soudem vydáno pro čin trestný i podle právního řádu České republiky, a podle § 364a zákona č. 141/1961 Sb., trestního řádu, předseda senátu okresního soudu rozhoduje mj. o zahlázení odsouzení cizozemským soudem. Záznamy o uznaných odsouzeních rozhodnutími cizozemských soudů tedy budou součástí předkládaných výpisů z rejstříku trestů, zahlázená odsouzení rozhodnutími cizozemských soudů se ve výpisu stejně jako zahlázená odsouzení rozhodnutími tuzemských soudů neobjeví. Reakce připomínkového místa: Ustanovení § 45 odst. 5 písm. b) stanoví, že zájemce o provozování Národního CERT prokazuje splnění podmínek podle odst. 4 písm. f) předložením výpisu z evidence Rejstříku trestů, který nesmí být starší než 3 měsíce. Upozorňujeme, že není zřejmé, z jakého důvodu by měl výpis z Rejstříku trestů vždy dokládat sám žadatel, když si jej může Úřad sám obstarat. Navrhujeme proto v souladu se snižováním administrativní zátěže žadatelů ustanovení upravit tak, že výpis si vyžádá ten, kdo splnění podmínky posuzuje (Úřad) a že žádost se podává a výpis se předává v elektronické podobě, a to způsobem umožňujícím dálkový přístup, tak, jak je tomu v jiných předpisech upravujících vymezení bezúhonnosti (např. v § 9 odst. 2 zákona o znalcích, znaleckých kancelářích a ústavech). Obdobně požadujeme upravit i návrh ustanovení § 51 odst. 2.

			V ustanovení § 51 je upravena základní způsobilost k členství v Komunitě, ale v písmenu c) se hovoří o bezúhonnosti, která ale není nikde vymezena. Navrhujeme proto buď písmeno c) upravit tak, že se v něm uvede „je bezúhonný; za bezúhonného se považuje žadatel, který...“ a pak návazně na to lze v odstavci 2 ponechat pojem „bezúhonnost“, nebo je třeba bezúhonnost v písmenu c) nahradit pojmem „základní způsobilost“ a v odstavci 2 uvést, že splnění podmínky podle odst. 1 písm. c) se prokazuje/dokládá. Ustanovení § 51 odst. 1 písm. c) navrhujeme z hlediska systematiky trestných činů a z jazykového hlediska přeformulovat následovně: „c) je bezúhonný; za bezúhonného se považuje žadatel, který nebyl v posledních 5 letech před podáním žádosti o registraci členství v Komunitě ani v průběhu trvání členství v Komunitě pravomocně odsouzen pro trestný čin, který byl spáchán v souvislosti s předmětem podnikání žadatele, nebo pro trestný čin proti majetku, trestný čin hospodářský, trestný čin obecně nebezpečný, trestný čin proti České republice, cizímu státu a mezinárodní organizaci, trestný čin proti pořádku ve věcech veřejných nebo trestný čin proti lidskosti, proti míru a válečný trestný čin, nehledí-li se na žadatele, jako by nebyl odsouzen,“. Pokud jde o dovětek týkající se bezúhonnosti osoby odsouzené v cizině, navrhujeme jej vypustit, protože obdobná formulace je zcela výjimečná, nachází se např. v návrhu zákona o zbraních, ale tam je to dáno tím, že se musí posuzovat konkrétní právní kvalifikace podle určitých odstavců, výše uložených trestů aj. Navrhujeme proto tuto otázku řešit obdobně jako jiné předpisy, kde je bezúhonnost vymezena jen obecně a

		ve vztahu k cizině je tato otázka řešena prostřednictvím dokladů, které musí žadatel předložit nebo si je příslušný orgán vyžádá. Ve vypořádací tabulce (bod 9) je uvedeno, že pokud jde o prokazování ve vztahu k cizozemským odsouzením, je vycházeno z předpokladu, že podle § 4 odst. 1 zákona č. 269/1994 Sb., o Rejstříku trestů, ve znění pozdějších předpisů, se do Rejstříku trestů zaznamenávají mj. údaje o odsouzení cizozemským soudem, jestliže o uznání rozhodnutí takového soudu rozhodl soud podle zvláštního právního předpisu a uznané rozhodnutí bylo cizozemským soudem vydáno pro čin trestný i podle právního řádu České republiky, a podle § 364a zákona č. 141/1961 Sb., trestního řádu, předseda senátu okresního soudu rozhoduje mj. o zahlazení odsouzení cizozemským soudem. Záznamy o uznaných odsouzeních rozhodnutími cizozemských soudů tedy budou součástí předkládaných výpisů z Rejstříku trestů, zahlazená odsouzení rozhodnutími cizozemských soudů se ve výpisu stejně jako zahlazená odsouzení rozhodnutími tuzemských soudů neobjeví. K uvedenému je třeba uvést, že uznaná cizozemská rozhodnutí o odsouzení osoby v jiném státě představují pouze zlomek všech cizozemských odsuzujících rozhodnutí. Do Rejstříku trestů se pak ještě zaznamenávají cizozemská rozhodnutí o odsouzení našich občanů, osob s trvalým pobytem na území České republiky a právnických osob s určitým vymezeným vztahem k území České republiky, pokud o tom rozhodne Nejvyšší soud, a v příloze výpisu se pak objevují informace o odsouzeních občanů ČR v jiných členských státech EU nebo ve Spojeném království. Z českého Rejstříku trestů tak lze získat

		informace o některých cizozemských odsouzeních, nikoli však o všech. Navrhujeme tedy upravit návrh obdobně jako např. v zákoně o znalcích, znaleckých kancelářích a znaleckých ústavech. Reakce NÚKIB: Pokud jde o povinnost zájemce o provozování Národního CERT obstarávat a předkládat výpis z evidence Rejstříku trestů, při formulaci dotčeného ustanovení bylo vycházeno ze skutečnosti, že výpis je předkládán za účelem uzavření veřejnoprávní smlouvy. Takto nahlíženo je Úřad spíše běžnou smluvní stranou než správním orgánem, na rozdíl od dokládání bezúhonnosti ze strany člena Komunity, s nímž Úřad jedná z postavení klasického správního orgánu, a proto potřebné údaje z evidence Rejstříku trestů zajišťuje sám. Zbylé části Vaší dodatečné připomínky bylo vyhověno a ustanovení § 51 odst. 1 písm. c) návrhu zákona bylo upraveno následujícím způsobem: „je bezúhonný; za bezúhonného se považuje člen Komunity, který nebyl v posledních 5 letech před podáním žádosti o registraci členství v Komunitě ani v průběhu trvání členství v Komunitě pravomocně odsouzen pro trestný čin, jehož skutková podstata souvisí s předmětem podnikání žadatele, nebo pro trestný čin hospodářský, trestný čin proti majetku, trestný čin obecně nebezpečný, trestný čin proti České republice, cizímu státu a mezinárodní organizaci, trestný čin proti pořádku ve věcech veřejných a trestný čin proti lidskosti, proti míru a válečný trestný čin nebo pokud se na žadatele ve vztahu k těmto

			pravomocným odsouzením hledí, jako by nebyl odsouzen". Reakce připomínkového místa: Ve vztahu k otázce obstarávání, resp. předkládání výpisu z Rejstříku trestů měníme naši připomínku v dané části na doporučující. Obecně máme za to, že by si orgány veřejné moci měli spíše měly obstarávat výpis z Rejstříku trestů sami, nicméně s ohledem na Vaše zdůvodnění akceptujeme, že by si danou otázku měl rozhodnout především NUKIB. Za úpravu § 51 odst. 1 písm. c) děkujeme. Vypořádáno.
10. Ministerstvo spravedlnosti	D	K § 43 Nepovažujeme za vhodné začleňovat právní úpravu stálé komise pro kontrolu činnosti NÚKIB do hlavy upravující výkon státní správy, resp. pod skupinový nadpis „instituce zapojené do výkonu státní správy v oblasti kybernetické bezpečnosti“. Kontrolní orgán není zapojen do výkonu státní správy, nýbrž plní kontrolní funkci. Dále upozorňujeme, že ačkoliv se v textu zákona hovoří výhradně o „kontrolním orgánu“, v nadpise § 43 je uvedeno označení „<i>stálá komise</i>“. Posledně uvedené označení lze přitom považovat za nevhodné, jelikož naznačuje, že se má zřejmě jednat o komisi podle zákona č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, ve znění pozdějších předpisů. Ve skutečnosti však o sněmovní komisi nejde, přičemž se právní úprava obsažená v jednacím řádu Poslanecké sněmovny na činnost kontrolního orgánu použije pouze analogicky. Doporučujeme proto v nadpise § 43 slova „<i>Stále komise</i>“ nahradit slovy „<i>Kontrolní orgán</i>“.	Akceptováno jinak - nyní § 46 Děkujeme za toto upozornění. Jistě dává smysl kontrolní orgán vyčlenit od orgánů výkonných. Pokud by k vyčlenění došlo, bylo by ale vhodné ponechat tento kontrolní orgán v blízkosti ostatních organizací upravovaných tímto návrhem, protože je to stále nejvhodnějším místem pro srozumitelnost text. Navrhujeme proto vyřešit připomínku tím způsobem, že tato úprava zůstane pod stejným paragrafem, nicméně dojde k úpravě pojmenování navrhované hlavy a ta bude vnitřně rozdělena (přidán další díl). V otázce přejmenování bylo našim cílem přiblížit zákonné označení k označení reálně používanému (https://www.psp.cz/sqw/hp.sqw?k=7800&o=8), nicméně návrhu změny také vyhovíme, tzn. došlo k přejmenování zpět na Kontrolní orgán pro kontrolu činnosti Úřadu. Připomínkové místo s vypořádáním souhlasí.

11. Ministerstvo spravedlnosti	D	K § 47 odst. 4 Doporučujeme vyjasnit, zda mají být ve větě druhé skutečně obsaženy dvě subjektivní lhůty, jelikož druhá z těchto subjektivních lhůt fakticky činí první subjektivní lhůtu nadbytečnou.	Vysvětleno – nyní § 50 odst. 4 Domníváme se, že takto stanovené lhůty se vzájemně doplňují. První lhůta vymezuje po jakou dobu (po dobu trvání členství v Komunitě) je povinen subjekt změnu údajů hlásit a druhá se vztahuje k již nastalé události, která musí být Úřadu ohlášena (ode dne, kdy tato změna nebo skutečnost nastala, nebo se o ní žadatel dozvěděl) a stanoví, do kdy musí registrovaný člen Komunity událost nahlásit. Současně je na porušení této povinnosti navázán přestupek (§ 60 odst. 11) a z důvodu právní jistoty je tak nutné mít postavené na jisto, kdy se již subjekt přestupkového jednání dopouští. Reakce připomínkového místa: Doporučující připomínka k § 47 odst. 4 (nově § 50 odst. 4) Nejsme si jisti, zda při vypořádání nedošlo k nedorozumění. Naše připomínka se nevztahovala k části ustanovení spočívající ve slovech „Po dobu trvání členství v Komunitě“. Problém po našem soudu spočívá v části „kdy tato změna nebo skutečnost nastala, nebo se o ní člen Komunity dozvěděl“. Otázkou je, zda k porušení povinnosti dojde v případě, kdy uplyne lhůta 30 dnů od změny, resp. vzniku skutečnosti, pokud se člen Komunity o této změně či skutečnosti nedozvěděl, resp. zda skutečnost, že člen Komunity dodrží druhou z lhůt (oznámi do 30 dnů ode dne, kdy se o změně/skutečnosti dozvěděl), „zhojí“ to, že změnu/skutečnost nenahlásil do 30 dnů ode dne, kdy změna nastala. Pokud je Vaším cílem vázat subjektivní lhůtu na okamžik, kdy se člen komunity o

		skutečnosti dozví, je možné ustanovení formulovat následovně: „a to ve lhůtě 30 dnů ode dne, kdy se člen Komunity o této změně nebo nastání skutečnosti dozvěděl“. Pokud však chcete založit povinnost hlásit změny/skutečnosti vždy do 30 dnů od jejich vzniku, pak by měla být část věty „, nebo se o ní člen Komunity dozvěděl“ vypuštěna. Reakce NÚKIB: K nedorozumění nedošlo. Navržená formulace měla pokrývat širší spektrum situací, které mohou nastat a současně měla být vůči povinné osobě - členovi Komunity mírnější a umožnit zhojení nedodržení lhůty 30 dnů od změny, resp. vzniku skutečnosti, pokud se člen Komunity o této změně či skutečnosti z objektivních důvodů nedozvěděl. Nicméně aby se odstranili možné výkladové pochybnosti, došlo k akceptování připomínky a úpravě předmětného ustanovení následovně: „Žadatel o registraci členství v Komunitě je povinen v žádosti podle odstavce 3 uvést pravdivé a úplné údaje potřebné pro posouzení jeho základní a zvláštní způsobilosti Úřadem. Po dobu trvání členství v Komunitě je člen Komunity povinen nahlásit změnu těchto údajů nebo skutečnosti rozhodné pro posouzení jeho základní a zvláštní způsobilosti, a to ve lhůtě 30 dnů ode dne, kdy tato změna nebo skutečnost nastala.“. Reakce připomínkového místa: Co se doporučujících připomínek týče, tak s úpravou § 50 odst. 4 souhlasíme.

			Vypořádáno.
12. Ministerstvo spravedlnosti	Z	K § 48 odst. 1 písm. e) Ve vztahu k věcnému vymezení bezúhonnosti upozorňujeme, že toto vymezení nepůsobí zcela konzistentně. Z uvedeného vymezení například vyplývá, že by podmínku bezúhonnosti nesplňovala osoba pravomocně odsouzená pro trestný čin podpory a propagace terorismu podle § 312e trestního zákoníku. Osoba pravomocně odsouzená pro trestný čin genocidia podle § 400 trestního zákoníku nebo za válečný trestný čin by však měla být podle návrhu předmětného ustanovení považována za bezúhonnou. Navrhujeme proto opětovně zvážit věcné vymezení bezúhonnosti. Dále upozorňujeme, že z návrhu není zřejmé, zda a případně jakým způsobem by měla být bezúhonnost prokazována ve vztahu k cizozemským rozhodnutím. Konečně, upozorňujeme rovněž na skutečnost, že není zřejmé, z jakého důvodu by měl výpis z Rejstříku trestů dokládat žadatel, pakliže si jej může NÚKIB sám obstarat. Požadujeme proto předmětné ustanovení dopracovat ve smyslu naší argumentace. <u>Tato připomínka je zásadní</u>	Akceptováno – nyní § 51 odst. 1 písm. c) Ustanovení bylo upraveno následovně: „nebyl v posledních 5 letech před podáním žádosti pravomocně odsouzen pro trestný čin, jehož skutková podstata souvisí s předmětem podnikání žadatele, nebo pro trestný čin hospodářský, trestný čin proti majetku, trestný čin obecně nebezpečný, trestný čin proti České republice, cizímu státu a mezinárodní organizaci, trestný čin proti pořádku ve věcech veřejných a trestný čin proti lidskosti, proti míru a válečný trestný čin; za bezúhonného se podle tohoto zákona nepovažuje ten, kdo byl v cizině pravomocně uznán vinným činem, jehož znaky odpovídají znakům některého z uvedených trestných činů; k zahrazeným odsouzením se nepřihlíží,“. Následně v návaznosti na výše uvedené doplnění byl doplněn i § 51 odst. 2, který zní následovně: „Bezúhonnost podle odstavce 1 písm. c) se dokládá výpisem z evidence Rejstříků trestů a dále doklady prokazujícími splnění podmínky bezúhonnosti vydanými státy, ve kterých se fyzická osoba zdržovala v posledních 3 letech nepřetržitě déle než 3 měsíce nebo právnická osoba vykonávala činnost v posledních 3 letech alespoň po dobu 3 měsíců. Výpis z evidence Rejstříku trestů a další doklady, jimiž se dokládá bezúhonnost, nesmí být starší 3 měsíců. Za účelem doložení bezúhonnosti si Úřad vyžádá podle právního předpisu upravujícího evidenci fyzických a právnických osob pravomocně odsouzených soudy v trestním řízení výpis z evidence Rejstříku trestů. Žádost o vydání výpisu z evidence Rejstříku trestů a výpis z evidence Rejstříku trestů se

		předávají v elektronické podobě, a to způsobem umožňujícím dálkový přístup." Reakce připomínkového místa: Viz připomínka č. 9. Reakce NÚKIB: Pokud jde o povinnost zájemce o provozování Národního CERT obstarávat a předkládat výpis z evidence Rejstříku trestů, při formulaci dotčeného ustanovení bylo vycházeno ze skutečnosti, že výpis je předkládán za účelem uzavření veřejnoprávní smlouvy. Takto nahlíženo je Úřad spíše běžnou smluvní stranou než správním orgánem, na rozdíl od dokládání bezúhonnosti ze strany člena Komunity, s nímž Úřad jedná z postavení klasického správního orgánu, a proto potřebné údaje z evidence Rejstříku trestů zajišťuje sám. Zbylé části Vaší dodatečné připomínky bylo vyhověno a ustanovení § 51 odst. 1 písm. c) návrhu zákona bylo upraveno následujícím způsobem: „je bezúhonný; za bezúhonného se považuje člen Komunity, který nebyl v posledních 5 letech před podáním žádosti o registraci členství v Komunitě ani v průběhu trvání členství v Komunitě pravomocně odsouzen pro trestný čin, jehož skutková podstata souvisí s předmětem podnikání žadatele, nebo pro trestný čin hospodářský, trestný čin proti majetku, trestný čin obecně nebezpečný, trestný čin proti České republice, cizímu státu a mezinárodní organizaci, trestný čin proti pořádku ve věcech veřejných a trestný čin proti lidskosti, proti míru a válečný trestný čin nebo pokud se na žadatele ve vztahu k těmto

			pravomocným odsouzením hledí, jako by nebyl odsouzen". Reakce připomínkového místa: Ve vztahu k otázce obstarávání, resp. předkládání výpisu z Rejstříku trestů měníme naší připomínku v dané části na doporučující. Obecně máme za to, že by si orgány veřejné moci měli spíše měly obstarávat výpis z Rejstříku trestů sami, nicméně s ohledem na Vaše zdůvodnění akceptujeme, že by si danou otázku měl rozhodnout především NUKIB. Za úpravu § 51 odst. 1 písm. c) děkujeme. Ze zasláního vyjádření nám však není stále zřejmé, jakým způsobem by měla být prokazována bezúhonnost ve vztahu k cizozemským odsouzením, zejména pak v případech, kdy je není možné zjistit z Rejstříku trestů. Bude v takových případech dostačující čestné prohlášení? Uvedené by bylo vhodné ještě vyjasnit. Reakce NUKIB: Ustanovení § 51 odst. 2 (prokázání bezúhonnosti) upravené následovně: „Bezúhonnost podle odstavce 1 písm. c) se dokládá výpisem z evidence Rejstříků trestů a dále dokladem prokazujícím splnění podmínky bezúhonnosti vydaným státem, ve kterém se fyzická osoba zdržovala v posledních 5 letech nepřetržitě déle než 3 měsíce nebo právnická osoba vykonávala činnost v posledních 5 letech alespoň po dobu 3 měsíců, zejména výpisem z evidence trestů nebo rovnocenným dokladem vydaným příslušným soudním nebo správním orgánem tohoto státu, nebo výpisem z evidence Rejstříku trestů, v jehož příloze

			jsou tyto informace obsaženy, nebo čestným prohlášením, nevydává -li cizí stát výpis nebo doklad podle tohoto odstavce.“. Připomínkové místo s vypořádáním souhlasí.
13. Ministerstvo spravedlnosti	D	K § 48 odst. 1 písm. g) Podle návrhu předmětného ustanovení má žadatel o registraci členství v Komunitě základní způsobilost, mimo jiné, pokud proti němu nebylo vydáno rozhodnutí o úpadku. Upozorňujeme, že formulace „<i>nebylo proti němu vydáno rozhodnutí o úpadku</i>“ není vhodná proto, že nereflektuje následná rozhodnutí vydaná v insolvenčním řízení. Po vydání rozhodnutí o úpadku může být například rozhodnuto podle § 158 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), že dlužník není v úpadku. V takovém případě tedy sice bylo vydáno rozhodnutí o úpadku, ale dlužník by v úpadku nebyl. Doporučujeme proto slova „<i>nebylo proti němu vydáno rozhodnutí o úpadku</i>“ nahradit slovy „<i>není v úpadku</i>“. Pokud předkladatel považuje za důležité klást důraz na právní jistotu žadatele o registraci členství v Komunitě, a proto váže negativní právní následky až na právní moc rozhodnutí o úpadku, lze uvedenou část ustanovení formulovat rovněž následujícím způsobem. „<i>není na základě pravomocného rozhodnutí insolvenčního soudu v úpadku</i>“. Konečně, pokud předkladatel považuje za vhodné umožnit členství v Komunitě rovněž žadatelům, jejichž úpadek je úspěšně řešen jedním ze sanačních způsobů, lze danou část ustanovení formulovat následovně: „<i>není na základě pravomocného rozhodnutí insolvenčního soudu v úpadku, ledaže insolvenční soud schválil reorganizační plán nebo schválil oddlužení a nerozhodl o přeměně v konkurs</i>“.	Akceptováno jinak – nyní § 51 odst. 1 písm. e) V návaznosti na připomínku došlo k úpravě předmětného ustanovení následovně: "není v likvidaci, není v úpadku, není proti němu zahájeno insolvenční řízení a není vůči němu nařízena nucená správa podle jiného právního předpisu." Odůvodnění: S ohledem na možnost registrovaného člena Komunity čerpat peněžní prostředky z programů EU, je nutné, aby požadavky na bezdlužnost byly v souladu s čl. 136 nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 ze dne 18. července 2018, kterým se stanoví finanční pravidla pro souhrnný rozpočet Unie, mění nařízení (EU) č. 1296/2013, (EU) č. 1301/2013, (EU) č. 1303/2013, (EU) č. 1304/2013, (EU) č. 1309/2013, (EU) č. 1316/2013, (EU) č. 223/2014 a (EU) č. 283/2014 a rozhodnutí č. 541/2014/EU a zrušuje nařízení (EU, Euratom) č. 966/2012. Nařízení č. 2018/1046 požaduje v čl. 136, aby subjekt nebyl v úpadku ani předmětem insolvenčního řízení. V aplikaci na podmínky české právní úpravy máme za to, že je nutné, aby subjekt alespoň čestně prohlásil, že v úpadku není, pokud ještě není podán návrh na zahájení insolvenčního a dále, aby nebylo vůbec proti žadateli zahájeno insolvenční řízení. Reakce připomínkového místa: Upozorňujeme, že v nově navrženém § 51 odst. 1 písm. e) lze považovat slova „není v úpadku,“ za

			nadbytečné. Akceptujeme rozhodnutí NÚKIB rozšířit výluky na oblast celého insolvenčního řízení. Za takové situace však dostačuje použití podmínky, že proti členu Komunity „není zahájeno insolvenční řízení“, jelikož předpokladem úpadku je zahájení insolvenčního řízení. Reakce NÚKIB: Formulace "není v úpadku" směřuje primárně na období, kdy žadatel/člen Komunity se již v úpadku nachází (tj. jsou naplněny definiční znaky úpadku podle § 3 insolvenčního zákona), ale prozatím nedošlo k zahájení insolvenčního řízení. Z ekonomického hlediska tak představuje úpadek stav, kdy již žadatel/člen Komunity není bez vnější ekonomické a další pomoci schopen dále po ekonomické stránce fungovat. Navrhovaná úprava má za cíl eliminovat případný nekalý úmysl žadatele/člena Komunity, aby prostřednictvím financí získaných z různých projektů v Komunitě řešil své ekonomické problémy. Reakce připomínkového místa: V případě textace § 51 odst. 1 písm. e) však máme jisté pochyby, zda nebude praxe tendovat spíše k formálnějšímu výkladu, který bude úpadek spojovat až s vydáním rozhodnutí o úpadku (z tohoto výkladu jsme ostatně vycházeli v našem dřívějším emailu). Z naší strany však jde pouze o doporučující připomínku. Snad by to šlo rozvést v důvodové zprávě. Vypořádáno.
14. Ministerstvo spravedlnosti	D	K § 50 odst. 2 a 3 Podle návrhu předmětného ustanovení zahájí NÚKIB v případě existence pochybností o tom, že žadatel splňuje podmínky podle § 47 odst. 2 návrhu zákona, řízení o nezpůsobilosti žadatele k registraci	Akceptováno – nyní § 53 odst. 3 V § 53 byl doplněn nový odstavec 3, který stanoví: „Úřad o nezpůsobilosti žadatele o registraci členství v

		členství v Komunitě, přičemž návrh § 50 odst. 3 předpokládá, že lze v uvedeném řízení vydat pouze rozhodnutí o nezpůsobilosti žadatele k registraci členství v Komunitě. Doporučujeme zvážit, zda by nebylo vhodné doplnit návrh o možnost vydat odlišné rozhodnutí v případě, kdy se v průběhu řízení prokáže, že je žadatel způsobilý ve smyslu § 47 odst. 2 návrhu zákona.	Komunity vydá rozhodnutí. Pokud se prokáže, že žadatel naplňuje základní a zvláštní způsobilost k členství v Komunitě podle § 51 a 52, Úřad řízení o jeho nezpůsobilosti zastaví." Připomínkové místo s vypořádáním souhlasí.
15. Ministerstvo spravedlnosti	D	K § 61 odst. 1 Doporučujeme v odůvodnění návrhu zákona postavit najisto, zda má soud v daných případech rozhodovat v řízení podle § 85 písm. b) zákona č. 292/2013 Sb., o zvláštních řízeních soudních.	Akceptováno – nyní § 63 odst. 3 Připomínkové místo s vypořádáním souhlasí.
16. Ministerstvo spravedlnosti	D	K § 61 odst. 5 Podle návrhu předmětného ustanovení může NÚKIB provést kontrolu splnění povinnosti odstranit nedostatky zjištěné při kontrole „ <i>nejdříve po uplynutí lhůty podle odstavce 1</i> “. Z návrhu tak plyne, že NÚKIB může uvedenou kontrolu provést i později, a tedy, že nemusí na uplynutí lhůty podle odstavce 1 nikterak reagovat. Doporučujeme proto přeformulovat předmětnou část ustanovení následujícím způsobem: „ <i>Úřad po uplynutí lhůty podle odstavce 1 provede kontrolu ...</i> “, aby bylo zřejmé, že má NÚKIB kontrolu provést v důsledku na uplynutí lhůty podle odstavce 1.	Vysvětleno Máte pravdu, NÚKIB může kontroly provést i později, avšak není to primární důvod zvolené formulace. Různorodost bezpečnostních opatření organizačního i technického typu, vyžaduje zachování určité možnosti flexibility posouzení i s ohledem na personální (kontrolní) kapacity NÚKIB. Plnění jednotlivých nápravných opatření jsou průběžně dokládána a vyhodnocována. V případě potřeby, například u časté neúplnosti či úplné absenci bezpečnostní dokumentace k řízení informační bezpečnosti, není apriori následná kontrola na místě nutná a jde proti principům dobré správy, jelikož jde ukončit v rámci probíhajícího příkazního řízení. I s ohledem na nárůst kontrolovaných subjektů není možné, ani při navýšení současných kontrolních možností úřadu, další kontrolu na místě provádět ve všech případech, jak u režimu vyššího tak nižšího. Připomínkové místo s vypořádáním souhlasí.
17. Ministerstvo zdravotnictví	Z	Obecně a k § 10 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	Vysvětleno

		Prosíme o vysvětlení, jakým způsobem budou dodrženy požadavky zákona a podzákoných předpisů v případě využívání cloudových SAAS (JIRA, GitHub aj.) zejména s ohledem na skutečnost, že jejich dodavatelé nemohou klást důraz na požadavky povinné osoby na tyto dodavatele? V souvislosti s výše uvedeným upozorňujeme, že rovněž nelze naplnit většinu povinností v rámci §10 uvedených tezí vyhlášky.	Povinnost zohledňovat požadavky plynoucí ze zákona a z návrhu vyhlášek při řízení dodavatele, tedy při jeho výběru a uzavření smlouvy, platí vždy. Pokud má již povinná osoba něco zasmulvněno a začnou mu s ohledem na transpozici směrnice NIS2 plynout nové povinnosti, měl by své smlouvy revidovat. Následně může uzavřít dodatek, případně původní smlouvu vypovědět a vybrat si dodavatele nového. Obdobně by měl subjekt postupovat ať už se jedná o kybernetickou bezpečnost nebo o jakékoli jiné povinnosti, které mu ukládají zákony. Z tohoto důvodu rovněž existuje lhůta, ve které se mohou povinné subjekty na změny po účinnosti zákona připravit. Stav, ve kterém by subjekty měly uzavřeny smlouvy nesplňující požadavky plynoucí z bezpečnostních opatření je jednoznačně nežádoucí. V krajním případě, kdy opravdu dodavatel trvá na tom, že nezohlední zákonné požadavky kladené na povinné osoby v režimu vyšších povinností v procesu kontraktace, lze tuto skutečnost zohlednit v plánu zvládání rizik nebo v prohlášení o aplikovatelnosti a riziko plynoucí z nedostatečného řízení dodavatelů evidovat. Je však nutné s uvedenými dokumenty kontinuálně pracovat, resp. pravidelně tyto dokumenty přezkoumávat a aktualizovat, tak aby bylo zajištěno kontinuální zlepšování, což je ostatně cílem právní regulace, stejně tak jako normy ISO/IEC 27001. Vaši připomínku nicméně evidujeme, vyhlášky jsou v současné chvíli v rozpracovaných fázích a nejsou součástí tohoto připomínkového řízení, to proběhne na začátku příštího roku. I pokud neuplatníte tuto připomínku znovu, v mezirezortním připomínkovém řízení k vyhláškám se k Vaší připomínce vrátíme. Připomínkové místo s vypořádáním souhlasí.

18. Ministerstvo zdravotnictví	Z	K § 14 a § 15 a tezím vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Mzd je v současné době plně outsourcováno v rámci správy i vlastnictví IT včetně infrastruktury a všech procesů. Outsourcing vykonává ÚZIS ČR a dále jeho subdodavatelé. Lze konstatovat, že ÚZIS ČR je provozovatelem všech informačních systémů a infrastrukturních prvků Mzd. V této souvislosti Mzd není schopno dostát požadavkům v uvedených ustanoveních včetně dalších povinností v tezích vyhlášek jako je mapování podpůrných aktiv, provedení analýzy rizik atp. či může tyto povinnosti provést čistě formalisticky - např. vyplnit prázdné PoA. Požadujeme do předkládaného předpisu doplnit uvedenou alternativu včetně stanovených povinností. Alternativně potvrzení naší domněnky, že uvedené požadavky máme plně převést na provozovatele.	Vysvětleno VV případě, že nelze plnit požadavek na zavedení více faktorové autentizace z důvodu technické nemožnosti (neaplikovatelnosti) tohoto opatření, je jako u ostatních neaplikovatelných opatření povinnost tuto skutečnost zohlednit v prohlášení o aplikovatelnosti dle § 9 odst. 1 písm. f) teze vyhlášky pro režim vyšších povinností a nejedná se tak o neplnění požadavků této vyhlášky a o nesoulad. Nicméně je třeba mít na vědomí, že zavádění vícefaktorové autentizace je jedním ze stěžejních požadavků v oblasti organizačních i technických opatření a v rámci nové akvizice je třeba plnit požadavek dle § 13 písm. g) teze vyhlášky pro režim vyšších povinností. Neshledáváme tudíž potřebu tuto konkrétní situaci více zohledňovat nad rámec navrhovaného znění. Připomínkové místo s vypořádáním souhlasí.
19. Ministerstvo zdravotnictví	Z	K § 20 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností V případě využití infrastrukturních či jiných služeb ve formě SAAS v rámci regulované služby nelze zajistit některé požadavky (např. vícefaktorovou autentizaci či délku hesla) pro konzumované cloudové služby. Požadujeme upravení uvedené situace.	Vysvětleno V případě, že nelze plnit požadavek na zavedení vícefaktorové autentizace z důvodu technické nemožnosti (neaplikovatelnosti) tohoto opatření, je jako u ostatních neaplikovatelných opatření povinnost tuto skutečnost zohlednit v prohlášení o aplikovatelnosti dle § 9 odst. 1 písm. f) teze vyhlášky pro režim vyšších povinností a nejedná se tak o neplnění požadavků této vyhlášky a o nesoulad. Nicméně je třeba mít na vědomí, že zavádění vícefaktorové autentizace je jedním ze stěžejních požadavků v oblasti organizačních i technických opatření a v rámci nové akvizice je třeba plnit požadavek dle § 13 písm. g) teze vyhlášky pro režim vyšších povinností. Neshledáváme tudíž potřebu tuto

			konkrétní situaci více zohledňovat nad rámec navrhovaného znění. Vaši připomínku nicméně evidujeme, vyhlášky jsou v současné chvíli v rozpracovaných fázích a nejsou součástí tohoto připomínkového řízení, to proběhne na začátku příštího roku. I pokud neuplatníte tuto připomínku znovu, v mezirezortním řízení k vyhláškám se k Vaší připomínce vrátíme. Připomínkové místo s vypořádáním souhlasí.
20. Ministerstvo zdravotnictví	Z	K § 27 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Vzhledem k tomu, že Mzd bude nově povinným subjektem v režimu vyšších povinností v oblasti výkonu veřejné správy a povinnosti budou vztaženy k Mzd jako celku, lze předpokládat, že u primárních aktiv souvisejících s regulovanou službou, které jsou velmi nevýznamné s nízkou zjištěnou hodnotou budou dle cílů podle § 16 stanoveny úrovně poskytovaných služeb takovým způsobem, že nebude třeba zajišťovat redundanci podpůrných aktiv podle § 27odst. 1 písm. c)?	Vysvětleno Opatření ustanovení § 27 VKB se realizuje v souladu s cíli BCM dle § 16 VKB, cíle jsou definovány na základě hodnocení rizik a BIA. Tento postup se neliší od současného znění VKB. Vaši připomínku evidujeme, vyhlášky jsou v současné chvíli v rozpracovaných fázích a nejsou součástí tohoto připomínkového řízení, to proběhne na začátku příštího roku. I pokud neuplatníte tuto připomínku znovu, v mezirezortním řízení k vyhláškám se k Vaší připomínce vrátíme. Připomínkové místo s vypořádáním souhlasí.
21. Ministerstvo zdravotnictví	Z	K § 27 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností V rámci resortu zdravotnictví již dnes existuje velká heterogenita při přístupu k definici primárních aktiv zajišťující základní službu u povinných subjektů. Typicky od jednoho primárního aktiva až po vyšší desítky primárních aktiv zahrnujících v zásadě všechny informační činnosti nemocnice. Rádi bychom společně s NÚKIB připravili metodickou pomůcku, kde bychom vymezili „ideální“ seznam primárních aktiv vztažených k definované regulované službě zejména pro regulované služby v režimu vyšších povinností. Tento	Akceptováno Nejedná se z našeho pohledu o klasickou připomínku, ale o žádost k budoucí spolupráci na metodické pomůcce k identifikaci primárních a podpůrných aktiv. V současné době je již Úřadem vydán podpůrný materiál na stránkách Úřadu, který by mohl být pro Vás užitečný (Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti), nicméně se

		postup volíme i s ohledem na teze § 27 odst. 1 písm. c) vyhlášky, které budou u některých podpůrných aktiv nerealizovatelné.	nebráníme konzultacím při přípravách Vašeho nového metodického materiálu. Připomínkové místo s vypořádáním souhlasí.
22. Ministerstvo zdravotnictví	Z	K bodu 18.1 přílohy k vyhlášce o regulovaných službách Požadujeme doplnit další kritérium s názvem: <i>Služba ukládající zdravotní dokumentaci od více poskytovatelů zdravotních služeb za účelem jejího sdílení podle zvláštních právních předpisů (z.č. 372/2011 a 325/2021).</i> Mzd plánuje v rámci implementace centrálních služeb eHealth předávání zdravotnické dokumentace v rámci afinitních domén, které budou budovány typicky pro vícero poskytovatelů zdravotních služeb, a to i třetími osobami. Afinitní doména tedy bude obsahovat prioritní typy zdravotnické dokumentace pacienta od vícero poskytovatelů zdravotních služeb. Tomu by měla odpovídat i její nadstandardní ochrana na úrovni regulované služby.	Neakceptováno Z momentálního znění návrhu se nám situace jeví tak, že daná služba zatím není v provozu. Vyhláška o regulovaných službách bude mít navíc své vlastní mezirezortní připomínkové řízení v rámci něhož může být služba do vyhlášky přidána, pokud dojde k vývoji situace. Vedle toho službu tohoto významu je také možné určit dle kritérií pro určení v případě potřeby. Připomínkové místo s vypořádáním souhlasí.
23. Ministerstvo zdravotnictví	Z	K § 38 a násl. zákona o kybernetické bezpečnosti Mzd požaduje, aby stav kybernetického nebezpečí byl namísto v zákoně o kybernetické bezpečnosti ukotven v zákoně č. 240/2000 Sb., o krizovém řízení (krizový zákon), ve znění pozdějších předpisů. Zvolené řešení a ukotvení tohoto stavu v zákoně o kybernetické bezpečnosti nepovažuje Mzd za systémové. Mzd je toho názoru, že legislativní úprava všech krizových stavů by měla být uvedena v jednom zákoně k tomu určeném (krizový zákon), jenž je v současné době předmětem novely a reflektuje zkušenosti zejm. z krizových situací epidemie onemocnění Covid-19 a migrační vlna velkého rozsahu.	Neakceptováno – nyní § 39 a násl. Na vhodném znění celé soustavy ustanovení o stavu kybernetického nebezpečí spolupracujeme s Ministerstvem vnitra – Generálním ředitelstvím Hasičského záchranného sboru a návrh bude upraven na základě těchto jednání. Navrhovaná právní úprava nemá za cíl zasahovat do práv způsobem, který by odpovídal nouzovému stavu a nemá za cíl být přímou součástí krizových stavů podle krizového zákona. Máme za to, že úpravy stavu kybernetického nebezpečí přináší nyní už jen taková opatření, která jsou srovnatelná s např. mimořádným stavem nouze v energetice, který je rovněž obsažen v energetickém zákoně, a tedy rovněž mimo krizový zákon. Připomínkové místo s vypořádáním souhlasí.

24. Ministerstvo zdravotnictví	Z	K § 39 a § 40 a násl. zákona o kybernetické bezpečnosti Mzd požaduje, aby pravomoc k vyhlášení stavu kybernetického nebezpečí a vydání opatření k řešení stavu kybernetického nebezpečí nebyla dána pouze řediteli NÚKIB. Rozhodnutí o stavu nebezpečí by mělo být provedeno na základě projednání s Ministerstvem vnitra, Ministerstvem obrany nebo po projednání v krizovém štábu, popř. Ústředním krizovým štábu. Stav kybernetického nebezpečí představuje celostátní ohrožení a Mzd nepovažuje za žádoucí, aby tato pravomoc byla dána pouze jednomu vedoucímu ústředního správního úřadu, a to bez žádného kontrolního mechanismu voleného orgánu nebo bez projednání s resorty, jichž se boj proti kybernetickým útokům bezprostředně dotýká (organizovaný zločin, kybernetická obrana).	Neakceptováno – nyní § 39 a násl. Na vhodném znění celé soustavy ustanovení o stavu kybernetického nebezpečí spolupracujeme s Ministerstvem vnitra – Generálním ředitelstvím Hasičského záchranného sboru a návrh bude upraven na základě těchto jednání. Navrhovaná právní úprava nemá za cíl zasahovat do práv způsobem, který by odpovídal nouzovému stavu, tj. zásah v intenzitě nouzového stavu je ponechán vládě a není svěřen do rukou ředitele Úřadu. V případě zmíněných ustanovení došlo s ohledem na výše uvedené k úpravám. Máme za to, že úpravy stavu kybernetického nebezpečí přináší nyní už jen taková opatření, která jsou srovnatelná s např. mimořádným stavem nouze v energetice, a proto je možné, aby jej vyhlášoval ředitel Úřadu. Připomínkové místo s vypořádáním souhlasí.
25. Ministerstvo zdravotnictví	Z	K § 40 zákona o kybernetické bezpečnosti S ohledem na skutečnost, že v § 39 odst. 4 je uvedeno, že „Opatření k řešení stavu kybernetického nebezpečí, jejichž platnost zůstane zachována (po vyhlášení nouzového stavu), se dále považují za krizová opatření nařízená vládou.“ je nezbytné, aby tato opatření byla dána do souladu s krizovými opatřeními uvedenými v krizovém zákoně. Současně Mzd požaduje upřesnění jednotlivých opatření tak, aby bylo zřejmé, že budou využita pouze pro překonání krizové situace a bylo zřejmé komu jsou určena (např. odst. 1 písm. a) komu je ředitel Úřadu oprávněn poskytnout věcné prostředky, odst. 1 písm. d) komu je ředitel Úřadu oprávněn nařídit práci v pohotovostním režimu). Jednotlivými krizovými opatřeními je zasahováno do práv a svobod občanů ČR (Ústava ČR a Listina základních práv a svobod), a je tedy nezbytné, aby byla v souladu s krizovým zákonem, jenž obsahuje	Vysvětleno – nyní § 39 a násl. Na vhodném znění celé soustavy ustanovení o stavu kybernetického nebezpečí spolupracujeme s Ministerstvem vnitra – Generálním ředitelstvím Hasičského záchranného sboru a návrh bude upraven na základě těchto jednání. Navrhovaná právní úprava nemá za cíl zasahovat do práv způsobem, který by odpovídal nouzovému stavu, tj. zásah v intenzitě nouzového stavu je ponechán vládě a není svěřen do rukou ředitele Úřadu. V případě zmíněných ustanovení došlo s ohledem na výše uvedené k úpravám. Máme za to, že úpravy stavu kybernetického nebezpečí přináší nyní už jen taková opatření, která jsou srovnatelná s např. mimořádným stavem nouze v energetice. Například část ustanovení týkající se

		jejich výčet. Současně je Mzd toho názoru, že by měly být vyžadovány pouze informace, které povedou k překonání krizové situace a nikoli všechny informace např. o personálních kapacitách celého úřadu. Dále Mzd považuje za žádoucí, aby bylo jasné stanoveno, koho se jednotlivá opatření týkají, aby se minimalizovalo riziko zneužití pravomocí.	shromažďování informací byla z návrhu odstraněna celá. Připomínkové místo s vypořádáním souhlasí.
26. Ministerstvo zdravotnictví	Z	Obecně Žádáme o vysvětlení, k jakým změnám povinností v rámci regulovaných služeb využívajících cloudová podpůrná aktiva jako jsou MS Azure, O365 aj. a možnosti jejich využití v regulovaných službách včetně strategicky významných služeb dojde, v případě přijetí navrhované úpravy.	Vysvětleno V tomto ohledu k žádným změnám nedochází. Jde stále o standardní řízení dodavatelů, kdy všechny povinnosti, které má poskytovatel regulované služby plnit, musí buď plnit sám nebo přenést na dodavatele v případě, že provoz nějaké části informačního systému zajišťuje dodavatelsky, např. s využitím služeb cloud computingu. Připomínkové místo s vypořádáním souhlasí.
27. Ministerstvo zdravotnictví	D	Obecně Jakým způsobem bude mít požadavek na infrastrukturní části regulované služby např. na O365? Prosím vysvětlete.	Vysvětleno Z pohledu aktuálních tezí prováděcích předpisů (konkrétně Vyhlášky pro režim vyšších povinností) lze v tomto kontextu za obecného předpokladu, že infrastrukturní část regulované služby bude v rozsahu systému řízení bezpečnosti informací, uvést např. požadavek na řízení dodavatelů poskytujících cloudové služby O365 (např. zohlednění relevantních oblastí z přílohy č. 7 vyhlášky) nebo požadavek na zavedení vícefaktorové autentizace. Toto jsou však pouze příklady konkrétních požadavků tohoto prováděcího předpisu, které jsou relevantní pro téma O365, nicméně se tohoto tématu dotýkají samozřejmě požadavky na zavedení všech organizačních i technických bezpečnostních opatření uvedených v tomto prováděcím předpise, jako tomu je i za aktuální legislativní úpravy. Nejedná se tudíž z pohledu

			vyhlášky pro vyšší režim o zásadní změny v této oblasti. S ohledem na možný přechod na M365 od společnosti Microsoft, je na místě dále vyhodnotit vznik případných nových povinností reflektujících současnou právní regulaci cloudových služeb v ČR. Zejména zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů - §6l - povinnost orgánů veřejné moci nakupovat z katalogu cloud computingu. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - § 4 odst. 5 - zařadit informační systém, který povinná osoba plánuje přemístit do cloudu, do bezpečnostní úrovně podle vyhlášky 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci a zajistit dodržování bezpečnostních pravidel podle vyhlášky č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu. V neposlední řadě je nutné také splnit povinnosti vyhodnocení tzv. „vstupních kritérií“ uvedených ve vyhlášce 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu. Připomínkové místo s vypořádáním souhlasí.
28. Unie zaměstnavatelských svazů České republiky	Z	<u>Obecné připomínky</u> Zákon v některých paragrafech odkazuje na „prováděcí právní předpis“, čímž je myšlena odpovídající a nově vznikající vyhláška. Myslíme si, že pro někoho, kdo zákon a nové vyhlášky má načtené je jasné, o který prováděcí právní předpis se jedná. Ovšem pro někoho, kdo si bude zákon číst poprvé, to tak jasné být nemusí. Bylo by proto podle nás lepší, kdyby odkaz na daný předpis byl uveden pod čarou stejně tak, jak jsou uvedeny čísla zákonů. Vyhlášek totiž s tímto zákonem vyjde aktuálně 6 a tento krok by čtenářům pomohl k lepšímu pochopení systému vztahu zákona a odpovídajících vyhlášek. Pokud	Neakceptováno Odkaz na prováděcí právní předpis je učiněn v souladu s čl. 45 odst. 3 Legislativních pravidel vlády. Rozumíme požadavku na materiál, který by pomohl lepšímu pochopení vztahu mezi zákonem a vyhláškami, příp. i návodnými grafickými materiály pro zákonem stanovené procesy. Úřad plánuje takové materiály pro adresáty norem vytvářet, v tuto chvíli již vzniká materiál obsahující návod na identifikaci.

		toto není možné, tak by adresátům pomohl podpůrný materiál NÚKIB k pochopení systému vyhlášek. Dále by byl zcela jistě nápomocný materiál s grafickým znázorněním, jak se má adresát normy identifikovat, kam jak a kam zaregistrovat atp.	Přípomínkové místo s vypořádáním souhlasí.
29. Unie zaměstnavatelských svazů České republiky	Z	Uplatňujeme připomínky k části návrhu zákona, která zapracovává mechanismus prověřování bezpečnosti dodavatelů do strategicky významné infrastruktury. Zásadní je nový regulační nástroj úřadu, kdy úřad má právo autoritativně zasáhnout do svobody podnikání a vlastnického práva soukromých subjektů a omezit volnou hospodářskou soutěž tím, že rozhodne o omezení nebo vyloučení konkrétních dodavatelů z plnění tzv. bezpečnostně významných dodávek poskytovatelům strategicky významných služeb, a to jak v rozsahu již realizovaných dodávek, tak v rozsahu všech budoucích dodávek. Proto by tento nástroj a proces, jež vede k vydání správního aktu (opatření obecné povahy) o omezení nebo vyloučení dodavatele z bezpečnostně relevantních dodávek poskytovatelům strategicky významné služby, měl dle našeho názoru splňovat nejpřísnější nároky na transparentnost, předvídatelnost a proporcionalitu právní úpravy tak, aby nebyla zasažena právní jistota mechanismem dotčených subjektů. Z tohoto pohledu uplatňujeme následující připomínky: Přesah problematiky mechanismu nad rámec kybernetické bezpečnosti. Samotná důvodová zpráva k návrhu zákona uvádí, že: „<i>mechanismus prověřování bezpečnosti dodavatelského řetězce, který je součástí návrhu zákona, je pak odrazem národních požadavků na zvýšení bezpečnosti a <u>snížení rizik plynoucích z netechnických aspektů zajišťování kybernetické bezpečnosti</u> a jako takový nemá doposud odraz v platné legislativě. V jistých aspektech je zčásti podobný úpravě zákona č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic).</i>“ Dále při vydání opatření obecné povahy, kterým úřad omezí nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky, úřad bude vyhodnocovat kritéria rizikovosti dodavatele	Neakceptováno NÚKIB nemá a ani nemůže mít za cíl určovat hospodářské ambice České republiky či její zahraniční politiku. Zmíněná kritéria posuzování rizikovosti dodavatele v rámci teze vyhlášky sloužila primárně jako vodítko/metodika k určení hrozby. Nutno dodat, že vyhláška o kritériích rizikovosti dodavatele byla, rovněž z důvodu obdobných připomínek, které směřovaly na smysl kritérií, zrušena. Kritériem tudíž zůstává bezpečnost ČR a její vnitřní či veřejný pořádek. V rámci procesu posuzování rizikovosti dodavatele je tak potřeba vzít v potaz také aspekty související s tzv. netechnickými otázkami, zejména ty související s třetí zemí, která může mít na dodavatele bezpečnostně významné dodávky, a tudíž na kybernetickou bezpečnost České republiky, vliv. Smyslem mechanismu není vytvářet zátěž pro jednotlivé segmenty, nýbrž tuto zátěž mitigovat skrz instrumenty popsané návrhem zákona a zamezit přístupu rizikových dodavatelů do kritických částí infrastruktury. Co se týče zapojení Ministerstva průmyslu a obchodu do procesu, tak to je dle § 30 odst. 1 navrhovaného zákona zapojeno přímo do procesu posuzování rizikovosti dodavatele. Navíc opatření obecné povahy o případném omezení či zákazu dodavatele NÚKIB rovněž projedná mimo jiné s ministerstvem průmyslu a obchodu (§ 31 odst. 2), aby byly získány všechny relevantní pohledy a perspektivy pro proporcionální

	určená vyhláškou, kteřa jsou výlučně netechnické povahy (politické charakteristiky země původu dodavatele, právní prostředí země původu dodavatele a „bezúhonnost“ dodavatele) a nijak nesouvisí se zajišťováním kybernetické bezpečnosti. V této souvislosti je tedy otázkou, který správní úřad by měl prověřování bezpečnosti dodavatelského řetězce provádět a mít pravomoc opatření obecné povahy vydat. Dle názoru SZPČR se prověřování a omezování nebo zákazu dodavatelů předně dotýká hospodářské soutěže a ekonomiky. Jejich omezení nebo vyloučení bude mít dopad na rozvoj ICT infrastruktury a na výši nákladů s tím spojených a je záležitostí státní průmyslové a obchodní politiky, kde ústředním orgánem státní správy je podle § 13 odst. 1 písm. a) zákona č. 2/1969 Sb., ve znění pozdějších předpisů, Ministerstvo průmyslu a obchodu České republiky (dále jen „ministerstvo“). Ministerstvo je ústředním správním orgánem rovněž pro zahraničně ekonomickou politiku. Dle § 13 odst. 3 mimo jiné koordinuje zahraničně obchodní politiku České republiky ve vztahu k jednotlivým státům, zabezpečuje sjednávání dvoustranných a mnohostranných obchodních a ekonomických dohod včetně komoditních dohod, aj. Ministerstvo je tedy právními předpisy určeno k řešení veškerých zahraničně-obchodních záležitostí. Současně dle platné právní úpravy patří do gesce ministerstva prověřování zahraničních investic, ke kterému je zmocněno na základě zák. č. 34/2021 Sb., a pojí se s prověřováním zahraničních investic z důvodu ochrany bezpečnosti České republiky a vnitřního a veřejného pořádku. Posuzování je tak založeno na obdobných kritériích rizikovosti jako navrhuje teze prováděcí vyhlášky k návrhu zákona o kybernetické bezpečnosti. SZPČR s ohledem na výše uvedené navrhuje, aby prověřování bezpečnosti dodavatelského řetězce a pravomoc vydávat opatření obecné povahy náležela ministerstvu s tím, že role a pravomoci úřadu by měla být obdobné jako jsou v procesu prověřování přímých zahraničních investic.	stanovení povinností daným opatřením obecné povahy. V souvislosti s politickou odpovědností je nutno zmínit, že úkol řešit bezpečnost dodavatelského řetězce byl NÚKIB dán Bezpečnostní radou státu (kteřa je do procesu také zapojena - § 31 odst. 2), přičemž se NÚKIB za svou činnost zodpovídá vládě, kteřa jej úkoluje. Připomínkové místo s vypořádáním souhlasí.

30. Unie zaměstnavatelských svazů České republiky	Z	Vágnost a arbitrárnost kritérií rizikovosti dodavatele Celé hodnocení rizikovosti dodavatele stojí na naplnění kritérií rizikovosti, které určuje sám úřad vyhláškou (a jejich určení je tedy zcela v pravomoci úřadu) a která spočívají v posuzování politických charakteristik země původu dodavatele, právního prostředí země původu dodavatele a posuzování integrity osoby dodavatele, tedy výlučně netechnických kritériích. S výjimkou kritérií pro posuzování integrity osoby dodavatele jsou tato kritéria podle názoru SZPČR zcela neměřitelná, arbitrární a jejich použití lehce zneužitelné. Forma a metodika vyhodnocení naplnění kritérií rovněž zcela chybí a lze si stěží představit, jak bude například posuzováno naplnění kritéria – existence právních předpisů v zemi mající vliv na dodavatele, které ukládají povinnost spolupráce s orgány veřejné moci, jež vykonávají činnost odpovídající činnosti zpravodajských služeb, a to bez nezávislého soudního dohledu či přezkumu. Dále není zřejmé, proč úřad v rámci zajišťování kybernetické bezpečnosti zcela rezignuje na zkoumání a vyhodnocování naplnění technických a jiných kritérií bezpečnosti produktů a služeb dodavatele jako jsou certifikace, smluvní závazky, audity kybernetické bezpečnosti, apod., které mohou sehrávat v hodnocení kybernetické bezpečnosti zcela zásadní roli. SZPČR navrhuje zvýšení transparentnosti procesu hodnocení kritérií a zavedení technických kritérií uplatňovaných u konkrétního dodavatele, resp. poskytovatele strategicky významné služby mezi kritéria hodnocení rizikovosti dodavatele.	Neakceptováno Kritéria cílila na strategická, nikoliv technická, kritéria záměrně. NÚKIB pevně věří, že je v schopnostech státu a jeho organizačních složek, v tomto případě též NÚKIB, posuzovat rizika na strategické rovině, tedy na základě strategických kritérií, ke kterým jednotlivé orgány státu disponují relevantními informacemi. Obdobně se tak děje i v jiných státech, včetně Spojených států amerických, Německa, Dánska či Estonska. Strategická kritéria jsou pro posouzení důvěryhodnosti/rizikovosti dodavatele klíčová. Posuzování technických či obchodně-ekonomických kritérií by pak mělo být primárně na jednotlivých povinných osobách, které v těchto otázkách disponují širokými znalostmi, jež dokáží aplikovat na své hospodářské potřeby. Stát, potažmo NÚKIB, by měl zasáhnout až v případě posuzování rizikovosti dodavatele na strategické úrovni, kdy stát disponuje informacemi, ke kterým nemohou mít povinné subjekty přístup. To znamená, že aspekty typu „technická a jiná kritéria bezpečnosti produktů a služeb dodavatele jako jsou certifikace, smluvní závazky, audity kybernetické bezpečnosti, apod.“ představují právě zmíněná technická kritéria, která jsou dobře posouditelná ze strany povinných osob a k jejichž vyhodnocení není potřeba stát. Nutno však dodat, že zmíněná kritéria posuzování rizikovosti dodavatele v rámci vyhlášky sloužila primárně jako vodítko/metodika k určení hrozby, přičemž vyhláška o kritériích rizikovosti dodavatele byla, mimo jiné důvodů uvedených v připomínce, vyřazena. Kritériem tudíž zůstává bezpečnost ČR a její vnitřní či veřejný pořádek.

			Připomínkové místo s vypořádáním souhlasí.
31. Unie zaměstnavatelských svazů České republiky	Z	Absence opravného prostředku proti opatření obecné povahy Výstupem procesu prověřování bezpečnosti dodavatelských řetězců má být opatření obecné povahy (OOP) vydané úřadem. V případě OOP neexistuje možnost podání řádného opravného prostředku. Proti omezení či zákazu obchodních vztahů stanovených OOP je tak není možnost bránit se opravným prostředkem (proti OOP nelze podat odvolání ani rozklad), což dále přispívá k netransparentnosti a možné arbitrárnosti rozhodování úřadu.	Vysvětleno Proti opatření obecné povahy lze podat návrh na zahájení přezkumného řízení nebo podat správní žalobu na jeho zrušení. V procesu vydávání OOP mohou oprávněné subjekty také uplatňovat proti jeho návrhu připomínky. Proti tomuto institutu sice tedy není možné podávat řádné opravné prostředky, ale je možné se proti němu bránit jinými způsoby. Závěry uvedené v OOP také musí být řádně a přezkoumatelně odůvodněny. Pokud by plnění opatření obecné povahy mohlo podstatným způsobem ohrožovat poskytování strategicky významné služby, může také být udělena výjimka z podmínek nebo zákazu jím stanovených. Připomínkové místo s vypořádáním souhlasí.
32. Unie zaměstnavatelských svazů České republiky	Z	Narušení podnikatelského prostředí V důsledku připravované legislativy by také mohlo být narušeno legitimní očekávání podnikatelů, protože mnoho parametrů mechanismu může být ze strany úřadu kdykoli změněno (vzhledem k tomu, že úřad přijímá vyhlášky tyto oblasti blíže upravující) a rovněž může dojít k zákazu či významnému omezení jeho dodavatelů. Takto rozsáhlá rozhodovací pravomoc poskytuje velký prostor pro libovůli při rozhodování úřadu a představuje tak rozsáhlé riziko. Konečným důsledkem mechanismu tak může být úplné dlouhodobé zastrašení podnikatelských subjektů od spolupráce s dodavateli z vybraných zemí. Je zapotřebí si také uvědomit, že při takto obecně nastavených kritériích může dojít k tomu, že „rizikovou“ zemí se v okamžiku změny politické reprezentace v ČR náhle stane stát, u nějž by to navrhovaná právní regulace v tuto chvíli absolutně nepředpokládala.	Vysvětleno Rozumíme, že nová právní úprava může vyvolávat v některých povinných subjektech obavy, nicméně odvětví, kterých se mechanismus bude týkat, jsou stanovena zákonem a NÚKIB stejně jako všechny ostatní správní orgány postupuje tak, aby naplňoval principy dobré správy. Případnou libovůli správních úřadů lze napravit správní žalobou podanou k nezávislému soudu. Připomínkové místo s vypořádáním souhlasí.

33. Unie zaměstnavatelských svazů České republiky	D	K § 30 zákona o kybernetické bezpečnosti Doporučujeme zvážit možné dopady na <i>poskytovatele strategicky významných služeb</i> v situaci, kdy klíčové informační systémy jsou ve „vendor locku“, a výměna dodavatele není reálná v termínech deklarovaných v ustanovení § 30 navrhované úpravy. Vzhledem k tomu, že dodavatel nemá žádnou povinnost uzavírat smlouvu, kterou uzavřít nechce, tak navrhovaná úprava bude bez doplnění stavět zadavatele veřejných zakázek před dilema, zda nedodržet dotčené právní předpisy, nebo narušit provoz svých informačních systémů. Mělo by proto dojít k lepšímu vymezení priorit ze strany předkladatele návrhu.	Vysvětleno - nyní § 31 Prioritou NÚKIB je zajistit bezpečnost dodavatelského řetězce. Lhůty k plnění povinností stanovených opatřením obecné povahy budou dostatečně dlouhé (mimo jiné může být při jejich stanovení zvážen i vendor lock-in) na to, aby se poskytovatelé strategicky významných služeb vypořádali i s vendor lock-in. V případě, kdy to nebude možné, mohou poskytovatelé strategicky významné služby požádat o výjimku dle § 32. Připomínkové místo s vypořádáním souhlasí.
34. Unie zaměstnavatelských svazů České republiky	D	K § 33 zákona o kybernetické bezpečnosti Doporučujeme se více zaměřit na možné (finanční) dopady na <i>poskytovatele strategicky významných služeb</i>, a to v souvislosti s možnou výpovědí závazku dodavateli podle § 33 navrhované úpravy. Z důvodů uvedených v § 30 navrhované úpravy tak sice lze vypovědět závazek ze smlouvy na veřejnou zakázku, avšak není výslovně vyloučena eliminace případných sankcí ze strany dodavatele.	Vysvětleno - nyní § 34 Vypovězení smluvního závazku na základě zákona by mělo být vždy bezúplatné; případná sjednaná sankce za výpověď smlouvy by měla mít buď charakter odstupného dle § 1992 občanského zákoníku (které je nicméně spojeno nikoliv s ukončením závazku ex nunc, ale ex tunc, případně výpověď smluvní, která by tak byla alternativní možností k ukončení závazku ze zákona. Na základě jiných připomínek bylo nicméně ustanovení upraveno a právo na ukončení dlouhodobých závazků tak bude přiznáno i subjektům, které nejsou v postavení zadavatele podle zákona o zadávání veřejných zakázek. Připomínkové místo s vypořádáním souhlasí.
35. Unie zaměstnavatelských svazů České republiky	Z	K návrhu prováděcí vyhlášky o regulovaných službách, k bodu 19.1. Přílohy Kritéria pro identifikaci regulované služby Navrhujeme vypustit: „, nebo	Akceptováno jinak Došlo k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších

	b) většina prováděných výzkumných projektů je financována z více než 50 % z veřejných zdrojů.“ Nebo alternativně doplnit za slova „nebo jiná výzkumná organizace“: „, s výjimkou výzkumné organizace zřizované nebo založené ministerstvem kultury, nebo výzkumné organizace zřízené nebo založené jiným zřizovatelem či zakladatelem, která je knihovnou, muzeem nebo galerií,“ <u>Odůvodnění:</u> Podle navrhovaného znění by regulovanou službou v režimu vyšších povinností byla každá výzkumná organizace zapsaná v seznamu vedeném podle § 33a zákona č. 130/2002 Sb., o podpoře výzkumu a vývoje z veřejných prostředků a o změně některých souvisejících zákonů (zákon o podpoře výzkumu a vývoje), a to pokud je většina prováděných výzkumných projektů financována z více než 50 % z veřejných zdrojů. V návrhu není nijak zohledněna celková výše veřejných zdrojů, které organizace vynakládá na výzkum. Povinnost by proto dopadla i na knihovny, muzea a galerie, které byly zřízeny především za účelem poskytování přístupu veřejnosti k informacím, znalostem a kulturnímu bohatství, a výzkum provádí jako doplněk k této činnosti. Jde přitom o organizace, které jsou již nyní z velké části podfinancované. Navíc by tyto organizace musely soutěžit o kvalifikované pracovníky pro tuto oblast s dalšími organizacemi a odčerpávaly by tak již dnes nedostatkové kvalifikované specialisty těm organizacím, které jsou pro provoz státu opravdu kritické. Paradoxně by tak tento požadavek vedl k dalšímu ohrožení státu. Domníváme se, že hledisko financování z veřejných zdrojů by samo o sobě nemělo být kritériem pro určení, že má organizace podléhat povinnostem dle zákona o kybernetické bezpečnosti. Případný kybernetický útok na výzkum na poli kultury pravděpodobně nebude	povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji. Zároveň se však domníváme, že není koncepční a účelné zavádět v rámci regulace výzkumu výjimky pouze na základě zaměření daného vývoje. Taková výjimka by předjímal, že některé obory výzkumu jsou méně důležité než jiné, přičemž veřejné prostředky jsou jim ovšem poskytovány také. Nicméně co se týče partnerských organizací, je třeba si uvědomit, že i ony mají za úkol zaměřit své řízení bezpečnosti na samotnou službu, která je regulována. To znamená, že v případě, že se partnerské organizace podílejí na velké výzkumné infrastruktuře například pouze prostřednictvím jejího financování, nebude v rámci jejich organizace nalezeno podpůrné aktivum, na které by musely zavádět opatření. Stejně tak, pokud jsou vlastníkem pouze malé části samotné infrastruktury a tuto mají oddělenou od své ostatní infrastruktury, která není regulována, zaměřují své řízení bezpečnosti informací pouze na tuto část výzkumné infrastruktury, která představuje aktiva sloužící k poskytování výzkumné činnosti. Vaši připomínku nicméně evidujeme, vyhlášky jsou v současné chvíli v rozpracovaných fázích a nejsou součástí tohoto připomínkového řízení, to proběhne na začátku příštího roku. I pokud neuplatníte tuto připomínku znovu, v mezirezortním připomínkovém řízení k vyhláškám se k Vaší připomínce vrátíme. Připomínkové místo s vypořádáním souhlasí.

		ohrožením pro chod státu a vynakládání nepřiměřených prostředků na obranu povede pouze ke zbytečnému vynakládání veřejných prostředků, nebo naopak k ukončení drobných výzkumů, neboť náklady na zavedení vyššího režimu kybernetické bezpečnosti by zdaleka přesáhly veřejné zdroje získané na výzkum.	
36. Unie zaměstnavatelských svazů České republiky	Z	K návrhu prováděcí vyhlášky o regulovaných službách, k bodu 19.2. Přílohy Kritéria pro identifikaci regulované služby Navrhujeme za slova <i>„Hostitelská nebo partnerská instituce velké výzkumné infrastruktury“</i> doplnit: <i>„, s výjimkou instituce zřizované nebo založené ministerstvem kultury, nebo instituce zřízené nebo založené jiným zřizovatelem, která je knihovnou, muzeem nebo galerií,“</i> nebo alternativně doplnit: <i>„, s výjimkou hostitelské nebo partnerské instituce velké výzkumné infrastruktury v oblasti sociálních a humanitních věd,“</i> <u>Odůvodnění:</u> Podle navrhovaného znění by regulovanou službou v režimu vyšších povinností byla každá výzkumná organizace, zapojená do některé z velkých infrastruktur. To je pochopitelné například u biomedicínského výzkumu, některé výzkumné infrastruktury jsou však zaměřeny na jazykovědu, digitální humanitní vědy nebo archeologii. Přehled všech infrastruktur v této oblasti je zde: https://www.vyzkumne-infrastruktury.cz/humanitni-vedy/. V návrhu není nijak zohledněna skutečnost, že výzkum v oblasti sociálních a humanitních věd je jednoznačně postaven na otevřeném publikování výsledků, stejně tak úkolem paměťových institucí je v co	Akceptováno jinak Děkujeme za zaslanou připomínku. Došlo k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji. Zároveň se však domníváme, že není koncepční a účelné zavádět v rámci regulace výzkumu výjimky pouze na základě zaměření daného vývoje. Taková výjimka by předjímala, že některé obory výzkumu jsou méně důležité než jiné, přičemž veřejné prostředky jsou jim ovšem poskytovány také. Nicméně co se týče partnerských organizací, je třeba si uvědomit, že i ony mají za úkol zaměřit své řízení bezpečnosti na samotnou službu, která je regulována. To znamená, že v případě, že se partnerské organizace podílejí na velké výzkumné infrastruktuře například pouze prostřednictvím jejího financování, nebude v rámci jejich organizace nalezeno podpůrné aktivum, na které by musely zavádět opatření. Stejně tak, pokud jsou vlastníkem pouze malé části samotné infrastruktury a tuto mají oddělenou od své ostatní infrastruktury, která není regulována, zaměřují své řízení bezpečnosti informací pouze na tuto část výzkumné infrastruktury, která představuje aktiva sloužící k poskytování výzkumné činnosti.

		nejširší míře zpřístupňovat uchovávané informace veřejnosti. Povinnost by proto dopadla i na knihovny, muzea a galerie, které byly zřízeny především za účelem poskytování přístupu veřejnosti k informacím, znalostem a kulturnímu bohatství, a výzkum provádí jako doplněk k této činnosti. Jde přitom o organizace, které jsou již nyní z velké části podfinancované. Navíc by tyto organizace musely soutěžit o kvalifikované pracovníky pro tuto oblast s dalšími organizacemi a odčerpávaly by tak již dnes nedostatkové kvalifikované specialisty těm organizacím, které jsou pro provoz státu opravdu kritické. Paradoxně by tak tento požadavek vedl k dalšímu ohrožení státu. Domníváme se, že samo hledisko zapojení organizace do velké infrastruktury by nemělo být jediným ukazatelem toho, že má organizace podléhat vyšším povinnostem dle zákona o kybernetické bezpečnosti. Případný kybernetický útok na výzkum na poli kultury pravděpodobně nebude ohrožením pro chod státu a vynakládání nepřiměřených prostředků na obranu povede pouze ke zbytečnému vynakládání veřejných prostředků a ke ztížení přístupu vědců k informacím, které uchovávají knihovny, muzea a galerie, neboť náklady na zavedení vyššího režimu kybernetické bezpečnosti by zdaleka přesáhly veřejné zdroje získané na účast těchto organizací ve velkých infrastrukturách.	Vaši připomínku nicméně evidujeme, vyhlášky jsou v současné chvíli v rozpracovaných fázích a nejsou součástí tohoto připomínkového řízení, to proběhne na začátku příštího roku. I pokud neuplatníte tuto připomínku znovu, v mezirezortním připomínkovém řízení k vyhláškám se k Vaší připomínce vrátíme. Připomínkové místo s vypořádáním souhlasí.
37. Unie zaměstnavatelských svazů České republiky	D	Zákon o kybernetické bezpečnosti, § 2 odstavec 1a – Primární aktiva a podpůrná aktiva nejsou jen v elektronické podobě. Vyškrtnutí „v elektronické podobě“. <u>Odůvodnění:</u> Ta aktiva, která odpovídají definici tohoto odstavce, se mohou zpracovávat i například jako fyzické dokumenty či objekty (serverovny). Znamenalo by to tedy, že by s takovými materiály či objekty nemuselo být nakládáno dle požadavků zákona. To by ovšem mělo za následek rovněž ohrožení aktiv. Zabezpečení aktiv je nutné nejen v kyberprostoru.	Neakceptováno Regulace dopadá i na dokumenty, které vznikly v elektronické podobě a poté byly např. vytisknuty, obdobně tak serverovny, ve kterých se nachází servery, které elektronickou podobu informací zpracovávají. Regulace cílí na elektronický původ, nikoliv na pouze fyzický svět (pro lepší pochopení si to lze prakticky představit tak, že na papír si něco napíše a nedám to do žádného regulovaného systému, což znamená, že tento dokument pod regulaci KB nespadá).

			Připomínkové místo s vypořádáním souhlasí.
38. Unie zaměstnavatelských svazů České republiky	D	Zákon o kybernetické bezpečnosti, § 5, odstavec d) – chybějící konkrétní právní předpis <u>Odůvodnění:</u> Zmíněný odstavec odkazuje na právní předpis upravující krizové řízení a kritickou infrastrukturu. Konkrétní odkaz na legislativu v poznámce pod čarou ale chybí.	Neakceptováno - nyní § 5 odst. 1 písm. d) Podle čl. 45 odst. 4 Legislativních pravidel vlády může mít normativní odkaz na jiný právní předpis podobu zobecněného názvu umožňujícího jednoznačné určení tohoto jiného právního předpisu. Tento způsob odkazování byl zvolen z toho důvodu, že dojde-li k novelizaci či vydání nového právního předpisu upravujícího krizové řízení a krizovou infrastrukturu, nebude nutné zákon o kybernetické bezpečnosti novelizovat. Připomínkové místo s vypořádáním souhlasí.
39. Unie zaměstnavatelských svazů České republiky	D	Zákon o kybernetické bezpečnosti, § 13, odstavec 1 a) – identifikování všech aktiv v rámci celé organizace, nikoliv jen v rámci regulované služby, nám nepřijde zatěžující. <u>Odůvodnění:</u> Pokud naše organizace poskytuje více služeb a jen jedna z nich spadá do regulovaných služeb, tak by nám dávalo smysl určit pouze ta aktiva, která se dané služby týkají. Návrh zákona ale vyžaduje určit všechna aktiva v celé organizaci a až poté identifikovat ta aktiva, která se dané regulované služby týkají. To ovšem pro některé organizace může být velmi zatěžující a časově náročné. Když opomineme podstatu a smysl identifikování všech aktiv, tedy že by organizace ideálně měla chránit všechna aktiva i mimo regulované služby, tak čemu ale taková evidence je, když odstavec 3 říká, že se aktiva nespádající do rozsahu řízení mohou vyjmout a ale zároveň mít uložen o tom záznam? Taková evidence aktiv bude v rámci kontrol NÚKIBu kontrolována?	Vysvětleno Dle směrnice NIS2 má být rozsah řízení KB stanoven na celou organizaci. Aby NÚKIB neúměrně nezatěžoval povinné subjekty, rozhodl se umožnit vyjmout z rozsahu primární aktiva, která s regulovanou službou nesouvisí. Definice řízení KB říká, že je to činnost směřující k zajištění KB regulované služby, tzn. zajištění regulované služby je hlavním cílem, neznamená to však, že by rozsah nemohl být stanoven na celou organizaci, pokud to povinná osoba vyhodnotí jako vhodné, aby mohla KB regulované služby řádně zajistit. Dotčené ustanovení dále stanoví, že je třeba identifikovat primární aktiva organizace a z nich vybrat ta, která souvisí s regulovanou službou. Až nakonec pak identifikovat podpůrná aktiva související s primárními aktivy potřebnými pro regulovanou službu. Tedy organizace nebude evidovat a určovat veškerá aktiva organizace, ale toliko veškerá primární aktiva - tedy informace a

			služby. Rozsah je pak stanoven pouze na primární aktiva související s regulovanou službou a na ně navázána podpůrná aktiva. Z výše uvedeného vyplývá, že se tak nejedná o identifikaci a evidenci veškerých aktiv organizace, ale pouze veškerých primárních aktiv organizace, což nepovažujeme v kontextu požadavku směrnice NIS2 za administrativně zatěžující, bude se totiž jednat o primární aktiva v množství jednotek a jednoduchého zdůvodnění (např. nesouvisí s regulovanou službou). Pracuje se s typovými aktivy, nikoliv s každou službou/informací jako takovou zvlášť. Jde o základní identifikaci služeb, které organizace poskytuje (za jakým účelem je vytvořena a co jsou její nejzákladnější poskytované služby). Evidence pak slouží k tomu, aby bylo možné ověřit, zda byl rozsah stanoven správně. Ze zkušeností z kontrol vyplývá, že povinné osoby mají rozsah často stanoven nesprávně již na úrovni primárních aktiv, proto bylo ustanovení zpřesněno, aby bylo pro povinné orgány a osoby návodnější. Následné hodnocení aktiv a rizik se vždy provádí ve stanoveném rozsahu, tedy až na omezeném okruhu, jak primárních, tak podpůrných aktiv. K Vámi položené otázce, zda se jedná o součást kontroly, je pak nutno sdělit, že ano, jelikož právě vhodné nastavení rozsahu a vytipování správných primárních aktiv je prvním krokem k funkčnímu nastavení procesu řízení bezpečnosti informací v dané organizaci. Připomínkové místo s vypořádáním souhlasí.
40. Unie zaměstnavatelských svazů České republiky	D	Zákon o kybernetické bezpečnosti, § 15, odstavec 2) – chybějící rozdělení na organizační a technická opatření <u>Odůvodnění:</u> Z jakého důvodu se u nižšího režimu vypustilo rozdělení bezpečnostních opatření na organizační a technická? Sice tento režim	Akceptováno jinak Účelem této rozdílnosti oproti vyhlášce v režimu vyšších povinností je udělat režim nižších povinností přehledný a přiměřeně náročný s ohledem na

		má podstatně méně povinností, ale stále se jedná jak o organizační, tak i technická opatření a rozdělení by mělo být zachováno stejné.	předpokládanou maturitu subjektů. Výčet bezpečnostních opatření včetně jejich obsahu, který je uvedený v prováděcích právních předpisech, nám dává smysl aktuálně na úrovni zákona rozdělovat pouze u režimu vyšších povinností. V režimu nižších povinností s ohledem na zobecnění povinností včetně jejich vzájemných prolnutí nám obdobné rozdělení, jako je nyní v režimu vyšších povinností, nepříjde opodstatněné. Navíc některé ustanovení prováděcích právních předpisů organizační a technické požadavky kombinují. Provedli jsme však korekci u § 15 odst. 2, aby bylo jasné že výčet bezp. opatření pro režim nižších povinností obsahuje povinnosti organizačního i technického charakteru. Připomínkové místo s vypořádáním souhlasí.
41. Unie zaměstnavatelských svazů České republiky	D	Zákon o kybernetické bezpečnosti, § 8 – registrace do Portálu NÚKIB je nutná i pro organizace, které již spadaly pod aktuální ZKB? <u>Odůvodnění:</u> Zajímalo by nás, jestli organizace spadající pod aktuální ZKB budou povinny se znovu registrovat do Portálu NÚKIB? Předpokládali bychom, že seznam takový organizací NÚKIB k dispozici zajisté má, a tak registrace ze strany organizací nebude nutná.	Vysvětleno NÚKIB seznamem současných povinných subjektů samozřejmě disponuje (databáze kontaktních údajů), avšak kritéria, na základě kterých je organizace (resp. poskytovaná služba) zařazena pod regulaci, se dle nové úpravy zcela mění. Zatímco nyní jsou regulovány informační systémy, dle nové úpravy jsou regulovány celé organizace, a to na základě poskytování regulované služby. Každá organizace přitom může poskytovat i více regulovaných služeb. Je tedy nutné, aby identifikaci regulovaných služeb (posouzení kritérií) a jejich následnou registraci, provedly všechny subjekty, tedy včetně těch, na které dopadá současná regulace. Kritériem pro regulovanou službu dle nové právní úpravy tudíž nemůže být pouze ten fakt, že dnes některý její systém pod regulaci spadá, ale organizace musí poskytovat regulovanou službu dle nové právní úpravy. Současná úprava v té

			době již nebude účinná a nebude tak možno na jejím základě posuzovat budoucí stav. Připomínkové místo s vypořádáním souhlasí.
42. Unie zaměstnavatelských svazů České republiky	D	Zákon o kybernetické bezpečnosti, § 8 – nedodržení lhůty pro registraci. <u>Odůvodnění:</u> Pokud organizace neregistruje svou regulovanou službu v požadované lhůtě, jaký bude další postup? NÚKIB podle odstavce 3 provede registraci organizace sám, ale není jasné, jestli bude organizaci o registraci informovat a jaké následky za pozdní registraci hrozí.	Vysvětleno V § 10 návrhu zákona je uvedeno, že na základě registrace bude proveden zápis do evidence regulovaných služeb, o čemž bude subjekt písemně vyrozuměn. K zápisu do evidence dojde vždy, ať už po registraci poskytovatelem regulované služby, nebo po registraci Úřadem. Jedná se o dvě na sebe navazující fáze procesu. Dále je třeba zmínit, že den doručení písemného vyrozumění o zápisu do evidence regulovaných služeb je rozhodným datem, se kterým celý zákon pracuje i na jiných místech a počítá se od něj běh některých lhůt. Právní následky pozdní registrace jsou pak výslovně stanoveny v přestupcích. Jedná se hned o první přestupek v § 60 odst. 1 písm. a). Připomínkové místo s vypořádáním souhlasí.
43. Unie zaměstnavatelských svazů České republiky	D	Zákon o kybernetické bezpečnosti, § 7 – možnost hlášení bezpečnostních incidentů i mimo Portál NÚKIB <u>Odůvodnění:</u> V případě, že nebude možné z nějakého důvodu nahlásit bezpečnostní incident přes Portál NÚKIB, návrh zákona umožňuje podat hlášení přes elektronickou poštu či datovou schránku. Bude k tomuto vydán formulář obsahující požadavky zmíněné ve Vyhlášce o Portálu NÚKIB, aby ten, kdo bude bezpečnostní incident hlásit, nemusel hledat danou vyhlášku a mohl využít jednotný formulář, což povede k rychlému a efektivnímu nahlášení bezpečnostního incidentu?	Vysvětleno Ano, formulář obsahující veškeré požadavky zmíněné ve vyhlášce o Portálu Úřadu bude zveřejněn na webových stránkách Úřadu. Naším záměrem určitě je maximální automatizace a efektivita procesu hlášení a řešení incidentů. Jediným rozdílem bude komunikační kanál, kterým budou relevantní informace sděleny Úřadu. Připomínkové místo s vypořádáním souhlasí.

44. Unie zaměstnavatelských svazů České republiky	D	Zákon o kybernetické bezpečnosti, § 21 – vydání výstrahy prostřednictvím elektronických schránek? <u>Odůvodnění:</u> Vnímáme velice pozitivně, že NÚKIB informuje a přidává výstrahy na své internetové stránky. Obáváme se ale, že není v silách mnohých organizací sledovat aktuality na stránkách NÚKIB a ač se jedná „pouze“ o výstrahu, nebereme je nadarmo. Bylo by proto možné informovat organizace vedené v Portálu NÚKIB elektronickou poštou? Či přihlášení se k alertingu, že nějaká taková aktualizace na stránkách NÚKIBu vyšla, což by mohla využít i veřejnost?	Akceptováno – nyní § 22 Úřad vždy informuje povinné osoby o relevantních vydaných dokumentech právě proto, aby po nich nemusel požadovat neustálou kontrolu aktualit na jeho webových stránkách. I přesto pro navýšení právní jistoty adresátů došlo k příslušnému doplnění tohoto ustanovení o informování prostřednictvím Portálu. Připomínkové místo s vypořádáním souhlasí.
45. Unie zaměstnavatelských svazů České republiky	D	Zákon o kybernetické bezpečnosti, § 22 – jakou formou bude poskytovatel regulované služby informován? <u>Odůvodnění:</u> Odstavec 3 zmíněného paragrafu říká, že NÚKIB bude dotčené poskytovatele regulované služby informovat. Není ale specifikováno, jakou formou.	Akceptováno - nyní § 23 Úřad své povinné osoby vždy informoval o relevantních opatřeních (nyní protiopatřeních) prostřednictvím sdělených kontaktních údajů, pokud se nejednalo o úkony, které mají doručování upraveno odchylně (správním řádem u reaktivních opatření vydaných prostřednictvím rozhodnutí). Ve vztahu k varování se tak bude postupovat obdobným způsobem. Došlo však k doplnění informování prostřednictvím Portálu, který bude platformou nahrazující původní komunikaci prostřednictvím sdělených kontaktních údajů. Připomínkové místo s vypořádáním souhlasí.
46. Unie zaměstnavatelských svazů České republiky	D	Zákon o kybernetické bezpečnosti, § 45 odstavec 1 – jak konkrétně se bude vést evidence penetračních testů? <u>Odůvodnění:</u> NÚKIB bude evidovat dle zmíněného paragrafu velice citlivé údaje. Zajímalo by nás například, jakou formu penetračního testu bude NÚKIB evidovat? Pouze záznam o tom, že u daného poskytovatele regulované služby test proběhl, nebo celou zprávu testu?	Vysvětleno - nyní § 48 odst. 1 V evidenci penetračních testů budou ukládány záznamy o provedených penetračních testech včetně zprávy o průběhu. Na údaje z evidence penetračních testů se vztahuje povinnost mlčenlivosti ze strany zaměstnanců Úřadu podle § 48 odst. 4. V souvislosti se všemi evidencemi vedenými Úřadem dále plošně platí, že informace v nich vedené se neposkytují podle právních předpisů upravujících svobodný přístup k

			informacím, tedy je zajištěna jejich základní ochrana před zveřejněním. Připomínkové místo s vypořádáním souhlasí.
47. Unie zaměstnavatelských svazů České republiky	D	Zákon o kybernetické bezpečnosti, § 58 – kdy bude rozhodnuto o konkrétním přestupku a tím pádem i jeho výši? <u>Odůvodnění:</u> Předpokládáme správně, že přestupek se zjistí kontrolou NÚKIBu? Bude zjištění znamenat, že hned bude organizace penalizována či bude mít nejdříve čas na nápravné opatření do určitého data? Z daného paragrafu tento postup není zcela jasný.	Vysvětleno - nyní § 60 Proces ukládání pokut za přestupky spočívající v porušení povinností stanovených zákonem o kybernetické bezpečnosti se principiálně neliší od procesu ukládání pokut za přestupky podle jiných zákonů. Přestupkem je porušení povinností stanovených zákonem, přičemž ukládání pokuty za přestupek probíhá ve standardním přestupkovém řízení vedeném podle pravidel obsažených zejm. v zákoně č. 255/2012 Sb., o přestupcích. Návrh zákona nestanoví pevnou posloupnost realizace jednotlivých zákonných oprávnění Úřadu (tedy že by nejprve měl provést kontrolu, pak uložit nápravné opatření a teprve poté uložit pokutu za přestupek), takové omezení dozorových orgánů není ani v praxi obvyklé. Naopak je napříč sektory a zákony zaužívanou (a soudní judikaturou aprobovanou) praxí, že přestupky lze stíhat nezávisle na uložených nápravných opatřeních (oba instituty mají rozdílné funkce, zatímco nápravné opatření slouží k nápravě nezákonného stavu, pokuta za přestupek je trestem za porušení povinností). NÚKIB se však dlouhodobě profiluje jako úřad, jehož primárním zájmem je zesouladění skutečného stavu s požadavky zákona, nikoli slepé trestání pochybení povinných osob. Zároveň je v zájmu kybernetické bezpečnosti České republiky, aby byly finanční prostředky investovány do kybernetické bezpečnosti organizace spíše než do placení pokut. Proto již za účinnosti současného zákona obvykle NÚKIB nejprve přistoupí k uložení nápravného opatření a teprve poté,

			co toto nápravné opatření není řádně splněno, ukládá pokutu za přestupek. Zákon však umožňuje uložit rovnou pokutu za přestupek (zejm. tam, kde uložení nápravného opatření již nemá význam), resp. ve skutkově jasných případech uložit pokutu za přestupek i bez provedení kontroly (tzv. od stolu na základě v té době shromážděných informací). Připomínkové místo s vypořádáním souhlasí.
48. Unie zaměstnavatelských svazů České republiky	D	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, § 4 odstavec 6 – zmizení bezpečnostní role garanta aktiv? <u>Odůvodnění:</u> Vyhláška pro nižší režim od prvního návrhu prošla radikální změnou, tedy velkým seškrtáním povinností. Vypadla tak i role garanta aktiv, která dle našeho názoru je klíčová pro řízení bezpečnosti daného aktiva. Vyhláška evidenci aktiv zmiňuje jen v odstavci 6 zmíněného paragrafu, kde odkazuje na zákon, který říká, že u primárních aktiv organizace určí související organizační části. Máme to tedy chápat tak, že daná organizační část převezme roli garanta aktiv? Ovšem roli, která není v této vyhlášce specifikována?	Vysvětleno Záměrem legislativního návrhu a jeho prováděcích právních předpisů pro režim vyšších i nižších povinností je stanovit požadavky přiměřeně, tak aby byly realizovatelné a nekladly na režim nižších povinností nepřiměřené požadavky. Proto je pro režim nižších povinností stanovena pouze povinná bezpečnostní role, kterou lze připodobnit k roli manažera kybernetické bezpečnosti (§ 4 odst. 3). S povinnou rolí ve smyslu garanta aktiv v současném návrhu prováděcího právního předpisu pro režim nižších povinností počítáno není. Připomínkové místo s vypořádáním souhlasí.
49. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	<u>Obecné připomínky</u> Zákon v některých paragrafech odkazuje na „prováděcí právní předpis“, čímž je myšlena odpovídající a nově vznikající vyhláška. Myslíme si, že pro někoho, kdo zákon a nové vyhlášky má načtené je jasné, o který prováděcí právní předpis se jedná. Ovšem pro někoho, kdo si bude zákon číst poprvé, to tak jasné být nemusí. Bylo by proto podle nás lepší, kdyby odkaz na daný předpis byl uveden pod čarou stejně tak, jak jsou uvedeny čísla zákonů. Vyhlášek totiž s tímto zákonem vyjde aktuálně 6 a tento krok by čtenářům pomohl k lepšímu pochopení systému vztahu zákona a odpovídajících vyhlášek. Pokud toto není možné, tak by adresátům pomohl podpůrný materiál NÚKIB	Neakceptováno Odkaz na prováděcí právní předpis je učiněn v souladu s čl. 45 odst. 3 Legislativních pravidel vlády. Rozumíme požadavku na materiál, který by pomohl lepšímu pochopení vztahu mezi zákonem a vyhláškami, příp. i návodnými grafickými materiály pro zákonem stanovené procesy. NÚKIB plánuje takové materiály pro adresáty norem vytvářet, v tuto chvíli již vzniká materiál obsahující návod na identifikaci.

		k pochopení systému vyhlášek. Dále by byl zcela jistě nápomocný materiál s grafickým znázorněním, jak se má adresát normy identifikovat, kam jak a kam zaregistrovat atp.	Připomínkové místo s vypořádáním souhlasí.
50. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Uplatňujeme připomínky k části návrhu zákona, která zapracovává mechanismus prověřování bezpečnosti dodavatelů do strategicky významné infrastruktury. Zásadní je nový regulační nástroj úřadu, kdy úřad má právo autoritativně zasáhnout do svobody podnikání a vlastnického práva soukromých subjektů a omezit volnou hospodářskou soutěž tím, že rozhodne o omezení nebo vyloučení konkrétních dodavatelů z plnění tzv. bezpečnostně významných dodávek poskytovatelům strategicky významných služeb, a to jak v rozsahu již realizovaných dodávek, tak v rozsahu všech budoucích dodávek. Proto by tento nástroj a proces, jež vede k vydání správního aktu (opatření obecné povahy) o omezení nebo vyloučení dodavatele z bezpečnostně relevantních dodávek poskytovatelům strategicky významné služby, měl dle našeho názoru splňovat nejpřísnější nároky na transparentnost, předvídatelnost a proporcionalitu právní úpravy tak, aby nebyla zasažena právní jistota mechanismem dotčených subjektů. Z tohoto pohledu uplatňujeme následující připomínky: Přesah problematiky mechanismu nad rámec kybernetické bezpečnosti. Samotná důvodová zpráva k návrhu zákona uvádí, že: „<i>mechanismus prověřování bezpečnosti dodavatelského řetězce, který je součástí návrhu zákona, je pak odrazem národních požadavků na zvýšení bezpečnosti a <u>snížení rizik plynoucích z netechnických aspektů zajišťování kybernetické bezpečnosti</u> a jako takový nemá doposud odraz v platné legislativě. V jistých aspektech je zčásti podobný úpravě zákona č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic).</i>“ Dále při vydání opatření obecné povahy, kterým úřad omezí nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky, úřad bude vyhodnocovat kritéria rizikivosti dodavatele určená vyhláškou, <u>která jsou výlučně netechnické povahy</u> (politické	Neakceptováno NÚKIB nemá a ani nemůže mít za cíl určovat hospodářské ambice České republiky či její zahraniční politiku. Zmíněná kritéria posuzování rizikivosti dodavatele v rámci vyhlášky sloužila primárně jako vodítko/metodika k určení hrozby. Nutno dodat, že vyhláška o kritériích rizikivosti dodavatele byla, rovněž z důvodu obdobných připomínek cílících na smysl kritérií, vyřazena. Kritériem tudíž zůstává bezpečnost ČR a její vnitřní či veřejný pořádek. V rámci procesu posuzování rizikivosti dodavatele je však stále potřeba vzít v potaz také aspekty související s tzv. netechnickými otázkami, zejména ty související s třetí zemí, která může mít na dodavatele bezpečnostně významné dodávky, a tudíž na kybernetickou bezpečnost České republiky, vliv. Smyslem mechanismu není vytvářet zátěž pro jednotlivé segmenty, nýbrž tuto zátěž mitigovat skrz instrumenty popsané zákonem a zamezit přístupu rizikových dodavatelů do kritických částí infrastruktury. Cílem omezení rizikových dodavatelů je tak kybernetická bezpečnost, která svou povahou úzce souvisí s dalšími bezpečnostními otázkami z tzv. fyzického světa. Co se týče zapojení Ministerstva průmyslu a obchodu do procesu, tak to je dle § 29 odst. 1 navrhovaného zákona zapojeno přímo do procesu posuzování rizikivosti dodavatele. Navíc opatření obecné povahy o případném omezení či zákazu dodavatele NÚKIB rovněž projedná mimo jiné s ministerstvem průmyslu a obchodu (§ 30 odst. 2), aby byly získány všechny

		charakteristiky země původu dodavatele, právní prostředí země původu dodavatele a „bezúhonnost“ dodavatele) a nijak nesouvisí se zajišťováním kybernetické bezpečnosti. V této souvislosti je tedy otázkou, který správní úřad by měl prověřování bezpečnosti dodavatelského řetězce provádět a mít pravomoc opatření obecné povahy vydat. Dle názoru SZPČR se prověřování a omezování nebo zákazu dodavatelů předně dotýká hospodářské soutěže a ekonomiky. Jejich omezení nebo vyloučení bude mít dopad na rozvoj ICT infrastruktury a na výši nákladů s tím spojených a je záležitostí státní průmyslové a obchodní politiky, kde ústředním orgánem státní správy je podle § 13 odst. 1 písm. a) zákona č. 2/1969 Sb., ve znění pozdějších předpisů, Ministerstvo průmyslu a obchodu České republiky (dále jen „ministerstvo“). Ministerstvo je ústředním správním orgánem rovněž pro zahraničně ekonomickou politiku. Dle § 13 odst. 3 mimo jiné koordinuje zahraničně obchodní politiku České republiky ve vztahu k jednotlivým státům, zabezpečuje sjednávání dvoustranných a mnohostranných obchodních a ekonomických dohod včetně komoditních dohod, aj. Ministerstvo je tedy právními předpisy určeno k řešení veškerých zahraničně-obchodních záležitostí. Současně dle platné právní úpravy patří do gesce ministerstva prověřování zahraničních investic, ke kterému je zmocněno na základě zák. č. 34/2021 Sb., a pojí se s prověřováním zahraničních investic z důvodu ochrany bezpečnosti České republiky a vnitřního a veřejného pořádku. Posuzování je tak založeno na obdobných kritériích rizikovosti jako navrhuje teze prováděcí vyhlášky k návrhu zákona o kybernetické bezpečnosti. SZPČR s ohledem na výše uvedené navrhuje, aby prověřování bezpečnosti dodavatelského řetězce a pravomoc vydávat opatření obecné povahy náležela ministerstvu s tím, že role a pravomoci úřadu by měla být obdobné jako jsou v procesu prověřování přímých zahraničních investic.	relevantní pohledy a perspektivy pro proporcionální stanovení povinností daným opatřením obecné povahy. V souvislosti s politickou odpovědností je nutno zmínit, že úkol řešit bezpečnost dodavatelského řetězce byl NÚKIB dán Bezpečnostní radou státu, přičemž se NÚKIB za svou činnost zodpovídá vládě, která jej úkoluje. Připomínkové místo s vypořádáním souhlasí.
51. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Vágnost a arbitrárnost kritérií rizikovosti dodavatele Celé hodnocení rizikovosti dodavatele stojí na naplnění kritérií rizikovosti, které určuje sám úřad vyhláškou (a jejich určení je tedy	Neakceptováno Kritéria cílila na strategická, nikoliv technická, kritéria záměrně. NÚKIB pevně věří, že je v schopnostech

	zcela v pravomoci úřadu) a která spočívají v posuzování politických charakteristik země původu dodavatele, právního prostředí země původu dodavatele a posuzování integrity osoby dodavatele, tedy výlučně netechnických kritériích. S výjimkou kritérií pro posuzování integrity osoby dodavatele jsou tato kritéria podle názoru SZPČR zcela neměřitelná, arbitrární a jejich použití lehce zneužitelné. Forma a metodika vyhodnocení naplnění kritérií rovněž zcela chybí a lze si stěží představit, jak bude například posuzováno naplnění kritéria – existence právních předpisů v zemi mající vliv na dodavatele, které ukládají povinnost spolupráce s orgány veřejné moci, jež vykonávají činnost odpovídající činnosti zpravodajských služeb, a to bez nezávislého soudního dohledu či přezkumu. Dále není zřejmé, proč úřad v rámci zajišťování kybernetické bezpečnosti zcela rezignuje na zkoumání a vyhodnocování naplnění technických a jiných kritérií bezpečnosti produktů a služeb dodavatele jako jsou certifikace, smluvní závazky, audity kybernetické bezpečnosti, apod., které mohou sehrávat v hodnocení kybernetické bezpečnosti zcela zásadní roli. SZPČR navrhuje zvýšení transparentnosti procesu hodnocení kritérií a zavedení technických kritérií uplatňovaných u konkrétního dodavatele, resp. poskytovatele strategicky významné služby mezi kritéria hodnocení rizikivosti dodavatele.	státu a jeho organizačních složek, v tomto případě též NÚKIB, posuzovat rizika na strategické rovině, tedy na základě strategických kritérií, ke kterým jednotlivé orgány státu disponují relevantními informacemi. Obdobně se tak děje i v jiných státech, včetně Spojených států amerických, Německa, Dánska či Estonska. Strategická kritéria jsou pro posouzení důvěryhodnosti/rizikivosti dodavatele klíčová. Posuzování technických či obchodně-ekonomických kritérií by pak mělo být primárně na jednotlivých povinných osobách, které v těchto otázkách disponují širokými znalostmi, jež dokáží aplikovat na své hospodářské potřeby. Stát, potažmo NÚKIB, by měl zasáhnout až v případě posuzování rizikivosti dodavatele na strategické úrovni, kdy stát disponuje informacemi, ke kterým nemohou mít povinné subjekty přístup. To znamená, že aspekty typu „technická a jiná kritéria bezpečnosti produktů a služeb dodavatele jako jsou certifikace, smluvní závazky, audity kybernetické bezpečnosti, apod.“ představují právě zmíněná technická kritéria, která jsou dobře posouditelná ze strany povinných osob a k jejichž vyhodnocení není potřeba stát. Nutno však dodat, že zmíněná kritéria posuzování rizikivosti dodavatele v rámci vyhlášky sloužila primárně jako vodítko/metodika k určení hrozby, přičemž vyhláška o kritériích rizikivosti dodavatele byla, mimo jiné důvodů uvedených v připomínce, vyřazena. Kritériem tudíž zůstává bezpečnost ČR a její vnitřní či veřejný pořádek. Připomínkové místo s vypořádáním souhlasí.

52. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Absence opravného prostředku proti opatření obecné povahy Výstupem procesu prověřování bezpečnosti dodavatelských řetězců má být opatření obecné povahy (OOP) vydané úřadem. V případě OOP neexistuje možnost podání řádného opravného prostředku. Proti omezení či zákazu obchodních vztahů stanovených OOP je tak není možnost bránit se opravným prostředkem (proti OOP nelze podat odvolání ani rozklad), což dále přispívá k netransparentnosti a možné arbitrárnosti rozhodování úřadu.	Vysvětleno. Proti opatření obecné povahy lze podat návrh na zahájení přezkumného řízení nebo podat správní žalobu na jeho zrušení. V procesu vydávání OOP mohou oprávněné subjekty také uplatňovat proti jeho návrhu připomínky. Proti tomuto institutu sice tedy není možné podávat řádné opravné prostředky, ale je možné se proti němu bránit jinými způsoby. Závěry uvedené v OOP také musí být řádně a přezkoumatelně odůvodněny. Pokud by plnění opatření obecné povahy mohlo podstatným způsobem ohrožovat poskytování strategicky významné služby, může také být udělena výjimka z podmínek nebo zákazu jím stanovených. Připomínkové místo s vypořádáním souhlasí.
53. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Narušení podnikatelského prostředí V důsledku připravované legislativy by také mohlo být narušeno legitimní očekávání podnikatelů, protože mnoho parametrů mechanismu může být ze strany úřadu kdykoli změněno (vzhledem k tomu, že úřad přijímá vyhlášky tyto oblasti blíže upravující) a rovněž může dojít k zákazu či významnému omezení jeho dodavatelů. Takto rozsáhlá rozhodovací pravomoc poskytuje velký prostor pro libovůli při rozhodování úřadu a představuje tak rozsáhlé riziko. Konečným důsledkem mechanismu tak může být úplné dlouhodobé zastrašení podnikatelských subjektů od spolupráce s dodavateli z vybraných zemí. Je zapotřebí si také uvědomit, že při takto obecně nastavených kritériích může dojít k tomu, že „rizikovou“ zemí se v okamžiku změny politické reprezentace v ČR náhle stane stát, u nějž by to navrhovaná právní regulace v tuto chvíli absolutně nepředpokládala.	Vysvětleno Rozumíme, že nová právní úprava může vyvolávat v některých povinných subjektech obavy, nicméně odvětví, kterých se mechanismus bude týkat, jsou stanovena zákonem a NÚKIB stejně jako všechny ostatní správní orgány postupuje tak, aby naplňoval principy dobré správy. Případnou libovůli správních úřadů lze napravit správní žalobou podanou k nezávislému soudu. Připomínkové místo s vypořádáním souhlasí.
54. Konfederace zaměstnavatelských a	D	K § 30 zákona o kybernetické bezpečnosti Doporučujeme zvážit možné dopady na <i>poskytovatele strategicky významných služeb</i> v situaci, kdy klíčové informační systémy jsou ve	Vysvětleno

podnikatelských svazů ČR		„vendor locku“, a výměna dodavatele není reálná v termínech deklarovaných v ustanovení § 30 navrhované úpravy. Vzhledem k tomu, že dodavatel nemá žádnou povinnost uzavírat smlouvu, kterou uzavřít nechce, tak navrhovaná úprava bude bez doplnění stavět zadavatele veřejných zakázek před dilema, zda nedodržet dotčené právní předpisy, nebo narušit provoz svých informačních systémů. Mělo by proto dojít k lepšímu vymezení priorit ze strany předkladatele návrhu.	Prioritou NÚKIB je zajistit bezpečnost dodavatelského řetězce. Lhůty k plnění povinností stanovených opatřením obecné povahy budou dostatečně dlouhé (mimo jiné může být při jejich stanovení zvážen i vendor lock-in) na to, aby se poskytovatelé strategicky významných služeb vypořádali i s vendor lock-in. V případě, kdy to nebude možné, mohou poskytovatelé strategicky významné služby požádat o výjimku dle § 32. Připomínkové místo s vypořádáním souhlasí.
55. Konfederace zaměstnavatelských a podnikatelských svazů ČR	D	K § 33 zákona o kybernetické bezpečnosti Doporučujeme se více zaměřit na možné (finanční) dopady na <i>poskytovatele strategicky významných služeb</i>, a to v souvislosti s možnou výpovědí závazku dodavateli podle § 33 navrhované úpravy. Z důvodů uvedených v § 30 navrhované úpravy tak sice lze vypovědět závazek ze smlouvy na veřejnou zakázku, avšak není výslovně vyloučena eliminace případných sankcí ze strany dodavatele.	Vysvětleno Vypovězení smluvního závazku na základě zákona by mělo být vždy bezúplatné; případná sjednaná sankce za výpověď smlouvy by měla mít buď charakter odstupného dle § 1992 občanského zákoníku (které je nicméně spojeno nikoliv s ukončením závazku ex nunc, ale ex tunc, případně výpověď smluvní, která by tak byla alternativní možností k ukončení závazku ze zákona. Na základě jiných připomínek bylo nicméně ustanovení upraveno a právo na ukončení dlouhodobých závazků tak bude přiznáno i subjektům, které nejsou v postavení zadavatele podle zákona o zadávání veřejných zakázek. Připomínkové místo s vypořádáním souhlasí.
56. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	K návrhu prováděcí vyhlášky o regulovaných službách, k bodu 19.1. Přílohy Kritéria pro identifikaci regulované služby Navrhujeme vypustit: „, nebo <i>b) většina prováděných výzkumných projektů je financována z více než 50 % z veřejných zdrojů.“</i>	Akceptováno jinak Došlo k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace,

	Nebo alternativně doplnit za slova „nebo jiná výzkumná organizace“: <i>„, s výjimkou výzkumné organizace zřizované nebo založené ministerstvem kultury, nebo výzkumné organizace zřízené nebo založené jiným zřizovatelem či zakladatelem, která je knihovnou, muzeem nebo galerií,“</i> <u>Odůvodnění:</u> Podle navrhovaného znění by regulovanou službou v režimu vyšších povinností byla každá výzkumná organizace zapsaná v seznamu vedeném podle § 33a zákona č. 130/2002 Sb., o podpoře výzkumu a vývoje z veřejných prostředků a o změně některých souvisejících zákonů (zákon o podpoře výzkumu a vývoje), a to pokud je většina prováděných výzkumných projektů financována z více než 50 % z veřejných zdrojů. V návrhu není nijak zohledněna celková výše veřejných zdrojů, které organizace vynakládá na výzkum. Povinnost by proto dopadla i na knihovny, muzea a galerie, které byly zřízeny především za účelem poskytování přístupu veřejnosti k informacím, znalostem a kulturnímu bohatství, a výzkum provádí jako doplněk k této činnosti. Jde přitom o organizace, které jsou již nyní z velké části podfinancované. Navíc by tyto organizace musely soutěžit o kvalifikované pracovníky pro tuto oblast s dalšími organizacemi a odčerpávaly by tak již dnes nedostatkové kvalifikované specialisty těm organizacím, které jsou pro provoz státu opravdu kritické. Paradoxně by tak tento požadavek vedl k dalšímu ohrožení státu. Domníváme se, že hledisko financování z veřejných zdrojů by samo o sobě nemělo být kritériem pro určení, že má organizace podléhat povinností dle zákona o kybernetické bezpečnosti. Případný kybernetický útok na výzkum na poli kultury pravděpodobně nebude ohrožením pro chod státu a vynakládání nepřiměřených prostředků na obranu povede pouze ke zbytečnému vynakládání veřejných prostředků, nebo naopak k ukončení drobných výzkumů, neboť	které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji. Zároveň se však domníváme, že není koncepční a účelné zavádět v rámci regulace výzkumu výjimky pouze na základě zaměření daného vývoje. Taková výjimka by předjímal, že některé obory výzkumu jsou méně důležité než jiné, přičemž veřejné prostředky jsou jim ovšem poskytovány také. Nicméně co se týče partnerských organizací, je třeba si uvědomit, že i ony mají za úkol zaměřit své řízení bezpečnosti na samotnou službu, která je regulována. To znamená, že v případě, že se partnerské organizace podílejí na velké výzkumné infrastruktuře například pouze prostřednictvím jejího financování, nebude v rámci jejich organizace nalezeno podpůrné aktivum, na které by musely zavádět opatření. Stejně tak, pokud jsou vlastníkem pouze malé části samotné infrastruktury a tuto mají oddělenou od své ostatní infrastruktury, která není regulována, zaměřují své řízení bezpečnosti informací pouze na tuto část výzkumné infrastruktury, která představuje aktiva sloužící k poskytování výzkumné činnosti. Vaši připomínku nicméně evidujeme, vyhlášky jsou v současné chvíli v rozpracovaných fázích a nejsou součástí tohoto připomínkového řízení, to proběhne na začátku příštího roku. I pokud neuplatníte tuto připomínku znovu, v mezirezortním připomínkovém řízení k vyhláškám se k Vaší připomínce vrátíme. Připomínkové místo s vypořádáním souhlasí.

		náklady na zavedení vyššího režimu kybernetické bezpečnosti by zdaleka přesáhly veřejné zdroje získané na výzkum.	
57. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	K návrhu prováděcí vyhlášky o regulovaných službách, k bodu 19.2. Přílohy Kritéria pro identifikaci regulované služby Navrhujeme za slova <i>„Hostitelská nebo partnerská instituce velké výzkumné infrastruktury“</i> doplnit: <i>„, s výjimkou instituce zřizované nebo založené ministerstvem kultury, nebo instituce zřízené nebo založené jiným zřizovatelem, která je knihovnou, muzeem nebo galerií,“</i> nebo alternativně doplnit: <i>„, s výjimkou hostitelské nebo partnerské instituce velké výzkumné infrastruktury v oblasti sociálních a humanitních věd,“</i> <u>Odůvodnění:</u> Podle navrhovaného znění by regulovanou službou v režimu vyšších povinností byla každá výzkumná organizace, zapojená do některé z velkých infrastruktur. To je pochopitelné například u biomedicínského výzkumu, některé výzkumné infrastruktury jsou však zaměřeny na jazykovědu, digitální humanitní vědy nebo archeologii. Přehled všech infrastruktur v této oblasti je zde: https://www.vyzkumne-infrastruktury.cz/humanitni-vedy/. V návrhu není nijak zohledněna skutečnost, že výzkum v oblasti sociálních a humanitních věd je jednoznačně postaven na otevřeném publikování výsledků, stejně tak úkolem paměťových institucí je v co nejširší míře zpřístupňovat uchovávané informace veřejnosti. Povinnost by proto dopadla i na knihovny, muzea a galerie, které byly zřízeny především za účelem poskytování přístupu veřejnosti k informacím, znalostem a kulturnímu bohatství, a výzkum provádí jako	Akceptováno jinak Došlo k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji. Zároveň se však domníváme, že není koncepční a účelné zavádět v rámci regulace výzkumu výjimky pouze na základě zaměření daného vývoje. Taková výjimka by předjímal, že některé obory výzkumu jsou méně důležité než jiné, přičemž veřejné prostředky jsou jim ovšem poskytovány také. Nicméně co se týče partnerských organizací, je třeba si uvědomit, že i ony mají za úkol zaměřit své řízení bezpečnosti na samotnou službu, která je regulována. To znamená, že v případě, že se partnerské organizace podílejí na velké výzkumné infrastruktuře například pouze prostřednictvím jejího financování, nebude v rámci jejich organizace nalezeno podpůrné aktivum, na které by musely zavádět opatření. Stejně tak, pokud jsou vlastníkem pouze malé části samotné infrastruktury a tuto mají oddělenou od své ostatní infrastruktury, která není regulována, zaměřují své řízení bezpečnosti informací pouze na tuto část výzkumné infrastruktury, která představuje aktiva sloužící k poskytování výzkumné činnosti. Vaši připomínku nicméně evidujeme, vyhlášky jsou v současné chvíli v rozpracovaných fázích a nejsou součástí tohoto připomínkového řízení, to proběhne na začátku příštího roku. I pokud neuplatníte tuto

		doplněk k této činnosti. Jde přitom o organizace, které jsou již nyní z velké části podfinancované. Navíc by tyto organizace musely soutěžit o kvalifikované pracovníky pro tuto oblast s dalšími organizacemi a odčerpávaly by tak již dnes nedostatkově kvalifikované specialisty těm organizacím, které jsou pro provoz státu opravdu kritické. Paradoxně by tak tento požadavek vedl k dalšímu ohrožení státu. Domníváme se, že samo hledisko zapojení organizace do velké infrastruktury by nemělo být jediným ukazatelem toho, že má organizace podléhat vyšším povinnostem dle zákona o kybernetické bezpečnosti. Případný kybernetický útok na výzkum na poli kultury pravděpodobně nebude ohrožením pro chod státu a vynakládání nepřiměřených prostředků na obranu povede pouze ke zbytečnému vynakládání veřejných prostředků a ke ztížení přístupu vědců k informacím, které uchovávají knihovny, muzea a galerie, neboť náklady na zavedení vyššího režimu kybernetické bezpečnosti by zdaleka přesáhly veřejné zdroje získané na účast těchto organizací ve velkých infrastrukturách.	připomínku znovu, v mezirezortním připomínkovém řízení k vyhláškám se k Vaší připomínce vrátíme. Připomínkové místo s vypořádáním souhlasí.
58. Konfederace zaměstnavatelských a podnikatelských svazů ČR	D	Zákon o kybernetické bezpečnosti, § 2 odstavec 1a – Primární aktiva a podpůrná aktiva nejsou jen v elektronické podobě. Vyškrtnutí „v elektronické podobě“. <u>Odůvodnění:</u> Ta aktiva, která odpovídají definici tohoto odstavce, se mohou zpracovávat i například jako fyzické dokumenty či objekty (serverovny). Znamenalo by to tedy, že by s takovými materiály či objekty nemuselo být nakládáno dle požadavků zákona. To by ovšem mělo za následek rovněž ohrožení aktiv. Zabezpečení aktiv je nutné nejen v kyberprostoru.	Vysvětleno Regulace dopadá i na dokumenty, které vznikly v elektronické podobě a poté byly např. vytisknuty, obdobně tak serverovny, ve kterých se nachází servery, které elektronickou podobu informací zpracovávají. Regulace cílí na elektronický původ, nikoliv na pouze fyzický svět (pro lepší pochopení si to lze prakticky představit tak, že na papír si něco napíše a nedám to do žádného regulovaného systému, což znamená, že tento dokument pod regulaci KB nespadá). Připomínkové místo s vypořádáním souhlasí.
59. Konfederace zaměstnavatelských a podnikatelských svazů ČR	D	Zákon o kybernetické bezpečnosti, § 5, odstavec d) – chybějící konkrétní právní předpis	Neakceptováno Podle čl. 45 odst. 4 Legislativních pravidel vlády může mít normativní odkaz na jiný právní předpis podobu

		<u>Odůvodnění:</u> Zmíněný odstavec odkazuje na právní předpis upravující krizové řízení a kritickou infrastrukturu. Konkrétní odkaz na legislativu v poznámce pod čarou ale chybí.	zobecněného názvu umožňujícího jednoznačné určení tohoto jiného právního předpisu. Tento způsob odkazování byl zvolen z toho důvodu, že dojde-li k novelizaci či vydání nového právního předpisu upravujícího krizové řízení a krizovou infrastrukturu, nebude nutné zákon o kybernetické bezpečnosti novelizovat. Připomínkové místo s vypořádáním souhlasí.
60. Konfederace zaměstnavatelských a podnikatelských svazů ČR	D	Zákon o kybernetické bezpečnosti, § 13, odstavec 1 a) – identifikování všech aktiv v rámci celé organizace, nikoliv jen v rámci regulované služby, nám nepřijde zatěžující. <u>Odůvodnění:</u> Pokud naše organizace poskytuje více služeb a jen jedna z nich spadá do regulovaných služeb, tak by nám dávalo smysl určit pouze ta aktiva, která se dané služby týkají. Návrh zákona ale vyžaduje určit všechna aktiva v celé organizaci a až poté identifikovat ta aktiva, která se dané regulované služby týkají. To ovšem pro některé organizace může být velmi zatěžující a časově náročné. Když opomineme podstatu a smysl identifikování všech aktiv, tedy že by organizace ideálně měla chránit všechna aktiva i mimo regulované služby, tak čemu ale taková evidence je, když odstavec 3 říká, že se aktiva nespádající do rozsahu řízení mohou vyjmout a ale zároveň mít uložen o tom záznam? Taková evidence aktiv bude v rámci kontrol NÚKIBu kontrolována?	Vysvětleno Dle směrnice NIS2 má být rozsah řízení KB stanoven na celou organizaci. Aby NÚKIB neúměrně nezatěžoval povinné subjekty, rozhodl se umožnit vyjmout z rozsahu primární aktiva, která s regulovanou službou nesouvisí. Definice řízení KB říká, že je to činnost směřující k zajištění KB regulované služby, tzn. zajištění regulované služby je hlavním cílem, neznamená to však, že by rozsah nemohl být stanoven na celou organizaci, pokud to povinná osoba vyhodnotí jako vhodné, aby mohla KB regulované služby řádně zajistit. Dotčené ustanovení dále stanoví, že je třeba identifikovat primární aktiva organizace a z nich vybrat ta, která souvisí s regulovanou službou. Až nakonec pak identifikovat podpůrná aktiva související s primárními aktivy potřebnými pro regulovanou službu. Tedy organizace nebude evidovat a určovat veškerá aktiva organizace, ale toliko veškerá primární aktiva - tedy informace a služby. Rozsah je pak stanoven pouze na primární aktiva související s regulovanou službou a na ně navázána podpůrná aktiva. Z výše uvedeného vyplývá, že se tak nejedná o identifikaci a evidenci veškerých aktiv organizace, ale pouze veškerých primárních aktiv organizace, což nepovažujeme v kontextu

			požadavku směrnice NIS2 za administrativně zatěžující, bude se totiž jednat o primární aktiva v množství jednotek a jednoduchého zdůvodnění (např. nesouvisí s regulovanou službou). Pracuje se s typovými aktivy, nikoliv s každou službou/informací jako takovou zvlášť. Jde o základní identifikaci služeb, které organizace poskytuje (za jakým účelem je vytvořena a co jsou její nejzákladnější poskytované služby). Evidence pak slouží k tomu, aby bylo možné ověřit, zda byl rozsah stanoven správně. Ze zkušeností z kontrol vyplývá, že povinné osoby mají rozsah často stanoven nesprávně již na úrovni primárních aktiv, proto bylo ustanovení zpřesněno, aby bylo pro povinné orgány a osoby návodnější. Následné hodnocení aktiv a rizik se vždy provádí ve stanoveném rozsahu, tedy až na omezeném okruhu, jak primárních, tak podpůrných aktiv. K Vámi položené otázce, zda se jedná o součást kontroly, je pak nutno sdělit, že ano, jelikož právě vhodné nastavení rozsahu a vytipování správných primárních aktiv je prvním krokem k funkčnímu nastavení procesu řízení bezpečnosti informací v dané organizaci. Připomínkové místo s vypořádáním souhlasí.
61. Konfederace zaměstnavatelských a podnikatelských svazů ČR	D	Zákon o kybernetické bezpečnosti, § 15, odstavec 2) – chybějící rozdělení na organizační a technická opatření <u>Odůvodnění:</u> Z jakého důvodu se u nižšího režimu vypustilo rozdělení bezpečnostních opatření na organizační a technická? Sice tento režim má podstatně méně povinností, ale stále se jedná jak o organizační, tak i technická opatření a rozdělení by mělo být zachováno stejné.	Akceptováno jinak Účelem této rozdílnosti oproti vyhlášce v režimu vyšších povinností je udělat režim nižších povinností přehledný a přiměřeně náročný s ohledem na předpokládanou maturitu subjektů. Výčet bezpečnostních opatření včetně jejich obsahu, který je uvedený v prováděcích právních předpisech, nám dává smysl aktuálně na úrovni zákona rozdělovat pouze u režimu vyšších povinností. V režimu nižších povinností s ohledem na zjednodušení povinností včetně

			jejich vzájemných prolnutí nám obdobné rozdělení, jako je nyní v režimu vyšších povinností, nepřijde opodstatněné. Navíc některé ustanovení prováděcích právních předpisů organizační a technické požadavky kombinují. Provedli jsme však korekci u § 15 odst. 2, aby bylo jasné že výčet bezp. opatření pro režim nižších povinností obsahuje povinnosti organizačního i technického charakteru. Připomínkové místo s vypořádáním souhlasí.
62. Konfederace zaměstnavatelských a podnikatelských svazů ČR	D	Zákon o kybernetické bezpečnosti, § 8 – registrace do Portálu NÚKIB je nutná i pro organizace, které již spadaly pod aktuální ZKB? <u>Odůvodnění:</u> Zajímalo by nás, jestli organizace spadající pod aktuální ZKB budou povinny se znovu registrovat do Portálu NÚKIB? Předpokládali bychom, že seznam takový organizací NÚKIB k dispozici zajisté má, a tak registrace ze strany organizací nebude nutná.	Vysvětleno NÚKIB seznamem současných povinných subjektů samozřejmě disponuje (databáze kontaktních údajů), avšak kritéria, na základě kterých je organizace (resp. poskytovaná služba) zařazena pod regulaci, se dle nové úpravy zcela mění. Zatímco nyní jsou regulovány informační systémy, dle nové úpravy jsou regulovány celé organizace, a to na základě poskytování regulované služby. Každá organizace přitom může poskytovat i více regulovaných služeb. Je tedy nutné, aby identifikaci regulovaných služeb (posouzení kritérií) a jejich následnou registraci, provedly všechny subjekty, tedy včetně těch, na které dopadá současná regulace. Kritériem pro regulovanou službu dle nové právní úpravy tudíž nemůže být pouze ten fakt, že dnes některý její systém pod regulaci spadá, ale organizace musí poskytovat regulovanou službu dle nové právní úpravy. Současná úprava v té době již nebude účinná a nebude tak možno na jejím základě posuzovat budoucí stav. Připomínkové místo s vypořádáním souhlasí.
63. Konfederace zaměstnavatelských a	D	Zákon o kybernetické bezpečnosti, § 8 – nedodržení lhůty pro registraci.	Vysvětleno

podnikatelských svazů ČR		<u>Odůvodnění:</u> Pokud organizace neregistruje svou regulovanou službu v požadované lhůtě, jaký bude další postup? NÚKIB podle odstavce 3 provede registraci organizace sám, ale není jasné, jestli bude organizaci o registraci informovat a jaké následky za pozdní registraci hrozí.	V § 10 návrhu zákona je uvedeno, že na základě registrace bude proveden zápis do evidence regulovaných služeb, o čemž bude subjekt písemně vyrozuměn. K zápisu do evidence dojde vždy, ať už po registraci poskytovatelem regulované služby, nebo po registraci Úřadem. Jedná se o dvě na sebe navazující fáze procesu. Dále je třeba zmínit, že den doručení písemného vyrozumění o zápisu do evidence regulovaných služeb je rozhodným datem, se kterým celý zákon pracuje i na jiných místech a počítá se od něj běh některých lhůt. Právní následky pozdní registrace jsou pak výslovně stanoveny v přestupcích. Jedná se hned o první přestupek v § 60 odst. 1 písm. a). Připomínkové místo s vypořádáním souhlasí.
64. Konfederace zaměstnavatelských a podnikatelských svazů ČR	D	Zákon o kybernetické bezpečnosti, § 7 – možnost hlášení bezpečnostních incidentů i mimo Portál NÚKIB <u>Odůvodnění:</u> V případě, že nebude možné z nějakého důvodu nahlásit bezpečnostní incident přes Portál NÚKIB, návrh zákona umožňuje podat hlášení přes elektronickou poštu či datovou schránku. Bude k tomuto vydán formulář obsahující požadavky zmíněné ve Vyhlášce o Portálu NÚKIB, aby ten, kdo bude bezpečnostní incident hlásit, nemusel hledat danou vyhlášku a mohl využít jednotný formulář, což povede k rychlému a efektivnímu nahlášení bezpečnostního incidentu?	Vysvětleno Ano, formulář obsahující veškeré požadavky zmíněné ve vyhlášce o Portálu Úřadu bude zveřejněn na webových stránkách Úřadu. Naším záměrem určitě je maximální automatizace a efektivita procesu hlášení a řešení incidentů. Jediným rozdílem bude komunikační kanál, kterým budou relevantní informace sděleny Úřadu. Připomínkové místo s vypořádáním souhlasí.
65. Konfederace zaměstnavatelských a podnikatelských svazů ČR	D	Zákon o kybernetické bezpečnosti, § 21 – vydání výstrahy prostřednictvím elektronických schránek? <u>Odůvodnění:</u> Vnímáme velice pozitivně, že NÚKIB informuje a přidává výstrahy na své internetové stránky. Obáváme se ale, že není v silách mnohých organizací sledovat aktuality na stránkách NÚKIB a ač se jedná „pouze“ o výstrahu, nebereme je nadarmo. Bylo by proto možné informovat organizace vedené v Portálu NÚKIB elektronickou	Akceptováno – nyní § 22 Úřad vždy informuje povinné osoby o relevantních vydaných dokumentech právě proto, aby po nich nemusel požadovat neustálou kontrolu aktualit na jeho webových stránkách. I přesto pro navýšení právní jistoty adresátů došlo k příslušnému doplnění tohoto ustanovení o informování prostřednictvím Portálu.

		poštou? Či přihlášení se k alertingu, že nějaká taková aktualizace na stránkách NÚKIBu vyšla, což by mohla využít i veřejnost?	Připomínkové místo s vypořádáním souhlasí.
66. Konfederace zaměstnavatelských a podnikatelských svazů ČR	D	Zákon o kybernetické bezpečnosti, § 22 – jakou formou bude poskytovatel regulované služby informován? <u>Odůvodnění:</u> Odstavec 3 zmíněného paragrafu říká, že NÚKIB bude dotčené poskytovatele regulované služby informovat. Není ale specifikováno, jakou formou.	Akceptováno - nyní § 23 Úřad své povinné osoby vždy informoval o relevantních opatřeních (nyní protiopatřeních) prostřednictvím sdělených kontaktních údajů, pokud se nejednalo o úkony, které mají doručování upraveno odchylně (správním řádem u reaktivních opatření vydaných prostřednictvím rozhodnutí). Ve vztahu k varování se tak bude postupovat obdobným způsobem. Došlo však k doplnění informování prostřednictvím Portálu, který bude platformou nahrazující původní komunikaci prostřednictvím sdělených kontaktních údajů. Připomínkové místo s vypořádáním souhlasí.
67. Konfederace zaměstnavatelských a podnikatelských svazů ČR	D	Zákon o kybernetické bezpečnosti, § 45 odstavec 1 – jak konkrétně se bude vést evidence penetračních testů? <u>Odůvodnění:</u> NÚKIB bude evidovat dle zmíněného paragrafu velice citlivé údaje. Zajímalo by nás například, jakou formu penetračního testu bude NÚKIB evidovat? Pouze záznam o tom, že u daného poskytovatele regulované služby test proběhl, nebo celou zprávu testu?	Vysvětleno V evidenci penetračních testů budou ukládány záznamy o provedených penetračních testech včetně zprávy o průběhu. Na údaje z evidence penetračních testů se vztahuje povinnost mlčenlivosti ze strany zaměstnanců Úřadu podle § 48 odst. 4. V souvislosti se všemi evidencemi vedenými Úřadem dále plošně platí, že informace v nich vedené se neposkytují podle právních předpisů upravujících svobodný přístup k informacím, tedy je zajištěna jejich základní ochrana před zveřejněním. Připomínkové místo s vypořádáním souhlasí.
68. Konfederace zaměstnavatelských a podnikatelských svazů ČR	D	Zákon o kybernetické bezpečnosti, § 58 – kdy bude rozhodnuto o konkrétním přestupku a tím pádem i jeho výši?	Vysvětleno - nyní § 60 Proces ukládání pokut za přestupky spočívající v porušení povinností stanovených zákonem o

		<u>Odůvodnění:</u> Předpokládáme správně, že přestupek se zjistí kontrolou NÚKIBu? Bude zjištění znamenat, že hned bude organizace penalizována či bude mít nejdříve čas na nápravné opatření do určitého data? Z daného paragrafu tento postup není zcela jasný.	kybernetické bezpečnosti se principiálně neliší od procesu ukládání pokut za přestupky podle jiných zákonů. Přestupkem je porušení povinností stanovených zákonem, přičemž ukládání pokuty za přestupek probíhá ve standardním přestupkovém řízení vedeném podle pravidel obsažených zejm. v zákoně č. 255/2012 Sb., o přestupcích. Návrh zákona nestanoví pevnou posloupnost realizace jednotlivých zákonných oprávnění Úřadu (tedy že by nejprve měl provést kontrolu, pak uložit nápravné opatření a teprve poté uložit pokutu za přestupek), takové omezení dozorových orgánů není ani v praxi obvyklé. Naopak je napříč sektory a zákony zaužívanou (a soudní judikaturou aprobovanou) praxí, že přestupky lze stíhat nezávisle na uložených nápravných opatřeních (oba instituty mají rozdílné funkce, zatímco nápravné opatření slouží k nápravě nezákonného stavu, pokuta za přestupek je trestem za porušení povinností). NÚKIB se však dlouhodobě profiluje jako úřad, jehož primárním zájmem je zesouladění skutečného stavu s požadavky zákona, nikoli slepé trestání pochybení povinných osob. Zároveň je v zájmu kybernetické bezpečnosti České republiky, aby byly finanční prostředky investovány do kybernetické bezpečnosti organizace spíše než do placení pokut. Proto již za účinnosti současného zákona obvykle NÚKIB nejprve přistoupí k uložení nápravného opatření a teprve poté, co toto nápravné opatření není řádně splněno, ukládá pokutu za přestupek. Zákon však umožňuje uložit rovnou pokutu za přestupek (zejm. tam, kde uložení nápravného opatření již nemá význam), resp. ve skutkově jasných případech uložit pokutu za přestupek i bez provedení kontroly (tzv. od stolu na základě v té době shromážděných informací).

			Připomínkové místo s vypořádáním souhlasí.
69. Konfederace zaměstnavatelských a podnikatelských svazů ČR	D	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, § 4 odstavec 6 – zřízení bezpečnostní role garanta aktiv? <u>Odůvodnění:</u> Vyhláška pro nižší režim od prvního návrhu prošla radikální změnou, tedy velkým seškrtáním povinností. Vypadla tak i role garanta aktiv, která dle našeho názoru je klíčová pro řízení bezpečnosti daného aktiva. Vyhláška evidenci aktiv zmiňuje jen v odstavci 6 zmíněného paragrafu, kde odkazuje na zákon, který říká, že u primárních aktiv organizace určí související organizační části. Máme to tedy chápat tak, že daná organizační část převezme roli garanta aktiv? Ovšem roli, která není v této vyhlášce specifikována?	Vysvětleno Záměrem legislativního návrhu a jeho prováděcích právních předpisů pro režim vyšších i nižších povinností je stanovit požadavky přiměřeně, tak aby byly realizovatelné a nekladly na režim nižších povinností nepřiměřené požadavky. Proto je pro režim nižších povinností stanovena pouze povinná bezpečnostní role, kterou lze připodobnit k roli manažera kybernetické bezpečnosti (§ 4 odst. 3). S povinnou rolí ve smyslu garanta aktiv v současném návrhu prováděcího právního předpisu pro režim nižších povinností počítáno není. Připomínkové místo s vypořádáním souhlasí.
70. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Obecná připomínka k návrhu zákona Z pohledu společností, u nichž je stanovena věcně usměrňovaná cena by bylo poněkud žádoucí, aby bylo možno náklady na kybernetickou bezpečnost promítat jako oprávněné náklady do kalkulací. Požadujeme tedy do zákona doplnit, že náklady spojené s kybernetickou bezpečností jsou oprávněnými náklady.	Neakceptováno Na základě připomínky provedena konzultace s vybranými dotčenými společnostmi z oblasti elektroenergetiky. Tyto společnosti sdělily, že náklady na kybernetickou bezpečnost jsou uznávány jako oprávněné náklady již nyní, bez navrhované kodifikace. Není tedy potřeba oblast explicitně upravovat. Naopak z diskusí vyplynulo, že by požadovaná úprava generovala další otázky, typu přesného vymezení „kybernetické bezpečnosti“, vykazování a dalších. Vytvářely by se tak další administrativní náklady, nad rámec nutných. Zároveň je třeba uvést, že opatření v oblasti kybernetické bezpečnosti jsou neoddělitelnou součástí budování bezpečné a stabilní technologie. Praxe tedy ukazuje, že navrhovaná úprava tedy není potřebná, neboť již prakticky funguje i bez navrhované kodifikace.

			Reakce připomínkového místa: Elektroenergetika tvoří malý segment a cena je v dané oblasti sice regulována, nicméně jiným mechanismem než u oboru VaK. Máme již zkušenost, že to co je někde akceptováno pro jednu regulaci, může být pro jinou regulaci hodnoceno zcela jinak. Ve vodárenství je odděleno vlastnictví „technologie“ od jejího provozovatele, který však je povinen zajišťovat kybernetickou bezpečnost a v případě nových kritérií se bude jednat o dopad povinností na celé společnosti, nikoli pouze na jimi provozované části, tudíž náklady nebude možné oddělit jen pro některé kalkulace, které zásobují více než 50 000 obyvatel a je proto potřeba nastavit pravidla, že takovéto náklady jsou uznatelné i pro kalkulace, které nemají povinnost zajistit kybernetickou bezpečnost ze zákona. Reakce NÚKIB: Po schůzce s připomínkovým místem bylo v předmětné problematice kontaktováno Ministerstvo financí a jeho stanovisko bylo následně předáno připomínkovému místu. Na základě stanoviska MF bylo ze strany připomínkového místa vypořádání připomínky odsouhlaseno. Připomínka je vypořádána.
71. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k tezí vyhlášky Mezi povinnými subjekty by v rámci vodárenství měli být i provozovatelé vodovodů nebo kanalizací, kteří provozují nejméně pro 5.000 obyvatel v součtu, aby se zajistila větší rovnost mezi provozovateli.	Neakceptováno. Aktuální návrh kritérií odpovídá dvěma vstupům. Prvním z nich je požadavek směrnice NIS 2 na zahrnutí všech provozovatelů vodovodů a kanalizací, kteří jsou středním a velkým podnikem. Druhým vstupem - s drobnými textovými úpravami - je zachování dosavadní regulace, která v rámci provozovatelů základní služby stanovovala kritérium

			tak, že dopadové kritérium bylo zejm. „závažné omezení druhu služby postihující více než 50 000 osob“, nehledě na jejich velikost. S ohledem na tyto dva vstupy došlo k vytvoření současného návrhu kritérií. Snižování daného kritéria nepovažujeme za účelné a pro subjekty za nadměrně zatěžující. Reakce připomínkového místa: Pokud je jedním z pramenů dopadové kritérium ze stávající právní úpravy, pak je otázkou, zda toto nepřehodnotit, neboť nový zákon zpřísňuje pohled na kybernetickou bezpečnost a zejm. u zásobování obyvatelstva základními službami s tím, že by jejich dodavatelé měli dbát na zvýšené riziko jejich provozování, které ostatně je patrné i z kontextu událostí dnešní doby. Narušení zabezpečení zásobování obyvatel pitnou vodou může vést k ohrožení zdraví mnoha obyvatel i u celků, které zásobují méně než 50 000 obyvatel a takovýchto systémů je mnoho. Na schůzce bylo dovysvětlením vypořádáno.
72. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k § 10 odst. 1 písm. f) a § 10 odst. 2 písm. b) návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Požadujeme upravit dle odůvodnění. <u>Odůvodnění:</u> Jaký je vztah tohoto požadavku k zásadám civilního práva, smluvní volnosti a k občanskému zákoníku? Dle našeho názoru není možné, aby soukromoprávní osoba donutila jinou osobu k uzavření smlouvy s určitým obsahem.	Vysvětleno Samotné vyhlášky nyní nejsou předmětem připomínkového řízení, tím je v současné chvíli jenom návrh zákona. Samotné vyhlášky jsou stále rozpracovány a probíhají v nich dílčí úpravy. Povinnost zohledňovat požadavky plynoucí ze zákona při řízení dodavatele, tedy při jeho výběru a uzavření smlouvy, platí vždy. Pokud má již subjekt něco zasmulvněno a začnou mu ze zákona plynout nové povinnosti, měl by své smlouvy revidovat. Následně může uzavřít dodatek, případně původní smlouvu

		vypovědět a vybrat si dodavatele nového. Obdobně by měl subjekt postupovat ať už se jedná o kybernetickou bezpečnost nebo o jakékoliv jiné povinnosti, které mu ukládají právní předpisy. Z tohoto důvodu rovněž existuje lhůta, ve které se mohou povinné subjekty na změny po účinnosti zákona připravit. Stav, ve kterém by subjekty měly uzavřeny smlouvy nesplňující požadavky plynoucí z bezpečnostních opatření je jednoznačně nežádoucí. Vztah tohoto požadavku je nicméně zcela v mezích zásad civilního práva. Autonomie vůle v dikci ustanovení §§ 1751-1753 a 1799 OZ, cílí na vztahy B2B avšak není vyloučena i pro vztahy B2C (v krajním případě C2C). Neztotožňujeme se s tvrzením, že (...) „není možné, aby soukromoprávní osoba donutila jinou osobu k uzavření smlouvy s určitým obsahem.“. Zejména s ohledem na autonomii vůle, což je stěžejní zásada civilního práva (Zásada autonomie vůle vychází z předpokladu, že subjekty soukromého práva mohou vstupovat svobodně ze své vůle do soukromoprávních vztahů a sjednat si většinu práv a povinností, nejsou-li v daném konkrétním případě omezeny zákonem.). Dále § 1725 OZ upravuje smluvní volnost. Pokud Vám Vaši dodavatelé odmítají akceptovat Vaše řízení dodavatelů, resp. zákonné požadavky do smluv plynoucích s právní regulace kybernetické bezpečnosti, lze toto zohlednit v RTP či PoA a kontinuálně pracovat na jejich řešení, třeba tak, že najdu dodavatele jiného. Reakce připomínkového místa: Ne vždy je možné sehnat jiného dodavatele a se stávajícím se dohodnout na podmínkách, které jsou požadovány. Pro některé produkty je pouze jeden dodavatel. Ostatně podmínky stanovené zákonem o

			kybernetické bezpečnosti nejsou ochotny akceptovat ani subjekty, které mu sami podléhají, ale vůči svým zákazníkům s nimi mají problém (např. dodavatelé el. energie). Tvrzení ve vypořádání připomínky tudíž není založené na pravdě a skutečných podmínkách trhu. Na schůzce bylo vysvětlením vypořádáno.
73. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k příloze č. 7 návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Požadujeme upravit dle odůvodnění. <u>Odůvodnění:</u> Opětovně není zřejmé, jaký je vztah tohoto ustanovení k občanskému zákoníku, jaká bude platnost soukromoprávní smlouvy, když nebude obsahovat ustanovení požadovaná přílohou č. 7 atp. Písm. g) - Žádáme o vysvětlení, zda se jedná o smlouvy, které mají být např. písemně. Písm. h) – Dle našeho názoru jde o nadbytečnou formulaci. I bez tohoto ustanovení jsou subjekty povinny řídit se právními předpisy.	Vysvětleno Teze vyhlášek pro režim vyšších a nižších povinností nejsou součástí nyní probíhajícího mezirezortního připomínkového řízení, to proběhne samostatně na začátku příštího roku. Je nutné na předmětnou problematiku nahlížet z pohledu řízení rizik u určených aktiv v rámci určeného rozsahu regulované služby, u řízení dodavatelů tomu není jinak. Smlouva, která nebude obsahovat doporučená ustanovení do smluv, bude samozřejmě platná, povinné subjekty mají přijmout technická, provozní a organizační opatření k řízení rizik. Je důležité mít u povinné osoby v určeném rozsahu nastaven způsob určení bezpečnostních požadavků, způsob hodnocení rizik, způsob stanovení úrovně zabezpečení, zohlednit charakter regulovaného systému a míru zásahu dodavatele do tohoto systému. Důležité je proto provést hodnocení rizik před samotným uzavřením smlouvy s významným dodavatelem a na základě stanovení úrovně a způsobu realizace bezpečnostních opatření lze jako jednu z možností vyhodnotit požadavek na specifická smluvní ujednání s významnými dodavateli, například zohlednit ty uvedené v příloze č. 7. Samotná kontrola dodržování je tedy zaměřena na nastavení celkového procesu

		řízení dodavatele a zda plní svůj účel. Výklad požadavků vyhlášky na smlouvy s významnými dodavateli je nutné chápat také z pohledu jeho účelnosti a přiměřenosti. K písm. g) - Jde o ustanovení smlouvy, které reflektuje způsob, jakým dochází k řízení změn, a to ve dvou rovinách: a) Jakým způsobem probíhá vzájemné schvalování změn obsahu smlouvy; b) Tzv. <i>change management</i> – tedy stanovení přezkumu možných dopadů změn (např. prostřednictvím analýzy rizik), akceptačního procesu (jakým způsobem je změna přijata), testování před nasazením do provozu, promítnutí do bezpečnostních politik, dokumentování změny, možnost navrácení do původního stavu apod. K písm. h) - Chápeme Váš pohled na nadbytečnost tohoto ustanovení, ale jedná se o poměrně často opomíjené ustanovení. Směřuje na ujednání, že smlouva je v souladu s aktuálními právními předpisy (především těmi, které se dotýkají plnění smlouvy) a směřuje k tomu, že smlouva musí plnit aktuální legislativní požadavky a v případě významných legislativních změn musí být upraven způsob, jakým bude těmto požadavkům přizpůsobena. Vždy je nezbytné ve smlouvě specifikovat, s kterými konkrétními právními předpisy má být plnění v souladu, a pokud je to možné, tak i konkrétní ustanovení jednotlivých předpisů. Obecně závaznými právními předpisy jsou zjednodušeně řešeno všechny normativní právní akty, které nejsou určeny pro individuálně stanovený okruh osob, tj. všechny zákony, vyhlášky, nařízení vlády, evropské předpisy, obecně závazné vyhlášky obcí apod. Specifikace těch relevantních, k jejichž dodržování se má dodavatel smluvně zavázat, a případně reagovat na jejich změnu,

			je tak nezbytná. Obecné proklamace o povinnosti dodržovat platné právní předpisy bez dalšího určení mohou ve výsledku vést k prohlášení neurčitosti tohoto ustanovení a k jeho praktické nevymahatelnosti. Připomínkové místo s vypořádáním souhlasí.
Konfederace zaměstnavatelských a podnikatelských svazů ČR 74.	Z	Připomínka k § 2 odst. 1 písm. a) návrhu zákona Požadujeme upravit nebo doplnit dle odůvodnění. <u>Odůvodnění:</u> Dle našeho názoru není pojem definován dostatečně, a to také v kontextu možnosti uložení pokuty podle § 58 ve výši 250 000 000 Kč nebo do výše 2 % čistého celosvětového ročního obrátu.	Neakceptováno Pojem aktiva je definován relativně obecně zcela záměrně, neboť aktivem může být prakticky cokoli relevantního, s čím je potřeba v rámci řízení kybernetické bezpečnosti počítat, resp. to zohledňovat a vést o tom úvahu. Definice aktiva se snaží již ve svém obsahu tuto relevanci stanovit, a to vázaností na zpracování informací a dat v elektronické podobě. Současně návrh zákona vymezuje, že aktiva mohou být primární a podpůrná a tyto skupiny dále definuje v písmenech b) a c), resp. v písm. d) dále definuje, co je potřeba chápat pod technickými aktivy. Do větších podrobností není vhodné v rámci definice takto základních pojmů zacházet, neboť je potřeba je aplikovat v rozličných situacích u rozličných subjektů. Výklad pojmu aktiva v konkrétní organizaci pak bude předurčen charakterem a specifiky této organizace. Pro potřeby návrhu zákona je možné chápat pojem aktiva jako ekvivalent pojmu „informační systém“ užívaného v současném zákoně o kybernetické bezpečnosti. Tento pojem přitom v zákoně také není blíže definován, naopak pojem aktiva je v tomto smyslu definován podrobněji než pojem informační systém (ačkoli je chápán obdobně). Připomínkové místo s vypořádáním souhlasí.

75. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k § 2 odst. 1 písm. c) návrhu zákona Požadujeme upravit dle odůvodnění. <u>Odůvodnění:</u> Dle našeho názoru je označení zaměstnance za podpůrná aktiva proti lidské důstojnosti.	Neakceptováno Jakkoliv oceňujeme Váš pohled na ochranu důstojnosti zaměstnanců, zařazení množiny „zaměstnanci“ do podmnožiny „podpůrných aktiv“ je technický pojem, který nemá za cíl snižovat lidskou důstojnost jednotlivých zaměstnanců. Jedná se o pojem dlouhodobě používaný, který je navíc podřízen běžně užívanému popisu pojmu "aktivum" jako čehokoliv, co má pro organizaci nějakou hodnotu (což, jak věříme, je zaměstnanec v první řadě). V neposlední řadě považujeme za vhodné neměnit dlouhodobě zaužívané pojmy za situace, kdy jejich použití nikdy nebylo problematické. Připomínkové místo s vypořádáním souhlasí.
76. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k § 4 odst. 1 návrhu zákona Požadujeme upravit dle odůvodnění. <u>Odůvodnění:</u> Dle našeho názoru by měla být tato kritéria stanovena zákonem a podléhat schválení Parlamentem ČR, protože na základě identifikace služby jako regulované jsou ukládány subjektům rozsáhlé povinnosti pouze ve formě prováděcího předpisu.	Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech [§ 3 a § 2 písm. d)], tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby [§ 3, ve spojení s § 2 písm. i) a k) a § 22a]. Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon [§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)], a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá [§ 3 a § 2 písm. b)]. Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly

			standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Připomínkové místo s vypořádáním souhlasí.
77. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k § 8 návrhu zákona Požadujeme upravit nebo doplnit dle odůvodnění. <u>Odůvodnění:</u> Z předloženého návrhu není zcela zřejmé, zda se budou muset registrovat i stávající určení poskytovatelé základní služby. Pokud již jednou jsou evidováni, tak je tento krok poněkud nadbytečný.	Vysvětleno NÚKIB samozřejmě disponuje seznamem současných povinných subjektů, avšak kritéria, na základě kterých je organizace zařazena do regulace, se dle nové úpravy zcela mění. Zatímco nyní jsou regulovány jednotlivé informační systémy, dle nové úpravy budou regulovány celé organizace a to na základě poskytování regulované služby. Každá organizace přitom může poskytovat i více regulovaných služeb. Je tedy nutné, aby identifikaci regulovaných služeb (posouzení kritérií) a jejich následnou registraci, provedly všechny subjekty, tedy včetně těch, na které dopadá současná regulace. Kritériem pro regulovanou službu dle nové právní úpravy tudíž nemůže být pouze fakt, že dnes některý její systém pod regulaci spadá, ale organizace musí poskytovat alespoň jednu či více regulovaných služeb dle nové právní úpravy. Registrace do nové evidence je tudíž zcela nezbytná. Připomínkové místo s vypořádáním souhlasí.
78. Konfederace zaměstnavatelských a	Z	Připomínka k § 13 odst. 1 písm. a) návrhu zákona Požadujeme upravit dle odůvodnění. <u>Odůvodnění:</u>	Neakceptováno

podnikatelských svazů ČR		Jedná se o poněkud nereálný požadavek, neboť primárním aktivem se rozumí „informace a služby“ ve firmě. Informace ve firmě neustále vznikají, nelze je proto trvale identifikovat. Přitom nesplnění „identifikace všech primárních aktiv“ je přestupkem s pokutou 250 000 000 Kč nebo do výše 2 % čistého celosvětového ročního obrátu.	Stanovený rozsah se vztahuje na aktiva související s regulovanou službou (nikoliv na všechna identifikovaná primární aktiva - pokud všechna nesouvisí s regulovanou službou). Pracuje se s typovými aktivy, nikoliv s každou službou/informací jako takovou zvlášť. Jde o základní identifikaci služeb, které organizace poskytuje (za jakým účelem je vytvořena a co jsou její zásadní služby). Primární aktiva, která nesouvisí s regulovanou službou není potřeba hodnotit (návrh zákona to nepožaduje). Cílem regulace není, aby povinná osoba řešila každý dokument, ale aby nastavila pravidla pro ochranu, například sdílení, šifrování. Připomínkové místo s vypořádáním souhlasí.
79. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k § 27 odst. 2 návrhu zákona Požadujeme upravit dle odůvodnění. <u>Odůvodnění:</u> Není zřejmé, jestli Úřad má vydávat speciální rozhodnutí o tom, že jde o strategicky významnou službu, nebo jestli každé rozhodnutí Úřadu o regulované službě v režimu vyšších povinností např. podle § 5 písm. b) znamená, že jde o strategicky významnou službu.	Akceptováno jinak – nyní § 28 Ustanovení § 28 bylo upraveno tak, aby bylo pro adresáty srozumitelnější. Obecně ale zůstává, že strategicky významné služby jsou ty regulované služby, které naplňují identifikační kritéria strategicky významných služeb stanovená vyhláškou o regulovaných službách. A zároveň jde o ty regulované služby, kde tak stanoví Úřad zvláštním rozhodnutím v případě, že „by její (pozn. regulované služby) narušení mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek.“ V odpovědi na v připomínce vznesenou otázku, zda jde o všechny regulované služby určené rozhodnutím podle § 5 odst. 1 písm. b), tak nikoliv. Platí, že všechny strategicky významné služby jsou regulovanými

			službami, nikoliv naopak. V případě určení regulované služby rozhodnutím Úřadu, nemusí dojít zároveň k určení této služby jako strategicky významné služby. Připomínkové místo s vypořádáním souhlasí.
80. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k § 30 návrhu zákona Požadujeme upravit nebo doplnit dle odůvodnění. <u>Odůvodnění:</u> V rámci opatření obecné povahy může úřad stanovit podmínky nebo zakázat využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu. V tomto ohledu nám není zcela jasné a předložený návrh neřeší, kdo bude následně hradit ztráty, resp. náhradu jednoho zařízení za druhé.	Vysvětleno – nyní § 31 Návrh zákona s prováděcími předpisy považujeme za ústavně konformní. Z toho důvodu NÚKIB nevidí důvod přidávat speciální ustanovení o kompenzaci. Vzhledem k charakteru navrhované právní úpravy, převážně v oblasti mechanismu bezpečnosti dodavatelského řetězce, která se snaží vyjít vstříc povinným osobám (například v otázkách životních cyklů technologií či zamezení možné závislosti na jedné technologii skrze systém výjimek), není nutné, aby možnost kompenzací byla upravena přímo v zákoně. Kompenzací se v obdobných případech lze domáhat na základě již existujících zákonných prostředků, které předmětným ustanovením § 31 nejsou jakkoliv dotčeny. Připomínkové místo s vypořádáním souhlasí.
81. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k § 34 odst. 1 návrhu zákona Požadujeme upravit nebo doplnit dle odůvodnění. <u>Odůvodnění:</u> Není zcela zřejmé, zda se uvedený požadavek vztahuje na IT zabezpečení nebo na samotnou službu, např. na poskytování dopravy? Pokud na samotnou službu dopravy, nemělo by to být obsahem tohoto zákona; tento zákon se zabývá kybernetickou bezpečností, ne povinností zajišťovat dopravní obslužnost. Tato připomínka se váže k přestupku v § 58 odst. 3 písm. e).	Vysvětleno - nyní § 35 Motivem připomínkovaného ustanovení § 35, ostatně jako celého předkládaného návrhu zákona je zvýšit kybernetickou bezpečnost nejdůležitějších služeb z pohledu státu s cílem zajištění jejich nerušeného a správného fungování. Ustanovení § 35 o zajištění dostupnosti služeb z ČR tak v souladu s tímto má za cíl zavést taková bezpečnostní opatření, která zajistí, že poskytovatelé strategicky významných služeb, jejichž poskytování je závislé na technických aktivech

			umístěných mimo ČR, budou v případě nutnosti schopni zajistit poskytování těchto služeb z území ČR. Připomínkové místo s vypořádáním souhlasí.
82. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k § 48 odst. 4 písm. b) návrhu zákona Požadujeme upravit nebo doplnit dle odůvodnění. <u>Odůvodnění:</u> Tato podmínka bude pro právnickou osobu se sídlem v ČR, která je však součástí nadnárodní skupiny, která má skutečné majitele např. v USA, diskriminační. Sesterské společnosti např. z Německa či Francie budou moci být členem Komunity (bude záležet na podmínkách stanovených Německem a Francií), ale česká společnost členem Komunity nebude moci být.	Vysvětleno - nyní § 51 odst. 5 písm. b) Omezení je dáno samotným nařízením Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center, které podmiňuje členství v Komunitě tím, že subjekt musí být usazen v členském státu, v našem případě v ČR. Současně nařízení umožňuje každému členskému státu formulovat vlastní bezpečnostní důvody, při jejichž naplnění bude žadatel vyhodnocen jako nezpůsobilý pro členství v Komunitě. Napříč EU není v této otázce jednotná úprava, proto může docházet k rozdílu v jednotlivých členských státech. Vnitrostátní bezpečnostní důvody jsou tak formulovány s ohledem na skutečnost, že Komunita má představovat rozsáhlou, otevřenou, interdisciplinární a různorodou skupinu evropských zúčastněných stran zapojených do rozvoje technologií kybernetické bezpečnosti, a celkově přispět k posílení konkurenceschopnosti a kapacit EU v oblasti kybernetické bezpečnosti. Připomínkové místo s vypořádáním souhlasí.
83. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k § 55 návrhu zákona Požadujeme upravit nebo doplnit dle odůvodnění. <u>Odůvodnění:</u> Toto zmocnění je příliš obsáhlé, neboť pouhou vyhláškou Úřadu mají být určeny subjekty, na něž dopadají rozsáhlé povinnosti. Dle našeho názoru by toto měl stanovovat přímo zákon.	Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě

			vyhlášky č. 317/2014 Sb., o významných informačních systémech [§ 3 a § 2 písm. d)], tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby [§ 3, ve spojení s § 2 písm. i) a k) a § 22a]. Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon [§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)], a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá [§ 3 a § 2 písm. b)]. Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Ustanovení § 55 původního znění návrhu zákona bylo zrušeno a jednotlivá zmocnění zůstala u konkrétních ustanovení v rámci návrhu zákona. Připomínkové místo s vypořádáním souhlasí.
84. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k § 58 a násl. návrhu zákona Požadujeme upravit nebo doplnit dle odůvodnění. <u>Odůvodnění:</u> V rámci této části je uvedeno velké množství nejrozličnějších přestupků, které nadto obsahují velmi vysoké pokuty. Úřad vždy proklamoval, že chce nejdříve edukovat a radit a teprve až následně trestat, což by mělo být zohledněno. Nehledě na to, že by se vše mělo posuzovat	Vysvětleno - nyní § 60 a násl. K odst. 1 připomínky Přestupky jsou pouze sankčním odrazem zaváděných povinností, bez možných sankcí by stát nebyl schopen efektivně vymáhat jejich plnění. Výše pokut je zásadně dána implementovanou směrnicí.

	z hlediska přiměřenosti, kdy opatření u jednoho typu subjektu nemusí být přiměřená nebo proveditelná oproti jinému subjektu ve stejném oboru. Obecně si myslíme, že pomocná úloha NÚKIB by měla být v zákoně zdůrazněna, protože dopad bude velký na mnoho subjektů a odborníků, kteří by byli schopni poradit bude nedostatek. Kupříkladu v § 59 odst. 4 je uvedeno, že „...<i>přestupky související se zohledněním požadavků vyplývajících z bezpečnostních opatření při výběru dodavatele nebo ve smlouvě s dodavatelem, přestupky spočívající v porušení povinností z mechanismu prověřování bezpečnosti dodavatelského řetězce a přestupky spočívající v neoznámení informací a udržování stavu neinformování Úřadu nebo uživatelů regulované služby jsou trvajícíchmi přestupky.</i>“ Toto ustanovení výrazně zvyšuje právní nejistotu, neboť je potenciál, že i po několika letech, kdy budou společnosti postupovat s nejlepším vědomím a svědomím, mohou zjistit, že v počátcích zavádění uvedeného předpisu do praxe chybovaly. Zároveň nám není jasné, jak se bude postupovat v případě výpovědi smluv anebo odstoupení od smluv v případě rizikového dodavatele v kontextu aplikace občanského zákoníku (Jak se bude např. postupovat v případě již proběhlých plnění?).	Hledisko přiměřenosti je jedním ze zásadních principů, kterým je řízena celá regulace kybernetické bezpečnosti v České republice. Konkrétním projevem je např. přístup orientovaný na rizika, kdy i poskytovatel regulované služby v režimu vyšších povinností zavádí bezpečnostní opatření v návaznosti na výsledky hodnocení rizik a dále s ohledem na bezpečnostní potřeby poskytovatele regulované služby, tedy s maximálním zohledněním specifík prostředí daného poskytovatele regulované služby. Zásada přiměřenosti, z níž vychází nutnost nalezení řešení odpovídajícího okolnostem daného případu, je také jednou z obecně platných zásad pro činnost veřejné správy. Hledisko přiměřenosti tak je jednoznačně v právní úpravě zavedeno. Pomocná a edukativní úloha NÚKIB je v zákoně zdůrazněna na následujících místech: § 44 odst. 4 písm. d) bod 4. „Úřad dále v oblasti kybernetické bezpečnosti, ve vybraných oblastech ochrany utajovaných informací a v souvislosti s nimi zajišťuje prevenci, vzdělávání a metodickou podporu.“ § 44 odst. 5 „Vládní CERT jako součást Úřadu: zajišťuje řešení, koordinaci, analýzu a preventivní působení vůči hrozbám v oblasti kybernetické bezpečnosti, zranitelnostem v oblasti kybernetické bezpečnosti, včetně vyhledávání zranitelností,

		kybernetickým bezpečnostním událostem a kybernetickým bezpečnostním incidentům, včetně jejich zvládání, působí jako kontaktní místo pro poskytovatele regulovaných služeb v režimu vyšších povinností, testuje zavedení a odolnost zabezpečení aktiv, včetně provádění penetračního testování se souhlasem dotčených orgánů či osob, je koordinátorem pro účely koordinovaného zveřejňování zranitelností, vede evidenci kybernetických bezpečnostních incidentů, událostí, kybernetických hrozeb a zranitelností, spolupracuje s orgány a osobami působícími v oblasti kybernetické bezpečnosti, poskytuje orgánům a osobám konzultace v oblasti kybernetické bezpečnosti, přijímá a vyhodnocuje podněty v oblasti kybernetické bezpečnosti od orgánů a osob“ Takto rozsáhlé rozvedení pomocné a edukativní úlohy NÚKIB považujeme za dostatečné. K odst. 2 připomínky Toto ustanovení naopak zvyšuje právní jistotu, neboť je na jisto postaveno, že se jedná o trvalé přestupky a tato skutečnost nemůže být předmětem sporu. Ustanovením je reflektováno, že není postihováno pouze jednorázové porušení povinnosti, ale za vysoce nežádoucí je považováno to, kdy je závažný stav udržován a existuje významný zájem na odstranění tohoto závažného stavu a co nejdřívejší náprava.

			K odst. 3 připomínky Vypovězení smluvního závazku na základě zákona by mělo být vždy bezúplatné, tj. nevyvolat dodatečné náklady na straně poskytovatelů strategicky významných služeb; případná sjednaná sankce za výpověď smlouvy by měla mít buď charakter odstupného dle § 1992 občanského zákoníku (které je nicméně spojeno nikoliv s ukončením závazku ex nunc, ale ex tunc, případně výpověď smluvní, která by tak byla alternativní možností k ukončení závazku ze zákona. Na základě jiných připomínek bylo nicméně ustanovení upraveno a právo na ukončení dlouhodobých závazků tak bude přiznáno i subjektům, které nejsou v postavení zadavatele podle zákona o zadávání veřejných zakázek. Připomínkové místo s vypořádáním souhlasí.
85. Konfederace zaměstnavatelských a podnikatelských svazů ČR	Z	Připomínka k § 61 odst. 1 návrhu zákona Požadujeme upravit nebo doplnit dle odůvodnění. <u>Odůvodnění:</u> Pokud nebude osoba smět vykonávat řídicí funkci, nebude pak pravděpodobně moci napravit porušovanou povinnost. Pozastavení výkonu funkce tak nemusí přispět k nápravě stavu, ale naopak k paralýze společnosti, pokud by ona osoba byla např. jediným jednatelem ve firmě.	Neakceptováno - nyní § 63 odst. 1 Rozhodnutím podle § 63 návrhu zákona se pozastavuje výkon řídicí funkce, obdobně jako je tomu v případě rozhodnutí podle § 63 zákona č. 90/2012 Sb., o obchodních korporacích, na který § 63 návrhu zákona navazuje a z něhož přebírá podstatnou část úpravy. Obdobně jako v případě vyloučení člena statutárního orgánu z výkonu funkce podle zákona o obchodních korporacích, i v případě návrhu zákona dochází k omezení výkonu konkrétní funkce, nikoli k omezení výkonu činnosti ostatních orgánů společnosti, či snad dokonce práv a povinností jejích podílníků. Pokud je ve společnosti jen jeden statutární orgán, podílíci společnosti mohou v případě pozastavení výkonu funkce statutárního orgánu

			ustanovit nový statutární orgán, prokuristu apod. Stejně lze postupovat i v případě, že jediný statutární orgán je současně jediným podílníkem společnosti (výkon těchto práv není rozhodnutím omezen, proto i když je např. jediný společník dočasně zbaven práva vykonávat pozici jednatele společnosti, pořád je oprávněn v rámci výkonu svých práv společníka ustanovit nového jednatele). Připomínkové místo s vypořádáním souhlasí.
86. Ministerstvo zemědělství	Z	Požadujeme vyhodnotit proveditelnost nastavených povinností ukládaných poskytovatelům regulované služby, např. upřesnit jaké informace o dodavatelích významných dodávek, jak v rámci veřejných zakázek nastavit bezpečnostní opatření z varování nebo opatření obecné povahy, bez úpravy v rámci zákona o veřejných zakázkách. Popisy různých rozsahů regulované služby jsou roztržštěné a neuspořádané, kritéria pro určení nejednoznačná. Dosud zůstává nevyřešeno rozhraní povinností subjektu kritické infrastruktury a poskytovatele strategicky významné služby. Ministerstvo zemědělství žádnou kritickou informační infrastrukturu ani základní službu neposkytuje a přesto je určeno subjektem kritické infrastruktury. Ve změně zákona č. 34/2021 Sb. je v § 7 písm. c) uvedeno: „správcem informačního systému kritické informační infrastruktury, správcem komunikačního systému kritické informační infrastruktury, správcem informačního systému základní služby nebo provozovatelem základní služby“ se nahrazují slovy „poskytovatelem strategicky významné služby“.	Neakceptováno Pro lepší orientaci byla připomínka rozdělena do samostatných bodů: 1) Všichni poskytovatelé regulované služby (včetně těch soukromých) musí řídit své dodavatele, tedy zohledňovat požadavky vyplývající z bezpečnostních opatření při výběru dodavatele a ve smlouvě s ním. Ustanovení týkající se řízení dodavatelů pak pro poskytovatele regulovaných služeb, kteří jsou zároveň veřejným zadavatelem, nad rámec toho stanovuje, že zohlednění požadavků vyplývajících z bezpečnostních opatření v zadávacích podmínkách na veřejnou zakázku nelze považovat za nezákonné omezení hospodářské soutěže, resp. nejedná se o vytváření bezdůvodných překážek hospodářské soutěže. Směřuje tedy přímo na § 36 odst. 1 zákona č. 234/2016 Sb. V zásadě přitom nepřináší nic nového, neboť ve vztahu ke všem zákonným povinnostem zadavatelů (vyplývajícím z jakýchkoli jiných právních předpisů) platí, že jejich zohlednění při výběru dodavatele v míře nezbytné pro jejich splnění nemůže být shledáno neodůvodněným omezením hospodářské soutěže. Povinnost zohledňovat požadavky plynoucí ze zákona při řízení dodavatele, tedy při jeho výběru a uzavření

		smlouvy, platí vždy. Obdobně by měl subjekt postupovat ať už se jedná o kybernetickou bezpečnost nebo o jakékoli jiné povinnosti, které mu ukládají další zákony. Úprava zákona č. 234/2016 Sb. tudíž nutná není, jelikož tento postup umožňuje jak současná právní úprava, tak navrhovaný zákon. K této problematice vydal Úřad metodický materiál – Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost (dostupný na https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/). 2) Regulovaná služba a poskytovatel regulované služby jsou definováni v ustanovení o vymezení pojmů, postup jejich identifikace a určení v následujících ustanoveních. Hned vzápětí také ustanovení o stanovení jejich režimu. Na základě připomínek došlo k dílčím úpravám a jak věříme, také ke zvýšení srozumitelnosti těchto ustanovení. Jiné způsoby stanovení a uspořádání těchto ustanovení byly zvažovány na začátku tvorby tohoto právního předpisu, nicméně tento byl vyhodnocen jako nejlogičtější a nejvíce srozumitelný z uvažovaných. 3) Pojem „kritická infrastruktura“, resp. „kritická informační infrastruktura“ se již v návrhu nevyskytuje, resp. je jedním ze vstupů do určení regulované služby v rámci ustanovení o určení regulované služby. Jedná se tak o naplnění tzv. automatu z čl. 2 odst. 3 směrnice NIS2. Tj. každá kritická infrastruktura (ať už podle současného krizového zákona nebo podle nově připravovaného zákona o prvcích kritické infrastruktury) je poskytovatelem regulované služby v režimu vyšších povinností. Stanovení strategicky významné služby je zcela odlišnou otázkou a kritéria

			pro její identifikaci jsou uvedena v ustanovení upravujících tuto specifickou oblast (v rámci návrhu v mezirezortním připomínkovém řízení § 26 - § 27). Základním pravidlem je, že strategicky významné služby jsou podmnožinou regulovaných služeb ve vyšším režimu, bez ohledu na vztah ke kritické infrastruktuře. 4) MZe bude v režimu vyšších povinností, stejně jako všechna ostatní ministerstva a ústřední orgány státní správy. Připomínkové místo s vypořádáním souhlasí.
87. Ministerstvo zemědělství	Z	K § 2 vymezení pojmů Požadujeme definovat všechna pojmosloví, která jsou uvedena pod jinými paragrafy předloženého návrhu (např. dodavatel bezpečnostně významné dodávky, bezpečnostně významná dodávka (§ 32), nepominutelné funkce stanoveného rozsahu, kritické části stanoveného rozsahu (§ 28) a další. Požadujeme definovat slovní spojení „významný dopad“, který je citován v § 5, § 16 – 19. Je potřeba vymezit jak dlouho bude služba nedostupná, aby se jednalo o významný dopad, v jakém rozsahu bude narušena důvěrnost nebo integrita. Požadujeme přesnější definici regulované služby podle písm. e), neboť její určení je zásadní pro další postup pro řízení kybernetické bezpečnosti. Je potřeba vymezit „důležité společenské činnosti“, jedná se o vágní slovní spojení. Definice řízení kybernetické bezpečnosti podle písm. g), které se týká regulované služby, tedy omezeného rozsahu primárních aktiv, není v souladu s rozsahem řízení kybernetické bezpečnosti podle § 13, které zahrnuje primární aktiva celé organizace, tedy nejsou-li definovaná aktiva regulované služby, týká se řízení kybernetické bezpečnosti celé organizace, tedy zajištění kybernetické bezpečnosti	Neakceptováno Pro větší přehlednost byla připomínka rozdělena na tři části: 1. Významný dopad. Pojem významný dopad je v rámci zákona používán pro různé situace a pokaždé je vysvětlen v prováděcích předpisech. Významný dopad v definici regulované služby je definován kritérii pro identifikaci a určení regulované služby [§ X Kritéria regulované služby: 1) Regulovaná služba je stanovena kritérii pro identifikaci regulované služby ve vymezených odvětvích nebo kritérii pro určení regulované služby, která vymezují významnost dopadu služby na zabezpečení důležitých společenských nebo ekonomických činností. 2) Kritéria pro identifikaci a určení regulovaných služeb stanoví prováděcí právní předpis. (Vyhláška o regulovaných službách)]. 2. Významný dodavatel.

	všech primárních aktiv organizace. AR se musí dělat na všechna aktiva organizace nebo jen na aktiva regulované služby? Požadujeme upřesnit definici významného dodavatele podle odst. 2 písm. h) ve vztahu k dodavateli bezpečnostně významné dodávky podle § 28 odst. 3 písm. c), a to jak ve stanoveném rozsahu kybernetické bezpečnosti, tak v rozsahu aktiv týkajících se regulované služby nebo organizace jako celku. Měl předkladatel na mysli, že významný dodavatel je dodavatelem služeb nebo ICT produktů k zajištění provozu alespoň jedné regulované služby v režimu vyšších povinností nebo k zajištění strategicky významné služby?	Každá povinná osoba má trochu jiné procesy, proto byla zvolena cesta poměrně obecné definice významného dodavatele. Navíc povinné osoby jsou povinny si v politice řízení dodavatelů stanovit pravidla a principy pro jejich výběr, čímž mají možnost zohlednit v vlastní specifické požadavky na zajištění bezpečnosti. Dále jsme významného dodavatele rozvedli v samotném odůvodnění návrhu zákona. 3. Definice regulované služby Regulovaná služba je definována tímto konkrétním způsobem s ohledem na fakt, že až naplněním konkrétních kritérií, která jsou uvedena dále v zákoně a následně prováděcím právním předpise, se stává služba regulovanou. V definiční rovině jsou pro ni podstatné dva faktory, že je poskytována prostřednictvím aktiv, a že má určitou společensko-ekonomickou významnost. Ta je dána právě naplněním kritérií daných buďto zákonem či prováděcím předpisem. 4. Rozsah ISMS Definice řízení KB říká, že je to činnost směřující k zajištění KB regulované služby, tzn. zajištění regulované služby je hlavním cílem. Neznamená to však, že by rozsah nemohl být stanoven na celou organizaci, pokud to povinná osoba vyhodnotí jako vhodné, aby mohla KB regulované služby řádně zajistit. Dotčené ustanovení dále stanoví, že je třeba identifikovat primární aktiva organizace a z nich vybrat ta, která souvisí s regulovanou službou. Až nakonec pak identifikovat podpůrná aktiva související s primárními aktivy potřebnými pro regulovanou službu. Tedy organizace nebude evidovat a určovat

			veškerá aktiva organizace, ale toliko veškerá primární aktiva - tedy informace a služby. Rozsah je pak stanoven pouze na primární aktiva související s regulovanou službou a na ně navázána podpůrná aktiva. Připomínkové místo s vypořádáním souhlasí.
88. Ministerstvo zemědělství	Z	K § 4 odst. 2 Uvedené ustanovení zakotvuje oblasti, pro které prováděcí právní předpis stanoví kritéria pro identifikaci. Zahrnut je též potravinářský průmysl a vodní hospodářství. Požadujeme potvrdit, že uvedené vymezení odpovídá směrnici (CELEX 32022L2555). Návrh uvádí „potravinářský průmysl“ a „vodní hospodářství“, směrnice hovoří o výrobě, zpracování a distribuci potravin. Není pojem „potravinářský průmysl“ širší? Stejná připomínka platí pro oblast vody, kdy směrnice uvádí odvětví „pitné vody“ a „odpadní vody“, nikoli „vodní hospodářství“, jak navrhuje předložený zákon. Dále směrnice odkazuje na střední podniky a větší a je tedy potřeba prověřit, zda i zákon, respektive prováděcí předpisy, budou odkazovat jen na tyto kategorie (teze vyhlášky odkazují na velké a střední podniky).	Vysvětleno Názvy odvětví nejsou pro identifikaci poskytovatele stěžejní, tedy ani použití pojmu, který je v obecné řeči používán pro širší okruh osob, není pro definování okruhu povinných osob rozhodujícím faktorem. Stěžejní je vymezení služby a kritérií poskytovatele regulované služby. Názvy odvětví, stejně jako specifikace služeb a kritérií poskytovatele, jsou přizpůsobeny národním realitám a pojmům, se kterými pracují právní předpisy České republiky v daném odvětví. To platí pro obě citovaná odvětví, tedy vodní hospodářství i potravinářský průmysl. V částech, kde to není možné, se pak používají směrnice pojmy, které odraz v právním řádu ČR nemají. To je i případ kritérií poskytovatele regulované služby v odvětví potravinářského průmyslu, který je v návrhu vyhlášky definován v zásadě shodně jako ve směrnici NIS 2. Obě odvětví pak odpovídají vymezení regulovaných osob podle příloh směrnice NIS 2. Co se týče regulace středních a velkých podniků, tam, kde jde o regulaci vycházející z požadavků směrnice NIS 2, je regulace vztahována na subjekty definované podle velikostních kritérií (v souladu se směrnicí NIS 2). Tam, kde jde o národní úpravu (nad rámec směrnice NIS 2), jsou pak použita další dodatečná kritéria. Připomínkové místo s vypořádáním souhlasí.

89. Ministerstvo zemědělství	Z	K § 5 Požadujeme definovat systémová rizika uvedená v písm. a) bod 3.	Akceptováno Bude doplněna důvodová zpráva Připomínkové místo s vypořádáním souhlasí.
90. Ministerstvo zemědělství	Z	K § 5, písm. c) Nutno ujasnit formulaci. Předpokládá se, že závažný zásah do schopnosti poskytovat jednu službu poskytovatele regulované služby režimu vyšších povinností může vést k narušení i jiné služby téhož poskytovatele regulované služby nebo služby jiného poskytovatele regulované služby v režimu vyšších povinností? Pokud závažný zásah do schopnosti poskytovat službu „x“ poskytovatele regulované služby v režimu nižších povinností, která má dopad do služby poskytovatele regulované služby v režimu vyšších povinností, musí se „x“ poskytovatele regulované služby v režimu nižších povinností změnit na poskytovatele regulované služby v režimu vyšších povinností?	Vysvětleno Ustanovení § 5 písm. c) upravuje situaci, kdy narušení určité posuzované služby může způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu poskytovatele regulované služby v režimu vyšších povinností. Závažný zásah se přitom může týkat jak jiné služby toho stejného poskytovatele, tak služby jiného poskytovatele (vždy však poskytovatele v režimu vyšších povinností), což vyplývá přímo z textu ustanovení („způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu stejného nebo jiného poskytovatele“). Na základě kritérií podle § 5 určuje Úřad poskytovatele regulované služby svým rozhodnutím. Nejde přitom o automatický proces, Úřad řízení zahájí (z moci úřední), má-li důvod domnívat se, že by kritéria u konkrétní služby mohla být naplněna. Službou, u níž bude v řízení posuzováno naplnění kritérií podle § 5 písm. c), bude moci být jak služba zařazená vyhláškou o regulovaných službách do nižšího režimu, tak služba zařazená vyhláškou o regulovaných službách do vyššího režimu, ale také služba, která ve vyhlášce o regulovaných službách vůbec upravena není [na rozdíl od písmene a) nejsou kritéria pod písmeny b) až d) vázána na služby uvedené v prováděcím právním předpisu, může tedy jít o jakoukoli službu]. Reakce připomínkového místa:

			Není jasné, zda musí PRS-RVP hlásit cizí služby, které nejsou pod jeho správou a které mohou v případě narušení bezpečnosti způsobit závažný zásah do jeho RS? Reakce NÚKIB: Povinnost hlásit cizí regulované služby, které jsou regulovanou službou ovlivněny nebo které ovlivňují regulovanou službu, v zákoně není obsažena, nic takového poskytovatelé dělat nemusejí. Pokud Úřad bude chtít uvedené kritérium pro určení regulované služby využít, bude si takové informace sám zjišťovat (a v této fázi se může poskytovatele na tyto skutečnosti doptat). Poskytovatelé regulovaných služeb jsou povinni činit pouze to, co je v zákoně výslovně uvedeno. Připomínkové místo s vypořádáním souhlasí.
91. Ministerstvo zemědělství	Z	K § 7 Podle návrhu má poskytovatel pro všechny poskytované regulované služby stanoven jeden režim poskytovatele regulované služby. Je režim plnění poskytovatele strategicky významné služby (PSVS) stejné jako plnění poskytovatele regulované služby v režimu vyšších povinností? Požadujeme vyjasnit.	Vysvětleno Předkládaný zákon zná pouze dva režimy poskytovatele regulované služby, a to vyšší a nižší. Poskytování strategicky významné služby tak není režimem. Strategicky významné služby jsou speciální množinou regulovaných služeb, na které dopadají podle navrhovaného zákona některé další povinnosti. Ty ale poskytovatel strategicky významných služeb musí plnit pouze u strategicky významných služeb, nikoliv však u dalších regulovaných služeb, které případně může poskytovat. Připomínkové místo s vypořádáním souhlasí.
92. Ministerstvo zemědělství	Z	K § 13 odst. 1 písm. c) Podpůrná aktiva se identifikují a hodnotí jen k primárním aktivům regulované služby v souvislosti s následnou analýzou rizik? Proč je	Neakceptováno

		nutné určovat, tedy identifikovat, aktiva celé organizace? Je nutné hodnotit primární aktiva organizační části organizace, která nesouvisí s regulovanou službou? Požadujeme upřesnit a doplnit. Dále požadujeme doplnit i stanovený rozsah strategicky významné služby a definici kritické části stanoveného rozsahu strategicky významné služby z § 28 3 a). Informace o vymezení služeb je nutné rozlišit a definovat na jednom místě zákona.	Stanovený rozsah se vztahuje na aktiva související s regulovanou službou (nikoliv všechna identifikovaná primární aktiva - pokud tedy všechna nesouvisí s regulovanou službou). Pracuje se s typovými aktivy, nikoliv s každou službou/informací jako takovou zvlášť. Jde o základní identifikaci služeb, které organizace poskytuje (za jakým účelem je vytvořena a co jsou její <i>core</i> služby). Primární aktiva, která nesouvisí s regulovanou službou není potřeba hodnotit (návrh zákona to nepožaduje). Nepovažujeme tuto změnu při identifikaci aktiv za nepřiměřenou Je pravda, že v tomto ustanovení se projevují zkušenosti Úřadu z kontrolní činnosti, kdy správně stanovit rozsah ISMS organizacím způsobuje značné problémy. Oproti platné právní úpravě došlo k otočení způsobu identifikace primárních aktiv, na které se nyní pohlíží z pohledu celé organizace a určují se ty, které souvisejí s regulovanou službou. Nesouhlasíme s tím, že pro zajištění Kybernetické bezpečnosti současné znění předmětného ustanovení nebude mít vliv a že se jedná o nepřiměřený zásah do práv povinných subjektů. Naopak naší snahou je zmírnění požadavku NIS2 zavádět opatření na celou organizaci v tom smyslu, že se první podívám na celou organizaci, ale opatření zavádím na těch aktivech, které se přímo dotýkají poskytování regulované služby. K návrhu na doplnění strategicky významné služby uvádíme následující - pokud je tím myšleno jejich doplnění do definic, tak v zákoně jsou uvedeny ty definice, které jsou používané napříč zákonem, ostatní pojmy jsou definovány v rámci částí návrhu zákona, pro které jsou relevantní.

			Připomínkové místo s vypořádáním souhlasí.
93. Ministerstvo zemědělství	Z	K § 13 odst. 3 Jestliže je řízení kybernetické bezpečnosti definováno jako činnosti k zajištění kybernetické bezpečnosti regulované služby (nejde o stanovený rozsah, ale rozsah související s regulovanou službou), proč je rozsah řízení kybernetické bezpečnosti (=stanovený rozsah) definován primárními aktivy celé organizace? Proč se musí určovat a evidovat všechna primární aktiva, která nesouvisí s poskytovatelem regulované služby. Je to neúměrná zátěž pro organizaci. 1. primárními aktivy regulované služby jsou a) souvisejícími s poskytováním regulované služby, b) souvisejícími s organizační částí organizace, c) souvisejícími podpůrná aktiva 2. primárními aktivy organizační části organizace, které lze po zdůvodnění vyjmout ze stanoveného rozsahu? Nutno upřesnit jaká primární aktiva a za jakých podmínek lze ze stanoveného rozsahu aktiva vyjmout a co to obnáší (vyjmutá aktiva se nehodnotí? Jaká jsou akceptovatelná zdůvodnění? Je možné z rozsahu řízení kybernetické bezpečnosti ŘKB vyjmout ta aktiva, která nesouvisí se zajišťováním regulované služby?	Vysvětleno Dle směrnice NIS2 měl být rozsah řízení KB stanoven na celou organizaci, aby NÚKIB neúměrně nezatěžoval povinné subjekty, rozhodl se umožnit vyjmout z rozsahu primární aktiva, která s regulovanou službou nesouvisí. Definice řízení KB podle písm. g) říká, že je to činnost směřující k zajištění KB regulované služby, tzn. zajištění regulované služby je hlavním cílem, neznamená to však, že by rozsah nemohl být stanoven na celou organizaci, pokud to povinná osoba vyhodnotí jako vhodné, aby mohla KB regulované služby řádně zajistit. Dále § 13 odst. 1 říká následující: je nutné identifikovat všechna primární aktiva [písm. a)], následně identifikovat ta, která souvisí s regulovanou službou [písm. b)] a nakonec identifikovat podpůrná aktiva související s primárními aktivy potřebnými pro regulovanou službu [písm. c)]. Rozsah je stanoven pouze na aktiva dle písm. b) a c), tedy na primární aktiva související s regulovanou službou a na ně navázána podpůrná aktiva. Není tedy pravda, že by dle § 13 odst. 2 rozsah tvořila všechna aktiva. Nesouhlasíme s tím, že to bude administrativně zatěžující, bude se jednat o primární aktiva v množství jednotek a jednoduchého zdůvodnění (např. nesouvisí s regulovanou službou). Pracuje se s typovými aktivy, nikoliv s každou službou/informací jako takovou zvlášť. Jde o základní identifikaci služeb, které organizace poskytuje (za jakým účelem je vytvořena a co jsou její core služby). Vše slouží k tomu, aby bylo možné ověřit, zda byl rozsah stanoven správně. Ze zkušeností z kontrol vyplývá, že povinné osoby mají

			rozsah stanoven nesprávně, proto bylo ustanovení zpřesněno. Hodnocení aktiv a rizik se vždy provádí ve stanoveném rozsahu. Připomínkové místo s vypořádáním souhlasí.
94. Ministerstvo zemědělství	Z	K § 16 odst. 1 (ve vazbě na § 18 odst. 2, § 19 odst. 1) Požadujeme slovní spojení „všechny incidenty“ nahradit slovním spojením „incidenty, které mají původ v kybernetickém prostoru a mají významný dopad“. V návrhu se uvádí: „...povinností v rámci stanoveného rozsahu je hlásit všechny kybernetické bezpečnostní incidenty,....“ Opravdu se má jednat o všechny? Jde jak o administrativní zatěžování poskytovatele regulované služby v režimu vyšších povinností, tak zahlcení Úřadu bezpečnostními incidenty Měla by se proto upřesnit definice kybernetického bezpečnostního incidentu. Podle stávající definice patří mezi kyberneticko bezpečnostní incidenty i provozní incidenty např.: došlo po 1 hodině k nedostupnosti služby z důvodu chyby v nastavení. Podle § 18 odst. 2 Úřad poskytuje metodickou a případně technickou podporu jen ke zvládnutí kyberneticko-bezpečnostních incidentů s významným dopadem. Podle § 19 odst. 1 poskytovatel regulované služby oznámí bez zbytečného odkladu uživatelům regulované služby kyberneticko-bezpečnostní incident s významným dopadem.	Akceptováno jinak Na základě připomínky byla povinnost hlášení omezena na všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a nejsou způsobeny vlastní provozní činností. Poskytovatelé regulované služby v režimu nižších povinností hlásí pouze kybernetické bezpečnostní incidenty s významným dopadem, poskytovatelé regulované služby ve vyšším režimu hlásí všechny kybernetické bezpečnostní incidenty. Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob. Připomínkové místo s vypořádáním souhlasí.
95. Ministerstvo zemědělství	Z	K § 17 odst. 1 Navrhovaný režim předložení do 24 hodin je pro Ministerstvo zemědělství neakceptovatelný. V případě zjištění incidentu v pátek odpoledne, nelze předložit do 24 hodin. Nejsme vybaveni provozem	Neakceptováno Lhůta pro hlášení incidentů je vázána na okamžik zjištění tohoto incidentu, který se nemusí shodovat s

		24 x 7. U složitějších problémů nemusíme být schopni předložit informace do 24h o detailech incidentu způsobeným nezákonným nebo svévolným zásahem s přeshraničním dopadem.	reálným časem, kdy incident skutečně nastal. Pokud tedy incident nastane např. v sobotu, ale je nahlášen až v pondělí bezodkladně po tom, co se o něm příslušný zaměstnanec dozvěděl, je zákonná povinnost splněna. Takto stanovená lhůta má zajistit případnou rychlou reakci Vládního CERT, příp. Národního CERT při řešení incidentu a napomoci navazujícím preventivním či analytickým aktivitám Vládního CERT, příp. Národního CERT. Obsahové náležitosti prvotního hlášení jsou omezeny na nezbytné minimum, díky kterému bude Vládní CERT schopen posoudit, zda má incident významný dopad na kybernetický prostor státu, a zároveň by předání těchto informací nemělo představovat pro ohlašovatele nadměrnou administrativní zátěž. Poskytovatelé regulované služby v režimu nižších povinností hlásí pouze kybernetické bezpečnostní incidenty s významným dopadem, poskytovatelé regulované služby ve vyšším režimu hlásí všechny kybernetické bezpečnostní incidenty. Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob. Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnici

			NIS 2, tzn. pokud bychom do zákona nezahrnuli požadavek na lhůtu, která je podle čl. 23 odst. 4 písm. a) směrnice NIS 2 stanovena na "bez zbytečného odkladu, nejpozději však do 24 hodin po zjištění", byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Z uvedeného důvodu národní právní úprava tento požadavek kopíruje. Připomínkové místo s vypořádáním souhlasí.
96. Ministerstvo zemědělství	Z	K § 26, § 27, § 41 odst. 3 písm. c), § 2 odst. 2 j) Strategicky významná služba je regulovaná služba. Toto začlenění v textu zákona pod samostatný oddíl 4 je matoucí. 1. Požadujeme obsah § 26 - 27 o poskytovateli strategicky významné služby zařadit za § 7. Poskytovatel strategicky významné služby je poskytovatel regulované služby v režimu vyšších povinností. Od regulované služby se liší se závažností dopadu a dalšími povinnostmi, což je možné upřesnit odkazem na příslušné oddíly (díly 5 a 6). 2. Požadujeme upřesnit následující: Podle § 27 je celá veřejná správa automaticky zařazena mezi poskytovatele strategicky významné služby. Podle § 41 odst. 3 c) je § 27 odst. 2 rozhodnutím NÚKIB o určení poskytovatele strategicky významné služby. Podle definice poskytovatele strategicky významné služby (§ 2 odst. 2 písm. j) je poskytovatel regulované služby, který poskytuje jednu nebo více strategicky významných služeb, podle § 2 odst. 2 písm. j). Není jasné, která regulovaná služba je strategicky významnou službou. 3. Pokud orgán neurčí žádnou jím poskytovanou regulovanou službu jako strategicky významnou na základě uvedených kritérií pro určení strategicky významné služby, má takový orgán zažádat o vyjmutí z evidence poskytovatele strategicky významné služby? Ze zákona není patrné, na základě jakých kritérií Úřad určuje strategicky významné služby.	Ad 1. Neakceptováno - nyní § 27 a 28. Zařazení strategicky významné služby je ovlivněno tím, že na její určené přímo navazují již zmíněné povinnosti. Tím nijak neodporuje logice zákona v tom, že strategicky významná služba je zároveň službou regulovanou (a že jí z toho plynou další povinnosti, které jsou zase systematicky zařazeny do zákona za část určující regulované služby). Ad 2. Vysvětleno - nyní § 28. Celá veřejná správa nespadá automaticky mezi strategicky významné služby. Veřejná správa je jednou z oblastí, ze které mohou být strategicky významné služby určeny, pokud naplní kritéria. Ta jsou následně uvedena v prováděcím právním předpise – Vyhláše o regulovaných službách. Ad 3. Vysvětleno. V případě, že orgán neposkytuje žádnou strategicky významnou službu, nebude veden v evidenci poskytovatelů strategicky významných služeb. Pro účely veřejné správy jsou kritéria uvedena ve tezi vyhlášky o regulovaných službách. Konkrétně se jedná o službu uvedenou v příloze č. 2 k této vyhlášce, kap. 1, oddíl 1.1 – Výkon svěřených pravomocí ve spojitosti s §5 písm. a, které taxativně vyjmenovávají ty orgány veřejné správy, které jsou

			považovány za poskytovatele strategicky významné služby. Reakce připomínkového místa: Nenašli jsem kritéria pro určování, jen pro identifikaci SVS. Podle jakých kritérií se řídí Úřad při určování SVS (Jak dělá BIA na RS?) Reakce NÚKIB: Kritéria pro identifikaci jsou obsahem budoucí vyhlášky o regulovaných službách, jejíž teze byly rozeslány v meziresortním připomínkovém řízení. Kritérium pro určení je obsaženo v § 28 odst. 1 písm. b): Strategicky významnou službou je regulovaná služba určená rozhodnutím Úřadu v případě, že by její narušení mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek. Kritériem je tedy to, že by narušení regulované služby mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek. Jedná se o kritérium sice obecné, avšak vyčerpávajícím způsobem pokrývající potenciální množinu služeb, které v současné době nejsou zahrnuty mezi strategicky významné služby (ať už proto, že například neexistují, nebo proto, že z jakýchkoliv jiných důvodů není jejich důležitost na takové úrovni, aby mezi ně zahrnuty byly). V rámci vyváženosti je pak samozřejmě nutné dodat, že se v případě určení služby podle tohoto kritéria jedná o víceméně standardní správní řízení a rozhodování, ve kterém jsou šetřena všechna práva jeho účastníků. Reakce připomínkového místa: Přesto nám však zbývá jedna zásadní otázka, již je podle nás nutno vyjasnit a ohledně níž náš rozpor

			trvá, a to obsah pojmu „strategicky významná služba“ (SVS), resp. jeho normativní ukotvení. V § 2 odst. 2 písm. i) návrhu zákona se obecně uvádí, že „<i>strategicky významnou službou (je) regulovaná služba, jejíž narušení by mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek</i>“ Podle § 28 odst. 1 písm. a) návrhu zákona je ústřední orgán státní správy poskytovatelem strategicky významné služby (PSVS), pokud „<i>naplňuje alespoň jedno kritérium pro identifikaci strategicky významné služby uvedené ve vyhlášce Úřadu v odvětvích 1. veřejná správa,...</i>“ V § 28 odst. 2 návrhu zákona je pak uvedeno jediné kvantitativní kritérium toho, co má být považováno za SVS, a co by tedy mělo být uvedeno ve vyhlášce, avšak opět velmi obecně („<i>Kritéria pro identifikaci strategicky významné služby zohledňují významnost dopadu narušení regulované služby na bezpečnost České republiky nebo vnitřní či veřejný pořádek.</i>“). O mnoho více se o charakteru předpokládaných SVS nedozvíme ani z důvodové zprávy k § 2 (str. 99): „<i>Strategicky významnou službou se rozumí pouze ta z regulovaných služeb, jejíž narušení bezpečnosti by mohlo vést k významnému omezení či ohrožení služeb pro občany státu a chod státu a současně s tím u nich hrozí vysoké riziko, že při narušení jejich poskytování bude negativně ovlivněn chod dalších regulovaných služeb. Jak současně vyplývá z ustanovení o kritériích strategicky významné služby, konkrétní strategicky významné služby jsou stanoveny buď na základě kritérií pro jejich identifikaci, nebo rozhodnutím Úřadu, a to za podmínek vymezených v daném ustanovení. Návrh zákona tedy vlastní definici strategicky významné služby doplňuje</i>

			<i>základními pravidly vyhodnocení významnosti omezení či ohrožení služeb pro občany státu a chod státu. “</i> Rozpor MZe v této věci proto nadále trvá. MZe je toho názoru, že je nutno normativně lépe ukotvit kritéria pro určení SVS pomocí průřezových nebo dopadových (či jiných specifitějších kvantitativních) kritérií např. na podobném principu, jaký byl stanoven například nařízením vlády č. 432/2010 Sb. v jeho § 1 nebo v příloze, odvětví VI., oblast G). Je nutné ujasnit, jak máme strategicky významnou službu v praxi určit, protože jediné kvantitativní kritérium v § 28 odst. 2 (a § 2 odst. 2 písm. i)) je nejednoznačné a příliš obecné a nelze podle něj v praxi určit, které z regulovaných služeb mají být strategicky významnou službou, a není pak ani jasné, podle jakých kritérií to bude následně určovat Úřad. Například veškeré dotační systémy nebo evidenční systémy ministerstev, které následně slouží dotačním systémům jsou regulovanými službami v návaznosti na ekonomické činnosti. Jsou však/měly by být automaticky regulovanými službami, jejichž narušení by mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní a veřejný pořádek a tedy strategicky významnou službou? Závěr: Po vypořádací schůzce připomínkové místo od rozporu ustoupilo a s vypořádáním souhlasí.
97. Ministerstvo zemědělství	Z	K § 28 Požadujeme přepracovat formulaci za účelem jasného pochopení textu.	Vysvětleno - nyní § 29 Uvedené ustanovení bylo daným způsobem napsáno záměrně, jelikož stanovený rozsah je institut upraven

		Uvádí se: „Kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby..“ a jazykově nevhodné „... stanoveného rozsahu stanovené...“. Stále se opakující „stanovený rozsah“. Např.: <i>Kritickou částí jsou aktiva, kterými je stanoven rozsah strategicky významné služby, jejichž hodnota dopadu v případě narušení bezpečnosti je vysoká nebo kritická. Jde zpravidla o aktiva, která zajišťují nepominutelné funkce definované v prováděcím právním předpisu.</i> Kde se v zákoně stanoví rozsah strategicky významné služby. Dále je potřeba ujasnit rozsah vztahu. Vhodné upřesnit rozsahu vztahu strategicky významné služby k regulované službě. Např.: <i>Rozsah aktiv k zajištění SVS odpovídá rozsahu aktiv k zajištění všech regulovaných služeb nebo je jeho podmnožinou.</i> Požadujeme vysvětlit a případně přeformulovat odst. 3 písm. a), který je s ohledem na výše uvedené zcela nesrozumitelný.	§ 13 odst. 2. Tento odstavce stanovuje, že organizační části a aktiva určená podle § 13 odstavce 1 písm. b) a c) tvoří rozsah řízení kybernetické bezpečnosti, pro který se dále v návrhu zákona používá označení "stanovený rozsah". Takový stanovený rozsah pak může mít svou kritickou část či svá aktiva dle jednotlivých ustanovení § 29. NÚKIB samozřejmě plánuje do budoucna v případě, že taková nutnost vyvstane, provést metodické vysvětlení. Toto vysvětlení však pro svou technickou šíři nemůže být součástí návrhu zákona. Připomínkové místo s vypořádáním souhlasí.
98. Ministerstvo zemědělství	Z	K § 30, 32 a 33 V textu se uvádí, že Úřad vydá opatření obecné povahy. Navrhujeme změnit text na „Úřad je oprávněn vydávat opatření obecné povahy“. Jako formu budou mít podmínky bezpečnostních opatření v opatření obecné povahy? Budou se k opatření obecné povahy moci vyjadřovat i poskytovatelé strategicky významné služby, kteří nepatří mezi dotčené osoby? V § 33 požadujeme doplnit povinnosti a postupy poskytovatele strategicky významné služby k plnění opatření obecné povahy. Úprava by například mohla znít následovně: a) v případě zákazu využití plnění: aa) vypoví smlouvu s dodavatelem, ba) vyloučí dodavatele z výběrového řízení, ca) zažádá NÚKIB o výjimku, pokud by plnění opatření obecné povahy poskytovatelem strategicky významné služby mohlo podstatným způsobem ohrozit poskytování strategicky významné služby, b) v případě stanovení podmínek v opatření obecné povahy:	Neakceptováno - nyní § 31, 33 a 34 Navrhovaný § 31 odst. 1 je formulován tak, aby uložil NÚKIB povinnost vydat předmětné opatření obecné povahy, pakliže jsou splněny předpoklady pro jeho vydání; klade se tak důraz na rovnost přístupu NÚKIB ke všem orgánům a osobám a absenci opportunity při vydávání opatření. Obdobná formulace je obsažena již v § 12 a 13 stávajícího zákona o kybernetické bezpečnosti. Co se týče formy podmínek stanovených opatřením, budou součástí výroku opatření obecné povahy a budou tedy sdílet jeho formu. Připomínky k návrhu opatření obecné povahy mohou v souladu s obecnou právní úpravou správního řádu podávat všechny orgány a osoby, které mohou být opatřením dotčeny; NÚKIB nadto vyzve všechny jemu známe dotčené osoby a dodavatele, že mohou

		ab) zohlední podmínky plnění v dodatku smlouvy s dodavatelem, bb) zohlední nové podmínky ve veřejných zakázkách, cb) zažádá NÚKIB o výjimku, pokud by plnění opatření obecné povahy poskytovatelem strategicky významné služby mohlo podstatným způsobem ohrozit poskytování strategicky významné služby, c) v případě povolení uplatnění výjimky a stanovení podmínek: ab) a bb) c) v případě nepovolení výjimky: aa) a ba) d) v případě zrušení opatření obecné povahy nebo pominutí důvodu povolení výjimky: ad) zrušení dodatku smlouvy s dodavatelem opírajícího se opatření obecné povahy, bb)? Je nezbytné, aby zákon o veřejných zakázkách umožňoval zohlednit nová bezpečnostní opatření plynoucí z opatření obecné povahy v průběhu zakázkového řízení.	připomínky uplatnit. Subjekty, které nemohou být opatřením dotčeny, připomínky k jeho návrhu nepodávají. Doplnění výčtu povinností, které mohou být poskytovateli strategicky významné služby uloženy, není vhodné, jelikož mohou tyto v závislosti na identifikované hrozbě nabývat různé podoby a jakýkoliv výčet by byl nezbytně pouze demonstrativní; stávající podoba navíc vychází z obvyklé podoby zmocnění k vydávání opatření obecné povahy, jak je uvedeno např. v současném zákoně o kybernetické bezpečnosti nebo ve stavebním zákoně. Ve vztahu k zadávání veřejných zakázek pak může zadavatel vyloučit za zadávacího řízení uchazeče podle § 48 odst. 2 zákona o zadávání veřejných zakázek, včetně případné změny zadávacích podmínek dle § 99 téhož zákona - tento postup byl konzultován také s Úřadem pro ochranu hospodářské soutěže a s Ministerstvem pro místní rozvoj jakožto garantem zákona o zadávání veřejných zakázek a oběma orgány byl shledán jako obecně souladný s právními předpisy. Připomínkové místo s vypořádáním souhlasí.
99. Ministerstvo zemědělství	Z	K § 32 Požadujeme upřesnit, zda souvisí bezpečnostně významné dodávky jen s poskytováním strategicky významné služby? Je-li veřejná správa poskytovatelem pouze jedné strategicky významné služby a dalších regulovaných služeb, podává hlášení pouze o dodavatelích a dodávkách k jedné strategicky významné službě? Jedná se o náhradu hlášení o provozovateli kritické informační infrastruktury nebo významného informačního systému? Jak tito dodavatelé bezpečnostně významné dodávky souvisí s významnými dodavateli uvedenými v § 25 návrhu zákona?	Vysvětleno - nyní § 33 <i>Požadujeme upřesnit, zda souvisí bezpečnostně významné dodávky jen s poskytováním strategicky významné služby?</i> Ano, souvisí pouze s poskytováním strategicky významné služby, ale povinnosti mohou dopadnout na více služeb, nejen na kritérium, na základě kterého byla služba identifikována jako strategicky významné služba, o tomto zaražení bude poskytovatel strategicky

		významné služby informován, viz nově upravené znění původního § 28 návrhu zákona. <i>Je-li veřejná správa poskytovatelem pouze jedné strategicky významné služby a dalších regulovaných služeb, podává hlášení pouze o dodavatelích a dodávkách k jedné strategicky významné službě?</i> Ano, hlášení vždy podává pouze k té službě, u které jsou naplněna kritéria pro strategicky významnou službu, nicméně hlášení je nutné podat vždy k celé této službě. <i>Jedná se o náhradu hlášení o provozovateli kritické informační infrastruktury nebo významného informačního systému?</i> Jedná se o částečnou náhradu, spíše jde o evoluci systému. Odstupuje se od původního dělení na správce a provozovatele, návrh zákona reguluje pouze poskytovatele služby. Poskytovatelům služby následně vzniká povinnost hlásit bezpečnostně významné dodavatele a dodávky do kritické části strategicky významné služby. <i>Jak tito dodavatelé bezpečnostně významné dodávky souvisí s významnými dodavateli uvedenými v § 25 návrhu zákona (nyní § 26)?</i> Nelze vyloučit, že návrh zákona dopadne i na významné dodavatele, nicméně nelze vyloučit, že významný dodavatel §2 odst. 2 písm. h) nebude současně i dodavatelem bezpečnostně významné dodávky podle §29 odst. 3 písm. c). Jedná se o jiný přístup ve vztahu vztažení regulace na dodavatele a stanovení jejich povinností, povinnosti budou stanoveny ve Vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších

			povinností. Je třeba zajistit bezpečnost dodavatelů, protože skrze ně je nastavena celková úroveň bezpečnosti poskytované služby. Připomínkové místo s vypořádáním souhlasí.
100. Ministerstvo zemědělství	Z	K § 40 odst. 1 c) Požadujeme vyjasnit: Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je oprávněn vyžádat si na základě smlouvy nebo zápisu o sdílení personálních kapacit a věcných prostředků přednostní poskytnutí personálních kapacit nebo věcných prostředků ... - o jaký smluvní vztah nebo zápis se má jednat? Požadujeme doplnit odkaz na právní předpis, který se uzavření takové smlouvy nebo zápisu stanoví. Povinnost vyhovět žádosti Národního úřadu pro kybernetickou a informační bezpečnost o personální kapacity nebo věcné prostředky není v souladu s poskytnutím na základě smlouvy nebo zápisu o sdílení. Jak mají být uzavírány smlouvy nebo vytvářeny zápisy o sdílení personálních kapacit a věcných prostředků?	Vysvětleno - nyní § 41 odst. 1 písm. c) Bude se jednat o inominátní smlouvu uzavřenou podle občanského zákoníku. Tyto smlouvy budou uzavírány zejména s ostatními státními orgány, které se určitým způsobem na zajišťování kybernetické bezpečnosti podílejí a případně také s provozovatelem Národního CERT. Jde o prostředek k tomu, jak mít pro případ zhoršené situace k dispozici vhodné odborníky či materiál, který není běžně ve vlastnictví Úřadu. Ustanovení bylo zároveň významně přeformulováno ve spolupráci s gestorem krizového řízení Ministerstvem vnitra - Generálním ředitelstvím hasičského záchranného sboru tak, aby opatření za stavu kybernetického nebezpečí nebyla nástrojem vyhrazeným krizovým stavům dle příslušného předpisu, tedy aby nedocházelo k omezování vlastnického práva. Proto je podmínkou aplikace tohoto opatření smluvní vztah. Připomínkové místo s vypořádáním souhlasí.
101. Ministerstvo zemědělství	Z	K § 40 odst. 1 d) Komu může Úřad nařídít práci v pohotovostním režimu? Jaká bude procesně vypadat takové nařízení pohotovosti podle § 40 návrhu zákona?	Akceptováno - nyní § 41 odst. 1 písm. e) Ustanovení bylo upraveno a zpřesněno na základě jednání s gestorem krizového řízení - Ministerstvem vnitra - Generálním ředitelstvím hasičského záchranného sboru. Pohotovostní režim a jeho nařízení je opět podmíněn předchozím smluvním ujednáním.

			Připomínkové místo s vypořádáním souhlasí.
102. Ministerstvo zemědělství	Z	K § 40 odst. 1 h) S navrženou úpravou nesouhlasíme. Podle návrhu je Národní úřad pro kybernetickou a informační bezpečnost oprávněn nařídit orgánům a osobám zpřístupnění neveřejných komunikačních sítí v jejich správě pro potřeby Úřadu. Zpřístupnění neveřejných komunikačních sítí ve správě orgánu vyžaduje soulad s interní bezpečnostní politikou orgánu, například přístupy přes bezpečnostní nástroje apod.	Vysvětleno - nyní § 41 odst. 1 písm. h) Zpřístupněním neveřejné sítě v tomto případě není mířeno na její primární užívání Úřadem, nicméně jen jako užívání podpůrné, které bude zpravidla zahrnovat pouze posílání informací a to v případě, že takové informace nebude možné doručit dostatečně rychlým způsobem jinak (jde tak z pravidla o situaci, kdy jsou nedostupné veřejné komunikační sítě). Prakticky se tak nemusí stát, aby Úřad měl do takové sítě přístup, nicméně postačí aby mu byla zpřístupněna zprostředkovaně, případně pokud bude zpřístupněna pouze ta část sítě, která je nezbytná k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru za stavu kybernetického nebezpečí. Bezpečnostní politiky mohou tuto variantu zohledňovat, nicméně nejedná se o nikterak standardní postup a vždy až o poslední variantu. Připomínkové místo s vypořádáním souhlasí.
103. Ministerstvo zemědělství	Z	K příloze vyhlášky č. 19. Věda, výzkum a vzdělávání Vědeckovýzkumné instituce budou podle kritérií vyhlášky o regulovaných službách zařazeny do režimu vyšších povinností. Požadujeme upravit kritéria pro zařazení do příslušného režimu, protože pro řadu vědeckovýzkumných institucí bude režim vyšších povinností finančně nezvladatelný. Souhlasili bychom s kompromisním řešením, kdy vědeckovýzkumné instituce budou zařazeny do režimu nižších povinností. Nabízí se též řešení, kdy pro zařazení do příslušného režimu by mělo být vyhodnoceno, o jak strategický výzkum se jedná a podle toho by se příslušná vědeckovýzkumná instituce zařazovala do odpovídajícího režimu. Je rozdíl, zda výzkumná činnost má dopad na zemědělské činnosti anebo dopad na bezpečnost státu, zdraví osob a strategické technologie.	Akceptováno jinak Došlo k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji. Připomínkové místo s vypořádáním souhlasí.

		Pro vědeckovýzkumné instituce Ministerstva zemědělství není pro zařazení do vyšších povinností relevantní ani citlivý výzkum, ani skutečnost, že většina prováděných výzkumných projektů je financována z více než 50 % z veřejných zdrojů. Čistě výzkumnou činností není možné ufinancovat navýšené náklady, které zákon o kybernetické bezpečnosti přináší. Návrh zákona by měl zapracovávat požadavky směrnice NIS 2 do českého právního řádu jako kompromis balancující mezi potřebou regulovat všechna podstatná odvětví a objektivní schopností členských států zajistit reálný výkon pravidel obsažených v transpozičních národních předpisech. Návrh zákona z povahy věci zasahuje do práv adresátů normy a je proto koncipován na tzv. dvourychlostním modelu kybernetické bezpečnosti. Poskytovatelé regulované služby jsou v rámci návrhu zákona proto rozděleni do dvou režimů – nižších a vyšších povinností. Zahrnutí nekomerčních výzkumných organizací do národní regulace však představuje národní úpravu nad rámec požadavků směrnice NIS2, i dle důvodové zprávy je relevance výzkumných organizací zaměřených na nekomerční užití výsledků z pohledu bezpečnosti vnitřního trhu nižší. Nicméně výzkumná organizace, jejímž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj za účelem využití tohoto výzkumu pro komerční účely, vysoká škola nebo jiná výzkumná organizace je navržena jako poskytovatel regulované služby v režimu vyšších povinností v případě, že provádí citlivou výzkumnou činnost, nebo většina prováděných výzkumných projektů je financována z více než 50 % z veřejných zdrojů. A díky tomu, že drtivá většina prováděných výzkumných projektů resortních v.v.i. je financována z více než 50 % z veřejných zdrojů, měli by tyto v.v.i. spadat automaticky do režimu vyšších povinností. A to je zásadní problém. Resortní výzkumné organizace Ministerstva zemědělství neprovádí citlivé výzkumné činnosti, neprovozují velké výzkumné infrastruktury, ani nespádají pod Akademii věd. Primárním cílem jejich existence je provádět nezávisle především aplikovaný zemědělský výzkum a experimentální vývoj a veřejně šířit výsledky těchto činností formou výuky, publikací nebo transferu znalostí.	

		Zásadní a zřejmě neznámou informací pro navrhovatele je fakt, že všechny náklady, které přímo souvisí s výzkumnou činností, jsou účtovány přímo k projektům, k nimž patří. Kromě přímých nákladů vznikají v souvislosti s výkonem činností i náklady nepřímé (tzv. režijní), které z jejich podstaty nelze přiřadit přímo. Do režijních nákladů se započítávají náklady spojené se zajištěním provozu objektu instituce (elektrická energie, zemní plyn, vodné, stočné, povinné revize, daň z nemovitosti, ostraha), osobní náklady zaměstnanců zajišťujících řízení a provoz instituce, materiálové náklady zaměstnanců zajišťujících řízení a provoz instituce, odpisy investičního majetku, poštovné, telekomunikační poplatky, pojištění majetku, bankovní poplatky a samozřejmě i náklady na IT infrastrukturu včetně zajištění její bezpečnosti. Přípustná výše nepřímých nákladů se liší dle typu projektu a poskytovatele, většinou je ale ve výši 20 % z celkových či 25 % z přímých nákladů projektu. V posledních letech je ale snahou poskytovatelů účelové podpory režijní náklady snižovat, přibývají povinnosti podle nových právních předpisů. Důvodová zpráva uvádí velmi hrubé odhady nákladů na zavedení a následné provádění bezpečnostních opatření pohybující se přibližně mezi 800 000 Kč a 1 500 000 Kč vůči jednomu zabezpečovanému systému. Dále uvádí, že podstatnou proměnnou celkových nákladů bude především to, jaký je daný počet jednotlivých systémů u každé konkrétní organizace a také skutečnost, že takový násobek výše uvedené částky bude potřeba daným organizacím alokovat v rámci veřejných rozpočtů. To však není v rámci v.v.i. principiálně reálné a proveditelné. A je tedy zcela mimo objektivní schopnost resortních organizací zajistit reálný výkon stanovených požadavků. Pro představu v rámci běžné v.v.i. může jít přibližně o 20 systémů, tedy náklady dle odhadů NÚKIB někde mezi 16 až 30 mil. Kč. Realitou je však také nižší vyspělost resortních v.v.i. v kybernetické bezpečnosti obecně (dosud jsou v tomto ohledu bez regulace), z čehož se dá odhadnout, že náklady na jejich zabezpečení budou spíše odpovídat vyšším odhadům NÚKIB. Pro představu uvádíme příklad	

		jedné typické rezortní organizace – celkový rozpočet organizace pod 100 mil. Kč, rozpočet režijních nákladů cca 20,6 mil. Kč a se současnými náklady vynakládané na kompletní zajištění IT infrastruktury cca 4 mil. Kč ročně.	
104. Ministerstvo zemědělství	D	Vymezení pojmů není vždy srozumitelné, jednoznačné a úplné z pohledu jejich dalšího užití v textu zákona. Dáváme ke zvážení, zda by užívané abstraktní právní pojmy neměly být alespoň příkladmo obsahově vymezeny v důvodové zprávě. Užívá se např. pojmu v § 5 „závažný zásah“, v § 2 a 5 aj. pojmu „významný dopad“. Členění jednotlivých paragrafů, jejich názvů a zejména obsahu je v řadě případů neuspořádané, nelogické a jejich návaznost není věcně kontinuální, vykazuje mnohdy obtížnou orientaci v dané problematice. V návrhu jsou zakotveny rozsáhlé povinnosti Poskytovatele regulované služby vůči Úřadu, které musí být (pod sankcemi) zajištěny (v režimu vyšších a v režimu nižších povinností), a to za stávajících personálních, finančních a kapacitních podmínek na jednotlivých ústředních orgánech státní správy. Mnohdy jsou ukládané povinnosti v rozsahu, který není nezbytně nutný a vykazuje znaky formalismu.	Akceptováno jinak Přístup k výkladu neurčitých právních pojmů použitých v dotčeném ustanovení návrhu zákona byl doplněn do důvodové zprávy v tom smyslu, že jejich obecná definice není právě s ohledem na jejich charakteristiku coby neurčitých právních pojmů a současně univerzální aplikovatelnost na skutkově zcela odlišné situace žádoucí (nadto např. pojem významný dopad je v rámci zákona používán pro různé situace a v závislosti na místě jeho použití nabývá v jednotlivých částech zákona odlišných významů). Jakákoli definice, o kterou by se předkladatel návrhu zákona pokusil, by z povahy věci musela poměrně obecná (aby pokryla všechny zamýšlené situace) a nepřinášela by adresátům normy žádnou přidanou hodnotu. Tam, kde je to možné a vhodné, jsou pojmy buďto vysvětleny v prováděcích předpisech, nebo jsou blíže přiblíženy v důvodové zprávě. Bližší výklad těchto pojmů pak bude prováděn v závislosti na konkrétních skutkových okolnostech posuzovaného případu. Obecně však tyto pojmy slouží k vydefinování situací, které dosahují natolik významné intenzity, že stát považuje za nezbytné je podřadit pod zákonnou regulaci. Co se týče připomínky ke zmatečnosti členění návrhu zákona, z připomínky není zřejmé, co konkrétně pisatel považuje za neuspořádané nebo nelogické. Můžeme doplnit, že návrh je koncipován s ohledem na

		jeho uživatele - čitatele tak, aby je provedl celou regulací kybernetické bezpečnosti od vysvětlení pojmů, přes způsob zařazení osob do regulace, stanovení jejich povinností, až po přehled sankcí, které je možné uložit za neplnění povinností. Další části zákona pak popisují pravomoci Úřadu, jeho činnost v oblasti kybernetické bezpečnosti a další procesní záležitosti, které jsou pro fungování zákona nezbytné, nicméně pro jeho čtenáře většinou zbytné. Rozsah povinností stanovených regulovaným osobám vychází primárně z požadavků směrnice NIS 2. Ve vztahu k subjektům zařazeným do nižšího režimu dochází k redukci jejich povinností tak, aby tyto osoby nebyly neúměrně zatěžovány. I ve vztahu k režimu vyšších povinností však navrhovaná úprava vychází z mezinárodních standardů a norem, které jsou v oblasti kybernetické bezpečnosti standardně zaváděny. Požadavky na regulované subjekty jsou tedy v souladu s dobrou praxí v odvětví. Vzhledem k tomu, že normy stanovující povinnosti mají povahu performativní, tedy stanovují kýžený stav a volbu postupu často nechávají na aplikaci samotnými subjekty s tím, že jsou ovládány přístupem založeným na riziku a principem proporcionality přijatých opatření vůči právě tomuto riziku, nelze ve vztahu k nim dle našeho názoru hovořit o formalismu. Připomínkové místo s vypořádáním souhlasí.

105. Ministerstvo zemědělství	D	Hodnocení a výběr (řízení) dodavatelů v rámci průběhu zadávacího řízení z hlediska posouzení naplnění požadavků a opatření kybernetické bezpečnosti dle tohoto zákona by mělo být podrobněji popsáno tak, aby zadavatel měl jednoznačně definované možnosti a nezpochybnitelné oprávnění pro uplatnění hodnotícího kritéria (kybernetická bezpečnost) k vyloučení uchazeče (dodavatele) z výběrového řízení. (Toto by mělo být zakotveno i v novelizaci zákona č. 134/2016 Sb., o zadávání veřejných zakázek).	Vysvětleno Všichni poskytovatelé regulované služby (včetně těch soukromých) musí řídit své dodavatele, tedy zohledňovat požadavky vyplývající z bezpečnostních opatření při výběru dodavatele a ve smlouvě s ním. Ustanovení týkající se řízení dodavatelů pak pro poskytovatele regulovaných služeb, kteří jsou zároveň veřejným zadavatelem, nad rámec toho stanovuje, že zohlednění požadavků vyplývajících z bezpečnostních opatření v zadávacích podmínkách na veřejnou zakázku nelze považovat za nezákonné omezení hospodářské soutěže, resp. nejedná se o vytváření bezdůvodných překážek hospodářské soutěže. Směřuje tedy přímo na § 36 odst. 1 zákona č. 134/2016 Sb. V zásadě přitom nepřináší nic nového, neboť ve vztahu ke všem zákonným povinnostem zadavatelů (vyplývajícím z jakýchkoli jiných právních předpisů) platí, že jejich zohlednění při výběru dodavatele v míře nezbytné pro jejich splnění nemůže být shledáno neodůvodněným omezením hospodářské soutěže. Povinnost zohledňovat požadavky plynoucí ze zákona při řízení dodavatele, tedy při jeho výběru a uzavření smlouvy, platí vždy. Obdobně by měl subjekt postupovat ať už se jedná o kybernetickou bezpečnost nebo o jakékoliv jiné povinnosti, které mu ukládají další zákony. Úprava zákona č. 134/2016 Sb. tudíž nutná není, jelikož tento postup umožňuje jak současná právní úprava, tak navrhovaný zákon. Připomínkové místo s vypořádáním souhlasí.
106. Ministerstvo zemědělství	D	K § 5 Kritéria pro určení regulované služby se jeví jako kritéria pro určení poskytovatele regulované služby (PRS) v režimu vyšších povinností. Nemělo by se uvedené upřesnit v názvu paragrafu? Orgán nebo osoba	Vysvětleno Návrh zákona je koncipován tak, že regulované služby a režim poskytovatele regulované služby jsou

		určen rozhodnutím Úřadu podle § 5, je vždy poskytovatelem regulované služby v režimu vyšších povinností. Chybí kritéria pro určení regulované služby v režimu nižších povinností.	relativně samostatnými instituty. To je dáno zejména tím, že zatímco regulovaných služeb může být u jednoho poskytovatele identifikováno/určeno několik, režim je pro každého poskytovatele stanoven pouze jeden (společný pro všechny regulované služby). Z toho důvodu se i rozhodnutím Úřadu podle § 5 určují regulované služby, nikoli jejich režim. Současně je však v § 6 návrhu stanoveno, že jakmile je u poskytovatele určena alespoň jedna služba podle kritérií uvedených v § 5 návrhu, bude režimem celého poskytovatele vždy režim vyšších povinností. Reakce připomínkového místa: Stále není jasné jaký rozdíl je mezi identifikací a určením – viz §5, §13 body 1a a 1b. Reakce NÚKIB: Pojmy identifikace a určení je potřeba vykládat v kontextu ustanovení, ve kterých jsou použita. Co se týče procesu identifikace a určení regulované služby, tj. úpravy obsažené v § 4 a § 5, platí, že identifikaci (tedy tzv. samo-posouzení) provádí sám poskytovatel na základě kritérií obsažených ve vyhlášce. Pokud poskytovatel dovodí, že kritéria splňuje, registruje se u Úřadu v souladu s § 8 odst. 1 a 2 a začne plnit požadavky zákona. Naopak určení podle § 5 provádí Úřad sám, v rámci správního řízení, podle kritérií uvedených v § 5 odst. 1, poskytovatel je účastníkem řízení, teprve až vydáním a nabytím právní moci rozhodnutí Úřadu je poskytovatel určen, je zaregistrován Úřadem a začne plnit své povinnosti. Samostatnou povinností je stanovení rozsahu řízení kybernetické bezpečnosti podle § 13, které následuje až po fázi identifikace/určení regulované služby a její

			registrace. Stanovení rozsahu činí sám poskytovatel, Úřad do toho to procesu nijak nezasahuje. Identifikace a určení, o kterém hovoří § 13 odst. 1 písm. a) a b), zde tedy zavazují pouze poskytovatele regulované služby (což plyne z návětí odst. 1). Užití různých pojmů zde má svůj důvod: poskytovatel identifikuje, tedy nalezne, všechna primární aktiva organizace. Nic neurčuje, nic netvoří, pouze hledá a nalézá (tedy identifikuje). V návaznosti na to však poskytovatel musí stanovit, která z těchto primárních aktiv souvisejí s poskytováním regulované služby. Taková aktiva tedy určí, protože o nich prohlásí, že souvisejí s poskytováním regulované služby. Stejně tak v případě odst. 1 písm. c) nejdříve provozovatel identifikuje (nalezne) organizační části organizace a podpůrná aktiva a následně o některých (až všech) z nich prohlásí (určí), že souvisí s poskytováním regulované služby. Připomínkové místo s vypořádáním souhlasí.
107. Ministerstvo zemědělství	D	K § 5 písm. a) bodu 1. a 4 Dáváme ke zvážení, zda by neměla být užívána jednotná terminologie. Jednou se uvádí Česká republika, jindy stát.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
108. Ministerstvo zemědělství	D	K § 27 Požadujeme vysvětlit, zda poskytovatel regulované služby má povinnost určit a hlásit strategicky významnou službu.	Vysvětleno - nyní § 28 Strategicky významná služba je určena kritérii ve vyhlášce, případně rozhodnutím Úřadu. V prvním případě poskytovatel provádí registraci služby pro naplnění identifikačních kritérií, jelikož je poskytovatelem regulované služby. V případě rozhodnutí Úřadu, provede registraci služby Úřad. Reakce připomínkového místa:

			Kritéria pro identifikaci jsou sice uvedena, ale pro určení SVS nikoli. Reakce NÚKIB: Kritéria pro identifikaci jsou obsahem budoucí vyhlášky o regulovaných službách, jejíž teze byly rozeslány v meziresortním připomínkovém řízení. Kritérium pro určení je obsaženo v § 28 odst. 1 písm. b): Strategicky významnou službou je regulovaná služba určená rozhodnutím Úřadu v případě, že by její narušení mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek. Kritériem je tedy to, že by narušení regulované služby mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek. Jedná se o kritérium sice obecné, avšak vyčerpávajícím způsobem pokrývající potenciální množinu služeb, které v současné době nejsou zahrnuty mezi strategicky významné služby (ať už proto, že například neexistují, nebo proto, že z jakýchkoliv jiných důvodů není jejich důležitost na takové úrovni, aby mezi ně zahrnuty byly). V rámci vyváženosti je pak samozřejmě nutné dodat, že se v případě určení služby podle tohoto kritéria jedná o víceméně standardní správní řízení a rozhodování, ve kterém jsou šetřena všechna práva jeho účastníků. Reakce připomínkového místa Připomínkové místo s vypořádáním souhlasí.
109. Ministerstvo zemědělství	D	K § 29 odst. 4 V návrhu se uvádí „Poskytnutí informací podle tohoto ustanovení není porušením mlčenlivosti podle jiného právního předpisu.“ Doporučujeme doplnit odkaz na příslušný právní předpis.	Akceptováno jinak - nyní § 30 odst. 4 Bylo upuštěno od generálního prolomení mlčenlivosti. Nově byly vytipovány subjekty, u kterých NÚKIB

			předpokládá potřebu prolomení mlčenlivosti a byla navržena i úprava dotčených právních předpisů. Připomínkové místo s vypořádáním souhlasí.
110. Ministerstvo zemědělství	D	K 34 Požadujeme upřesnit formulaci ve stanoveném čase a ve stanovené kvalitě služby. Je vhodné se odklánět od norem řady 27 000, které jsou již propracované a v praxi osvědčené?	Vysvětleno - nyní § 35 Pojmy stanovený čas a kvalita jsou dále rozpracovány v návrhu vyhlášky o opatřeních poskytovatele regulované služby v režimu vyšších povinností. A to konkrétně v § 16 odst. 2, který stanoví, že: "Cíle řízení kontinuity podle odst. 1 písm. c) tohoto ustanovení jsou stanoveným časem a kvalitou regulované služby podle § 35 zákona. Stanoveným časem je doba obnovení chodu podle odst. 1 písm. c) bod 2. tohoto ustanovení a stanovenou kvalitou regulované služby je minimální úroveň poskytovaných služeb podle odst. 1 písm. c) bod i) tohoto ustanovení." Připomínkové místo s vypořádáním souhlasí.
111. Ministerstvo zemědělství	D	K § 35 a § 36 Dáváme ke zvážení prohození § 35 a § 36 a stávající § 35 nadepsat „Hlášení údajů“.	Akceptováno jinak - nyní § 36 a 37 Stanovené pořadí ustanovení není namístě měnit, neboť § 36 upravuje povinnost plněnou vůči Úřadu, a to v co nejkratší době od začátku poskytování služby (resp. bezprostředně po změně ohlášených údajů). Pro snazší orientaci dotčených subjektů je proto vhodnější, aby uvedená „administrativní“ povinnost byla uvedena na začátku Hlavy III. Na druhou stranu platí, že orientace dotčených subjektů v textu návrhu zákona bude usnadněna úpravou pojmenování § 36 a § 37, konkrétně prvního uvedeného na „Hlášení údajů subjektů poskytujících služby jmen domén“ a druhého uvedeného na „Shromažďování údajů o registraci jmen domén“. Pojmenování hlavy III návrhu zákona bylo upraveno

			na „Subjekt poskytující služby registrace jmen domén a subjekt spravující a provozující registr domén nejvyšší úrovně“. Připomínkové místo s vypořádáním souhlasí.
112. Ministerstvo zemědělství	D	K § 62 Dáváme ke zvážení vhodné nastavení sankcí z hlediska rovného přístupu a nediskriminace. Zejména podle odstavce 2 bude uplatňována různá donucovací pokuta s ohledem na velikost obrátu podnikající fyzické osoby nebo právnické osoby. Za stejné „provinění“ bude ukládán odlišný „trest“.	Vysvětleno - nyní § 64 Ukládání sankcí se nad rámec speciální úpravy obsažené v návrhu zákona řídí obecně platnými základními zásadami správního trestání, tedy mj. i zásadou rovného přístupu a nediskriminace. Pokuta (a je lhostejno, zda jde o pokutu za přestupek, nebo např. donucovací pokutu podle správního řádu) musí být stanovena tak, aby byla zejm. přiměřená, nediskriminační, odpovídající pochybení a přístupu orgánu, který ji ukládá, k trestání obdobných prohřešků u jiných osob, a nelikvidační pro osobu, které je ukládána (jde jen o příkladný výčet pravidel, kterými jsou správní orgány, tedy nejen NÚKIB, při ukládání pokut vázány a které vycházejí primárně z judikatury správních soudů). Donucovací pokuta podle § 129 správního řádu není trestem ve smyslu trestání nesplnění povinnosti stanovené návrhem zákona, ale donucovacím prostředkem používaným pouze v rámci exekuce správního rozhodnutí. Ustanovení § 64 odst. 2 návrhu zákona nestanoví specifické podmínky pro ukládání donucovacích pokut, naopak se v tomto případě bude Úřad řídit obecnou úpravou obsaženou ve správním řádu. Návrh zákona však speciálně upravuje výši donucovací pokuty, kterou lze v rámci exekuce rozhodnutí Úřadu uložit. Důvodem (uvedeným v důvodové zprávě k návrhu) je zjevná zastaralost částek stanovených správním řádem a jejich naprostá disproporčnost ve vztahu k pokutám, kterým subjekty

			čelí za porušení povinností stanovených návrhem zákona. Upravená výše donucovací pokuty tak reflektuje maxima pokut, které je možné uložit za neplnění povinností podle návrhu zákona. Odlišnosti v maximech možných donucovacích pokut u jednotlivých subjektů jsou žádoucí, neboť i povinnosti, které jimi budou vymáhány, budou u jednotlivých subjektů odlišného charakteru, závažnosti a výše. Výsledná výše však bude vždy odrážet základní zásady správního trestání uvedené výše. Připomínkové místo s vypořádáním souhlasí.
113. Ministerstvo zemědělství	D	K § 72 Dáváme ke zvážení zrušení vyhlášky, která ještě nebyla vyhlášena, konkrétně se jedná o vyhlášku uvedenou pod bodem č. 6: Vyhláška č. XX/XXXX Sb., o bezpečnostních pravidlech pro využívání služeb cloud computingu orgány veřejné moci.	Vysvětleno Vyhláška o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu již byla vydána ve Sbírce zákonů pod č. 190/2023 Sb. a nabyla účinnosti 1. 7. 2023. Připomínkové místo s vypořádáním souhlasí.
114. Ministerstvo zemědělství	D	K účinnosti Dáváme ke zvážení nastavení účinnosti nového právního předpisu na 18. října 2024, a to s ohledem na předpokládané množství prováděcích právních předpisů.	Akceptováno Účinnost návrhu zákona je již nyní navržena na 18. října 2024, a to z s ohledem na transpoziční lhůtu směrnice NIS 2. Připomínkové místo s vypořádáním souhlasí.
115. Česká konference rektorů	Z	K § 2 odst. 1 písm. b) Doporučujeme změnit definici primárního aktiva následovně: „primárním aktivem jsou data, informace, služby a procesy“	Akceptováno jinak Po vyhodnocení vícero připomínek od odlišných autorů na úpravu definice primárních aktiv jsme upravili definice následovně: "primárním aktivem informace a služby". Vysvětlení použití této definice a

			Data a informace jsou rozdílné pojmy. Stejně tak jsou rozdílnými pojmy služby a procesy. Data v sobě mohou a nemusí nést část informace. Současně informace bude vždy složena z dat. Informace jsou vnímány jako něco „kvalifikovanějšího“, nežli data. Data jsou fakta, která se stávají informacemi tehdy, pokud jsou vnímána či vyjádřena v kontextu a nesou význam, který je pochopitelný pro lidi. Pokud tedy chcete jako primární aktivum označit i data, pak nelze dát rovnítko mezi pojem informace a data. Služby nejsou totéž, co procesy. Pokud chcete vymezit procesy jako primární aktivum, bylo by vhodnější uvést definici ve které procesy přímo označíte za primární aktivum. Je zřejmé, že je využívána terminologie jak ze zák. 181/2014 Sb., tak i z norem ISO 27000. Nicméně uvedení že: „službou se rozumí také procesy“ může být v praxi mnohem více matoucí a zavádějící. Výslovné uvedení procesů a dat, jakožto samostatných primárních aktiv by tak mělo vést k posílení právní jistoty adresátů.	jejího kontextu ve vztahu k pojmům data a služby je náležitě upraveno v důvodové zprávě. Připomínkové místo s vypořádáním souhlasí.
116. Česká rektorů	konference	Z	K § 2 odst. 1 písm. b) Doporučujeme vypouštění slov: „včetně provozních údajů“ Jako primární aktivum jsou nově určeny i provozní údaje. Vlastní pojem může být vykládán značně různorodě. Může se jednat o data spadající např. pod § 97 odst. 4 zák. č. 127/2005 Sb., o elektronických komunikacích, ale také se může jednat např. o údaje v podobě „data sheetu“, na kterém budou zaznamenány údaje o provozu či o metadata ze systémů.	Akceptováno Připomínkové místo s vypořádáním souhlasí.

		Byť jsou provozní údaje v současném zákoně č. 181/2014 Sb., uvedeny v § 6a a § 15a, tak se vztahují toliko ke KII či KKI. U § 15a je to o vyžádání dat k incidentu. Dle návrhu zákona se ale bude tato povinnost (tj. určit provozní údaje jako primární aktivum) nově vztahovat na všechny regulované subjekty (jak v režimu vyšších, tak nižších povinností) a zejména na všechny jimi spravované služby, systémy aj. Provozní údaje jsou stále data. Evidovat data či provozní údaje bez kontextu jako samostatná primární aktiva nemá smysl a půjde o zbytečné a neúčelné zatížení povinného subjektu. Domníváme se, že je na povinném subjektu, aby vyhodnotil, která data a provozní údaje bude identifikovat a hodnotit jako aktiva.	
117. Česká rektorů	konference	Z K § 2 odst. 1 písm. c) Doporučujeme vypouštění slov: ~~„technickým aktivem technické a programové prostředky a vybavení, kdy technickým a programovým prostředkem a vybavením se rozumí také komunikační prostředky, sítě elektronických komunikací a průmyslová, řídicí nebo jiná obdobná specifická aktiva;“~~ V zákoně dochází k uvedení některých technických aktiv. Domníváme se, že by zákon měl být dostatečně srozumitelný, ale na druhou stranu dostatečně obecný a neomezující vývoj ICT. Z tohoto důvodu se domníváme, že je vhodné odstranit uváděný demonstrativní výčet. Byť se jedná o demonstrativní výčet, tak právě jeho uvedení nemusí posílit právní jistotu adresátů a jednoznačně stanovit, že tato aktiva spadají do kategorie podpůrných aktiv. Dle našeho názoru je vhodnější: - Mít v zákoně uvedenu obecnou definici V případě nejasností v praxi vymezit, co se rozumí technickým aktivem např. metodickým výkladem NÚKIB aj.	Akceptováno jinak Stávající definice neomezuje vývoj ICT a Úřad se domnívá, že výčtem byla naopak zajištěna vyšší míra právní jistoty, nicméně návrh ustanovení byl upraven a nyní zní: "technickým aktivem technické a programové prostředky a vybavení, a to včetně průmyslových, řídicích nebo jiných obdobných technických aktiv". Byl odstraněn demonstrativní výčet, kdy současně byla zachována část, kterou povinné osoby často opomíjí při identifikaci technických aktiv, na které se vztahují bezpečnostní opatření vyhlášek, potažmo zákona o kybernetické bezpečnosti. Dle Úřadu, nově navrhované znění tak nad rámec velice obecné definice konkretizuje, že OT je součástí technických aktiv, což posiluje právní jistotu. Připomínkové místo s vypořádáním souhlasí.

118. Česká rektorů	konference	Z	K § 2 odst. 2 písm. a) o Změna definice: o „kybernetickým prostorem digitální prostředí tvořené aktivity umožňující vznik, výměnu a další zpracování informací a dat,“ Pokud má být vytvořen soulad s dalšími právními předpisy (EU a ČR), zejm. (EU) 679/2016, pak pojmy: „vznik, výměna a další“ jsou nadbytečné, protože jsou již obsaženy v pojmu „zpracování“. Z hlediska větší právní jistoty je tedy vhodnější využít toliko pojem zpracování.	Akceptováno Zpracováním se ve smyslu GDPR myslí v zásadě jakékoli nakládání s daty a informacemi, z této premisy vycházíme a „vznik a výměna“ jsou v definici de facto nadbytečné, protože jsou již obsaženy v pojmu „zpracování“. Co se týče dalšího rozšiřování pojmu, zde podle našeho názoru postačí interpretace v odůvodnění normy, konkrétně: Definice kybernetického prostoru v zásadě přejímá definici obsaženou v dosavadním zákoně o kybernetické bezpečnosti a nadále tak platí, že kybernetickým prostorem je myšleno informační prostředí k realizaci informačních transakcí, které je vytvořeno aktivity relevantními pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě, jinak také technologiemi, jejichž definice a podmínky užívání mohou upravovat zvláštní zákony, mj. informačními systémy, službami a sítěmi elektronických komunikací. Jedná se přitom i o taková aktiva, informační systémy, služby a sítě elektronických komunikací, které nejsou připojeny k veřejné síti, tj. k internetu. Připomínkové místo s vypořádáním souhlasí.
119. Česká rektorů	konference	D	K § 2 odst. 2 písm. b) o Doplnění definice: bezpečností informací zajištění dostupnosti, důvěrnosti, integrity a autentičnosti informací a dat o Původní triáda CIA je v současné době ne zcela dostačující.	Neakceptováno Nahrazení CIA modelu jiným konceptem je na NÚKIB pravidelně diskutovaná otázka a prozatím jsme vždy došli k závěru, že je stávající pojetí dostatečné. Zákon o kybernetické bezpečnosti má sloužit jako univerzální předpis řešící kybernetickou bezpečnost různých druhů služeb, které reguluje. Navrhované doplnění se v převážné míře váže na

			o Specificky je chráněna i autentičnost (tj. pravost, původnost) dat. (EU) 2022/2555 explicitně tuto oblast zmiňuje. Uvědomujeme si, že tato problematika byla uvedena již v NIS1, nicméně v současné době, zejména s výrazným rozmachem neuronových sítí (typu ChatGPT, AzureOpenAI aj.) bude na místě se zaměřit právě na problematiku autentičnosti tj. pravosti/původnosti dat a informací. Současně je s autentičností spojena i hrozba spočívající v záměně dat, informací či identity. Doporučujeme rozšířit znění zákona či prováděcí vyhlášky	oblast digitálních podpisů nebo obecně služeb vytvářejících důvěru a upravuje trochu jinou otázku, než která je předmětem úpravy kybernetické bezpečnosti v navrhovaném zákoně. Legislativa, která odvětví služeb vytvářejících důvěru reguluje, však i nadále zůstává v platnosti (pouze část kybernetické bezpečnosti je nově přenesena do zákona o kybernetické bezpečnosti), problematiku jdoucí nad rámec zákona o kybernetické bezpečnosti tedy budou i nadále řešit k tomu příslušné předpisy a příslušní regulátoři. Pojem bezpečnost informací se netýká obsahu informace, ale pouze funkčnosti prostředí, v němž je informace tvořena, zpracována, uchovávána a komunikována. Narušením autenticity obsahu informace ovšem zároveň dochází k narušení integrity tohoto funkčního prostředí. Autenticita informace je tedy pro potřeby zákona o kybernetické bezpečnosti chápána jako součást integrity. Připomínkové místo s vypořádáním souhlasí.
120. Česká rektorů	konference	Z	K § 2 odst. 2 písm. d) Vymezit konkrétněji, co je myšleno pod závažným ovlivněním aktiva poskytovatele nebo uživatelů. o V kontextu upřesnění pojmu „významný dopad“ považujeme za potřebné i upřesnění pojmu „závažného ovlivnění aktiva poskytovatele nebo uživatelů.“ Přestože bylo odůvodněno v předchozím vypořádání, že dopad pojmu „závažné ovlivnění“ bude záležet na konkrétní situaci, problematika může být interpretační praxe a rozdílnost aplikací, a to zvláště při sektorové rozsáhlosti a rozdílnosti poskytovatelů regulovaných služeb. Vzhledem k unikátnímu využití pojmu (a tomu, že je s ním pracováno de facto jen zde) by ještě stálo za úvahu zavést alespoň na	Neakceptováno Významné hrozby jsou v zákoně definovány pro potřeby informační povinnosti poskytovatele regulované služby, který má informovat své uživatele o způsobech eliminace dopadů realizace hrozby nebo o hrozbě samotné. Toto informování se však bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek, zejména ve vztahu k uživatelům. Závažné ovlivnění bude v různých situacích a v kontextu různých poskytovatelů regulovaných služeb vykládáno různě. Odvětví od odvětví a poskytovatel od poskytovatele bude vliv na aktiva a újma, kterou je hrozba schopna způsobit, posuzována různě. Z toho

			úrovni podzákonného předpisu demonstrativní indikaci relevantních určujících znaků či situací.	důvodu se Úřadu nejeví jako vhodné definici významné hrozby blíže rozvádět (taková definice by pořád musela být dostatečně obecná, aby byla univerzálně aplikovatelná na všechny regulované subjekty, a tedy by ani v jiné formě nemohla přinést žádné významné zpřesnění). Máme za to, že v kombinaci s podmínkou značné újmy, kterou významná hrozba musí být schopna způsobit, by mělo být adresátům normy jasné, jakým způsobem mají u sebe v organizaci stanovit hranici pro určení významnosti hrozby. Způsob stanovení této hranice by měl být zanesen v bezpečnostních politikách a bezpečnostní dokumentaci regulované osoby. Pokud pak bude hranice významnosti hrozby stanovena smysluplně a s ohledem na specifika a potřeby organizace a jejích zákazníků, Úřad nemá důvod nastavené metriky rozporovat. Připomínkové místo s vypořádáním souhlasí.
121. Česká rektorů	konference	Z	K §2 odst. 2 písm. e) o Změna definice: o kybernetickou bezpečnostní událostí událost, která ~~může způsobit kybernetický bezpečnostní incident~~ mohla narušit dostupnost, integritu nebo důvěrnost aktiv, ale plnému vzniku takové události bylo úspěšně zabráněno nebo taková událost nenastala o Navržené znění definice vychází z čl. 6 odst. 5 směrnice NIS 2 a lépe vystihuje podstatu „kybernetické bezpečnostní události“. o „Událost“ by měla být definována jako situace, která nastala nebo se předpokládá, že nastala. Tento předpoklad existuje, protože existuje přímá nebo nepřímá indicie, že událost nastala. Takováto definice dle našeho názoru lépe a pochopitelněji reflektuje podstatu kybernetické bezpečnostní události (i z časového hlediska –	Akceptováno jinak Definice kybernetické bezpečnostní události byla na základě Vaší připomínky upravena následujícím způsobem: "událost, která může nebo mohla vyústit v kybernetický bezpečnostní incident". Připomínkové místo s vypořádáním souhlasí.

			„mohla“, nikoliv „může“), je stále v souladu se stávající definicí kybernetického bezpečnostního incidentu a inkorporuje prvky významné události dle čl. 6 odst. 5 směrnice NIS 2, kterou zákon jinak nepřijímá.	
122. Česká rektorů	konference	Z	K § 2 odst. 2 písm. g) o Změna definice: <u>zvládáním kybernetického bezpečnostního incidentu úkony vedoucí k zajištění prevence, detekce, analýzy, omezení dopadů incidentu, reakce na incident a následného zotavení nápravným opatřením,</u> Uvedení pojmu „zotavení“ není vhodné. Po incidentu nemusí nutně dojít k zotavení, ale je třeba přijmout nápravná opatření, která mohou být různého charakteru. V praxi mnohdy nemusí záměrně dojít k zotavení napadeného systému, naopak incident a jeho řešení může vést k záměrnému odstavení zranitelných systémů. Tyto úkony lze považovat za nápravná opatření, nikoli však za zotavení.	Neakceptováno Zotavení (obnova) může v praxi představovat např. zrušení systému (např. zapomenuté služby na které se incident stal), nebo náhradu HW. Zavedení opatření vedoucích k tomu, aby se incident znovu nestal (tedy Vámi zmiňovaná nápravná opatření) jsou součástí reakce na incident. Samotný pojem "nápravná opatření" je nadto v rámci zákona vyhrazen pro rozhodnutí Úřadu podle § 57, proto by nebylo účelné jej zavádět na tomto místě. Na základě připomínky došlo k nahrazení termínu "zotavení" pojmem "obnova". Připomínkové místo s vypořádáním souhlasí.
123. Česká rektorů	konference	Z	K § 2 Doplnění pojmu: „významný dopad“ Zákon na řadě míst pracuje s pojmem významný dopad, jakožto ze skutečností, která má vztah k obecné regulaci subjektů spadajících do působnosti ZKB. Tento je do určité míry vymezen jen ve vztahu k poskytovateli v režimu nižších povinností (viz § 16 odst. 3). Ale s pojem významný dopad je pracováno i ve vztahu k poskytovateli v režimu vyšších povinností, kde však jakýkoliv rámec toho, co je považováno za významný dopad chybí. Je zřejmé, že pro každého poskytovatele může významný dopad představovat jinou situaci.	Neakceptováno Připomínka správně uvádí, že pojem významný dopad se v návrhu zákona a jeho prováděcích předpisech vyskytuje na mnoha místech. Vždy je pak použit ve vztahu ke konkrétní situaci, konkrétní povinnosti. V kontextu těchto rozdílných situací a povinností pak může nabývat mírně odlišného významu (a za tím účelem je vždy doplněn o specifikaci dopadu, např. „incident s významným dopadem na poskytování regulované služby“ nebo „významný dopad na kybernetický prostor státu“). Tam, kde je to možné a vhodné, byly do návrhu zákona nebo prováděcích předpisů včleněny bližší konkretizace pojmu nebo způsob jeho identifikace (např. kritéria pro stanovení významnosti dopadu kybernetického incidentu pro

			Navrhujeme uvést, že významný dopad a jeho hodnocení je uvedeno v jednotlivých vyhláškách vztahujících se k poskytovatelům regulovaných služeb. Aplikovatelným kritériem by mohla být například finanční ztráta regulovaného subjektu v důsledku incidentu či riziko finanční újmy vyjádřené v procentech (např. 0,5 % ročního obrátu).	režim nižších povinností, kritéria pro identifikaci a určení poskytovatele regulované služby, která vyjadřují významnost dopadu služby na zabezpečení důležitých společenských nebo ekonomických činností, nebo kritéria pro posouzení významnosti dopadu na kybernetický prostor státu související s hlášením incidentů v režimu vyšších povinností). S ohledem na různé použití pojmu pro různé účely je pak nemožné stanovit jednu hranici významnosti, která by byla univerzálně platná pro všechny případy (zmíněná finanční újma může být pro jeden subjekt nevýznamná, zatímco pro jiný již půjde o významnou hranici, nadto se její významnost nebo vůbec způsobilost vyhodnocení může měnit v kontextu ustanovení, ve kterém je s významným dopadem pracováno). Navrhovaná univerzální proklamace, že významný dopad a jeho hodnocení je uvedeno v jednotlivých vyhláškách vztahujících se k poskytovatelům regulovaných služeb, je z našeho pohledu zbytečná a nepřináší čtenářům právních předpisů žádný užitek. Nadto je u relevantních případů uvedena buďto přímo v zákoně, nebo v důvodové zprávě k návrhu zákona. Připomínkové místo s vypořádáním souhlasí.
124. Česká konference rektorů	Z	K § 2	Doplnění pojmu CERT. Navrhované znění: <u>„CERT je tým, který je v jasně definovaném poli působnosti zodpovědný za řešení kybernetických bezpečnostních incidentů a</u>	Akceptováno jinak Na základě Vaší připomínky došlo k doplnění definice Národního a Vládního CERT a zavedení legislativní zkratky: "národní/vládní tým koordinace a zvládání kybernetických bezpečnostních incidentů, událostí a hrozeb (dále jen "Národní/Vládní CERT")". Podrobnější definice činností obou týmů jsou rozvedeny v příslušných ustanoveních.

		<u>reakcí na kybernetické hrozby. Jedná se o tým zajišťující řešení a koordinaci činností souvisejících s kybernetickým bezpečnostním incidentem vedoucích k jeho zvládnutí.“</u> V zákoně je s pojmem CERT pracováno jako s notoriitou, nicméně roli bezpečnostního/reakčního týmu běžně plní týmy typu CERT/CSIRT. V profesním vnímání jsou zkratky CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team) vnímány „synonymně“, rozhodně se o synonymum nejedná. Rozdíl je jednak v licencování značky CERT u Carnegie Mellon Univerzity a jednak i v drobném rozdílu: Emergency Response a Security Incident Response. Doporučujeme umožnit výkon týmu CERT i jiným akreditovaným týmům CSIRT (viz https://www.trusted-introducer.org/index.html). Národní bezpečnostní tým využívá označení CSIRT, přičemž fakticky vykonává úkony požadované po CERT.	Připomínkové místo s vypořádáním souhlasí.
125. Česká konference rektorů	Z	K § 15 odst. 1 písm. b) bod 2 o Změna definice: <u>„bezpečnost komunikačních sítí technických aktiv“</u> Případně: „bezpečnost <u>informačních a komunikačních systémů</u>“ V rámci technických opatření uvedených v zákoně není nikde uvedena ochrana informačních systémů (počítače, servery aj.). Domníváme se, že je třeba mít v zákoně uveden pojem obecný, nadřazený a tento by pak měl být blíže specifikován v prováděcích předpisech.	Neakceptováno V rámci zavádění bezpečnostních opatření jsou obecně nad „technickými aktivy“ zaváděna veškerá „technická opatření“ dle § 15 odst. 1 písm. b) návrhu zákona. Požadavky v oblasti „bezpečnost komunikačních sítí“ dle § 15 odst. 1 písm. b) bod 2. návrhu zákona jsou pouze podmnožinou „technických opatření“, které cílí na zavádění bezpečnostní opatření nad komunikačními sítěmi a jejich komunikací (např. síťovou infrastrukturou) nad užší podmnožinou technických aktiv. Zatímco jiná technická opatření v § 15 odst. 1 písm. b) návrhu zákona cílí na jiné oblasti zabezpečení v rámci technických aktiv, jako např. i na Vámi uvedené počítače a servery. Jednotlivá bezpečnostní opatření, včetně těch technických, jsou

			S ohledem na vymezení základních pojmů v § 2 odst. 1 písm. c) je jako vhodný nadřazený pojem jeví „technické aktivum“, nicméně uvádíme i možnou alternativu.	již náležitě rozvedena v dílčích prováděcích předpisech, jak navrhuje. Připomínkové místo s vypořádáním souhlasí.
126. Česká rektorů	konference	Z	K § 17 odst. 1 o Změna lhůty 24 hodin pro předložení hlášení o kybernetickém bezpečnostním incidentu. <u>Poskytovatel regulované služby bez zbytečného odkladu po zjištění kybernetického bezpečnostního incidentu, nejpozději však do 24 72 hodin předloží Úřadu nebo Národnímu CERT prvotní hlášení, v němž uvede, zda se domnívá, že byl kybernetický bezpečnostní incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad.</u> Úprava, která stanovuje lhůtu 24 hodin na nahlášení informací týkajících se každého kybernetického bezpečnostního incidentu [tj. dle §2 odst. 2 písm. f) – každé „narušení bezpečnosti informací v rámci aktiv“]. Tato úprava zásadně podstatně mění současnou právní úpravu a mnohdy nebude reálně proveditelná. Proces hlášení kybernetických bezpečnostních incidentů je sice upraven směrnicí NIS2, ale lhůta 24 hodin se dle čl. 23 odst. 4 písm. a) směrnice NIS2 vztahuje pouze k zjištění významného incidentu. Dle čl. 23 odst. 1 je významným incidentem takový „každý incident, který má významný dopad na poskytování jejich služeb“. Dle této dikce se tedy rozhodně nejedná o každý kybernetický bezpečnostní incident, ale pouze o takový, který má významný dopad na poskytování služeb regulovaného subjektu. Česká právní úprava v tomto případně významně, a ne zcela odůvodněně rozšiřuje povinnost hlásit všechny kybernetické bezpečnostní incidenty ve velmi krátké a mnohdy nesplnitelné lhůtě.	Neakceptováno Lhůta pro hlášení incidentů je vázána na okamžik zjištění tohoto incidentu, který se nemusí shodovat s reálným časem, kdy incident skutečně nastal. Pokud tedy incident nastane např. v sobotu, ale je nahlášen až v pondělí bezodkladně po tom, co se o něm příslušný zaměstnanec dozvěděl, je zákonná povinnost splněna. Takto stanovená lhůta má zajistit případnou rychlou reakci Vládního CERT, příp. Národního CERT při řešení incidentu a napomoci navazujícím preventivním či analytickým aktivitám Vládního CERT, příp. Národního CERT. Obsahové náležitosti prvotního hlášení jsou omezeny na nezbytné minimum, díky kterému bude Vládní CERT schopen posoudit, zda má incident významný dopad na kybernetický prostor státu, a zároveň by předání těchto informací nemělo představovat pro ohlašovatele nadměrnou administrativní zátěž. Poskytovatelé regulované služby v režimu nižších povinností hlásí pouze kybernetické bezpečnostní incidenty s významným dopadem, poskytovatelé regulované služby ve vyšším režimu hlásí všechny kybernetické bezpečnostní incidenty. Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je

		Doporučujeme vypustit limitaci lhůtou 24 hodin na prvotní hlášení, případně alespoň tuto lhůtu prodloužit a stanovit ji obdobně jako tomu je např. u GDPR (resp. § 41 odst. 2 zák. 110/2019 Sb., o zpracování osobních údajů) na 72 hodin.	žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob. Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnicí NIS 2, tzn. pokud bychom do zákona nezahrnuli požadavek na lhůtu, která je podle čl. 23 odst. 4 písm. a) směrnice NIS 2 stanovena na „bez zbytečného odkladu, nejpozději však do 24 hodin po zjištění“, byli bychom v rozporu se směrnicí NIS 2 a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Z uvedeného důvodu národní právní úprava tento požadavek kopíruje. Připomínkové místo s vypořádáním souhlasí.
127. Česká konference rektorů	D	K § 17 odst. 1 Navrhujeme pojem „prvotní“ vypustit či nahradit vhodnějším synonymem. „Poskytovatel regulované služby bez zbytečného odkladu po zjištění kybernetického bezpečnostního incidentu, nejpozději však do 24 hodin předloží Úřadu nebo Národnímu CERT ~~prvotní~~ hlášení, v němž uvede, zda se domnívá, že byl kybernetický bezpečnostní incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad.“ Užití pojmu „prvotní“ může evokovat, že se jedná o jakýsi draft – doporučujeme slovo „prvotní“ vypustit či nahradit vhodnějším synonymem.	Neakceptováno Směrnice NIS 2 pro tuto fázi hlášení používá pojem „včasné varování“ (<i>early warning</i>), který indikuje předložení prvotního draftu obsahujícího pouze nezbytně nutné informace jako příp. přeshraniční dopad a informaci, zda byl incident způsoben svévolným nebo nezákonným zásahem. V návrhu zákona je pojem „varování“ vyhrazen pro jiný institut, proto bylo ve vztahu k hlášení incidentů přistoupeno k pojmu vystihujícímu důraz na skutečnost, že je hlášení rozděleno do více fází. Připomínkové místo s vypořádáním souhlasí.

128. Česká rektorů	konference	Z	K § 17 odst. 4 Nemožnost nahlášení kybernetických bezpečnostních incidentů včetně dobrovolných hlášení jiným způsobem. Veškeré hlášení je vztaženo toliko k elektronické komunikaci. Absolutně není počítáno s výpadkem těchto služeb na straně toho, kdo má povinnost hlásit, avšak z objektivních důvodů (např. právě významné zasažení kybernetickým bezpečnostním incidentem), toto není schopen tímto způsobem učinit (např. mu nefunguje IT infrastruktura). Současně je v § 58 odst. 1 písm. h) uvedeno, že pokud tak povinný subjekt neučiní, dopustí se přestupku. Domníváme se, že by bylo vhodné definovat i jinou možnou „krizovou“ komunikaci v případě hlášení incidentu než jen tu uvedenou v § 17 odst. 4 a současně by mělo dojít k úpravě § 59 odst. 2, kde by v takovýchto případech měl být posuzován i materiální znak přestupku, tj. jeho škodlivost.	Neakceptováno Máme za to, že poslat prvotní hlášení prostřednictvím elektronické pošty lze i bez funkční infrastruktury regulované organizace. Kontaktní osoba to může učinit klidně ze svého mobilního telefonu, jde především o to, aby CERT mohl na tuto situaci bezprostředně reagovat. Pokud by došlo k nahlášení prostřednictvím neelektronických prostředků, např. standardní poštou, hrozí poměrně velké průtahy v řešení incidentu a možné reakci. Variantou je zachování pohotovostní telefonické linky, nicméně při počtu regulovaných subjektů není možné zajistit dostatečnou dostupnost takové linky, navíc by šlo těžko dodržet obsahové náležitosti hlášení. Připomínkové místo s vypořádáním souhlasí.
129. Česká rektorů	konference	Z	K § 19 odst. 1 Navrhujeme rozšíření pravomocí uvedených v tomto odstavci o pozdržení zveřejnění, např. následovně: „Úřad je oprávněn uložit poskytovateli regulované služby, který je dotčen kybernetickým bezpečnostním incidentem s významným dopadem, povinnost informovat uživatele regulované služby o tomto incidentu. <u>Úřad je dále oprávněn uložit poskytovateli regulované služby, který ví o významné kybernetické hrozbě, zranitelnosti či je dotčen kybernetickým bezpečnostním incidentem s významným dopadem, povinnost zveřejnění daných informací pozdržet v případech, ve kterých by vedlo k ohrožení dalších poskytovatelů regulovaných služeb.</u> V rozhodnutí o uložení této povinnosti stanoví Úřad rozsah informační povinnosti <u>či informačního embarga</u>“	Neakceptováno - nyní § 20 odst. 1 Rozsah informační povinnosti je ve směrnici NIS 2 vztažen pouze na incidenty (čl. 23 odst. 1) a hrozby (čl. 23 odst. 2). Informování o proběhlých incidentech je přednostně ponecháno v dispozici zasaženého subjektu, který, na rozdíl od Úřadu, má o incidentu podrobný přehled a sám nejlépe posoudí, zda je vhodné a žádoucí o něm informovat (v krajních případech mu tuto povinnost může uložit Úřad). Informace o hrozbách mohou obsahovat skutečnosti, které ve výsledku přispívají k příp. odvrácení incidentů u dalších subjektů, a nemají potenciál tyto subjekty ohrozit.

			Tento návrh je motivován zavedením systémů koordinovaného zveřejňování zranitelností směrnicí NIS 2. Zveřejněné informace o významných hrozbách, zranitelnostech postihujících více poskytovatelů regulovaných služeb, či incidentech s významným dopadem mohou občas citelně ohrozit další regulované subjekty v momentech, kdy neměly dostatečný čas se na danou výzvu připravit (zveřejnění se může de facto stát návodem pro méně informované či schopné hackery). V takových případech může být vhodné zavést dočasné informační embargo.	Úřad na základě svých zkušeností nepovažuje neinformování o incidentech a hrozbách za vhodné, naopak podporuje sdílení a předávání těchto informací. Zranitelnosti jsou právě z důvodů souvisejících s koordinovaným zveřejňováním zranitelností z informační povinnosti vyňaty. Koordinované zveřejňování zranitelností bude řešeno na jiné než zákonné úrovni, a to v souladu s požadavky směrnice NIS 2 uvedenými v čl. 12. Připomínkové místo s vypořádáním souhlasí.
130. Česká konference rektorů	Z	K § 26 odst. 6 Nejasné fungování institutu připomínek k opatření obecné povahy v případě vyloučení § 172 správního řádu. Zákon sice vylučuje v § 23 odst. 5 použití § 172 správního řádu, ale v odst. 6 nedostatečně nahrazuje fungování institutu připomínek a souvisejících záruk transparentnosti výkonu státní správy, doporučujeme tedy výslovně uvést, že se NÚKIB musí připomínkami zabývat a vypořádat je v odůvodnění opatření obecné povahy (analogicky k § 172 odst. 4 správního řádu).	Neakceptováno – nyní § 24 odst. 6 Zákon o kybernetické bezpečnosti ani v současné podobě neobsahuje jiný, než v současnosti navrhovaný proces vydávání reaktivního protioopatření (dříve reaktivního opatření). Účelem reaktivního protioopatření je co nejrychleji a v případech, které nesnesou odkladu, reagovat na aktuální riziko. Z tohoto důvodu byl jediný přílehlavý nástroj obsažený v rámci správního řádu příslušně upraven a návrhová část celého procesu opatření obecné povahy nebyla zavedena jako součást procesu vydávání reaktivního protioopatření, stejně jako nebyla součástí procesu původního reaktivního opatření. Zavedení navrhovaného by tedy bylo v přímém rozporu s účelem tohoto ustanovení, které je již ověřeným institutem, který byl ze strany Úřadu již několikrát úspěšně použit. Připomínkové místo s vypořádáním souhlasí.	
131. Česká konference rektorů	Z	K § 28 ve spojení s § 32 odst. 1 a § 58 odst. 3 písm. b) až d) Nejasný termín „bezpečnostně významná dodávka“.	Vysvětleno - nyní § 29, 33 odst. 1 a 60 odst. 3 písm. b) až d)	

			Z nového návrhu zákona vyplývá povinnost hlásit informace o dodavatelích bezpečnostně významných dodávek a evidovat tyto informace, přičemž nedodržení této povinnosti je přestupkem podle § 58. Pojem „bezpečnostně významné dodávky“ je sice definován v § 28, nicméně stále zůstává velmi vágní, není jasné, co pod takovou dodávku spadá a co nikoliv – není například jasné, jakého rozsahu nebo předmětu musí předmětná dodávka být. Není tedy jasné, který dodavatel spadá pod povinnost hlášení. Navrhujeme proto povinnost hlášení v návrhu vypustit, případně alespoň lépe specifikovat, zejména s ohledem na rozsah, předmět takové dodávky. Ve vztahu k tomuto pojmu není zejména jasné: 1) co vše je považováno za Bezpečnostně významnou dodávku 2) jaká má být úroveň detailu posuzovaného podpůrného aktiva 3) který dodavatel spadá do povinnosti hlášení. Jako vhodné řešení se jeví odkázat na prováděcí předpis, kde bude výše uvedené vysvětleno.	Pojem bezpečnostně významné dodávky je v návrhu zákona a ve zvláštní části důvodové zprávy k němu rozpracován co nejpodrobněji, jak to jeho povaha umožňuje. Vymezení konkrétních dodávek a jejich dodavatelů vychází z oboru činnosti dotčeného poskytovatele strategicky významné služby a zejména z jeho vlastního hodnocení aktiv dle prováděcího právního předpisu - vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. Pro odstranění případné přílišné tvrdosti zákona, kdy by někteří poskytovatelé služeb vztahovaly do tohoto pojmu výrazně více či méně dodavatelů a poddodavatelů než jiní, slouží korektiv vynaložení přiměřeného úsilí při zjišťování a hlášení dodavatelů a dodávek dle § 33 odst. 1 návrhu zákona. NÚKIB v tomto ohledu rovněž plánuje pokračovat v dosavadní dobré praxi vydávání podpůrných a metodických materiálů, které poskytnou vodítka pro co možná nejjednodušší aplikaci povinností, které s těmito pojmy pracují. Připomínkové místo s vypořádáním souhlasí.
132. Česká rektorů	konference	Z	K § 32 odst. 1 písm. b) Lhůta pro hlášení 10 dnů je příliš krátká. Není možné pro instituce větší velikosti (např. univerzita) hlásit v takto krátké lhůtě požadované informace o dodavatelích, zvláště pokud by bylo nutné hlásit všechny dodávky, i malého rozsahu. Navrhujeme nahradit lhůtu textem „bez zbytečného odkladu“ nebo významně prodloužit. Zásadní otázkou je, zda je v praxi takové hlášení s ohledem na množství změn a procesy vůbec realizovatelné.	Neakceptováno - nyní § 33 odst. 1 písm. b) Lhůta 10 dnů je mířena na proces nahlášení informací podle § 33 odst. 1 písm. a) a jejich změn. Nemíří na proces zjišťování těchto informací. Lhůta počne běžet až ve chvíli, kdy poskytovatel strategicky významné služby bude těmito informacemi disponovat. Realita pak bude taková, že poskytovatel strategicky významné služby si v prvním roce po písemném vyrozumění o označení regulované služby jako strategicky významné služby v evidenci regulovaných služeb (zde proběhla změna oproti původnímu návrhu,

			kdy se přechodná lhůta vázala na účinnost zákona) nastaví procesy a začne zjišťovat požadované informace. Tyto pak bude muset nejpozději po roce a deseti dnech nahlásit NÚKIB. Připomínkové místo s vypořádáním souhlasí.
133. Česká rektorů	konference	D	K § 40 písm. e) e) zakázat orgánům a osobám, které k tomu byly Úřadem vyzvány, používání technických aktiv v případě, že jsou taková Z navrhovaného textu předpisu není jasné, o jakou výzvu se má jednat. Z důvodu nespecifičnosti tak navrhneme vypustit.
			Neakceptováno - nyní § 41 odst. 1 písm. d) Možnost zakázat orgánům a osobám, které k tomu byly Úřadem vyzvány, používání technických aktiv míří na situaci, kdy je žádané zakázat orgánům a osobám technická aktiva, nicméně lze očekávat, že by v případě zákazu u některého ze subjektů mohlo dojít k tak výraznému narušení poskytované služby, že by zákaz aktiva způsobil větší škodu než užitek. Jde tak o nástroj pro omezení okruhu adresátů tak, aby byl výsledný efekt pozitivní. Připomínkové místo s vypořádáním souhlasí.
134. Česká rektorů	konference	Z	K § 41 odst. 5 Doplnění činnosti: <u>poskytovatelům regulovaných služeb v režimu vyšších povinností poskytuje své vyjádření ke kybernetickému bezpečnostnímu incidentu</u> V ustanovení § 18 odst. 1) je uvedeno: „<u>Úřad nebo Národní CERT poskytne bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení podle § 17, poskytovateli regulované služby své vyjádření ke kybernetickému bezpečnostnímu incidentu.</u>“ Tato povinnost však pak není provozovateli stanovena v § 41. Úřad může činit toliko to, co mu zákon umožňuje, a proto se domníváme, že by bylo vhodné předmětné ustanovení doplnit.
			Neakceptováno - nyní § 44 odst. 5 Vyjádření ke kybernetickému bezpečnostnímu incidentu ze strany Vládního CERT je součástí činností souvisejících se zvládáním a koordinací kybernetických bezpečnostních incidentů, které jsou zakotveny v § 44 odst. 5 písm. a) bod 4 navrhovaného znění zákona. Jelikož je zvládání upraveno v § 18, není nutné tuto povinnost znovu zmiňovat. Připomínkové místo s vypořádáním souhlasí.

135. Česká rektorů	konference	Z	K §42 odst. 3 písm. c) Doplnění činnosti: <u>poskytovatelům regulovaných služeb v režimu nižších povinností poskytuje své vyjádření ke kybernetickému bezpečnostnímu incidentu, metodickou podporu, pomoc a součinnost při výskytu a zvládání kybernetického bezpečnostního incidentu s významným dopadem a při zveřejňování informací o zranitelnostech v oblasti kybernetické bezpečnosti.</u> V ustanovení § 18 odst. 1) je uvedeno: „<u>Úřad nebo Národní CERT poskytne bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení podle § 17, poskytovateli regulované služby své vyjádření ke kybernetickému bezpečnostnímu incidentu.</u>“ Tato povinnost však pak není provozovateli stanovena v § 42 odst. 3.	Neakceptováno – nyní § 45 odst. 1 písm. c) Vyjádření ke kybernetickému bezpečnostnímu incidentu ze strany Národního CERT je součástí pomoci a součinnosti při výskytu a zvládání incidentu, které jsou zakotveny (a tedy obsaženy) ve Vámi zmiňovaném ustanovení navrhovaného znění zákona. Jelikož je zvládání upraveno v § 18, není nutné tuto povinnost znovu zmiňovat. Připomínkové místo s vypořádáním souhlasí.
136. Česká rektorů	konference	Z	K § 54 odst. 3 písm. i) vs. § 67 odst. 1 Doporučujeme opravit používání zkratk pro řízené služby a poskytovatele řízené služby. Zkratka MSP je zavedena jednou pro řízené služby, podruhé pro poskytovatele řízené služby.	Akceptováno - nyní § 57 a § 68 Zkratka byla z § 57 odst. 3 písm. i) a j) odstraněna, resp. byla změněna celá struktura ustanovení, odstraněna byla i v § 68 odst. 1. Připomínkové místo s vypořádáním souhlasí.
137. Česká rektorů	konference	Z	K § 59 odst. 2 Navrhujeme vypustit daný odstavec. Kromě toho, že se dané ustanovení může jevit jako narušující současné pojetí a použitelnost materiálního korektivu, také je formulováno formou vyvratitelné domněnky a tím pádem fakticky zbytečné.	Akceptováno - nyní § 61 Připomínkované ustanovení bylo z návrhu zákona vypuštěno. Připomínkové místo s vypořádáním souhlasí.

138. Česká rektorů	konference	Z	K § 65 odst. 3 Navrhujeme vypustit z daného odstavce nepřipustnost rozkladu proti rozhodnutí o určení regulované služby podle § 5. Zatímco v případě rozhodnutí o výmazu je nepřipustnost rozkladu pochopitelná, rozhodnutí o určení regulované služby může pro daný subjekt představovat podstatně zásadnější zásah do práv a povinností, mělo by tak být možné proti němu podat rozklad. Institut přezkoumání splnění kritérií regulované služby a relevance zápisu do evidence poskytovatelů nemůže tuto možnost v plném rozsahu a srovnatelné efektivitě nahradit, zejména z pohledu vznikuvších povinností a včasnosti opravy. Vybálcování dotčených zájmů provedené v důvodové zprávě se nám pak jeví jako nedostatečné a nepřesvědčivé.	Neakceptováno - Ustanovení bylo zrušeno a jednotlivé jeho části byly přemístěny do příslušných částí návrhu zákona (zde § 5) Důvody pro vyloučení možnosti podat rozklad proti rozhodnutí o určení podle § 5 návrhu zákona jsou vedeny veřejným zájmem na rychlém a efektivním zařazení poskytovatele regulované služby do regulace. Jde o obdobnou situaci jako při určování provozovatelů základní služby podle současného zákona o kybernetické bezpečnosti, u něhož je také vyloučena možnost podat rozklad. Za dobu účinnosti současného zákona a určování provozovatelů základní služby se přitom nestalo, že by subjekt se svým určením nesouhlasil a podal proti rozhodnutí Úřadu žalobu. Vzhledem k zájmům, jejichž ochrana byla určováním provozovatelů základních služeb sledována (zejména národní bezpečnosti a ochrana obyvatelstva), bylo nutné, aby proces určování podle zákona o kybernetické bezpečnosti probíhal, pokud možno, bez výraznějšího zpoždění. Tyto důvody lze v plném rozsahu aplikovat i na určování subjektů podle § 5 návrhu zákona, a to tím spíše, že kritéria § 5 zákona mívají na strategické a vysoce důležité služby/subjekty (u nichž by narušením bezpečnosti jejich informačních systémů mohlo dojít k významnému ohrožení veřejné bezpečnosti, zdraví osob nebo majetku nebo jiných chráněných zájmů státu). Ve veřejném zájmu je tak provedení zařazení regulované služby do regulace co nejvíce v souladu se zásadou rychlosti a hospodárnosti, neboť neúměrným a nijak účelným prodlužováním celého procesu může být výše zmíněný zájem představující účel tohoto

			návrhu zákona ohrožen. Do doby registrace a zápisu do evidence regulovaných služeb tyto orgány nebo osoby nejsou odpovědné za zabezpečování svých systémů a hlášení incidentů. Jakékoli prodlužování procesu zařazení orgánů nebo osob do regulace návrhu zákona oddaluje okamžik, od kterého jsou tyto orgány a osoby odpovědné za zajišťování kybernetické bezpečnosti své organizace a ochranu poskytované služby. Určení regulované služby podle § 5 probíhá ve standardním správním řízení podle zákona č. 500/2004 Sb., přičemž v rámci správního řízení je jednak subjektu dána možnost se vyjadřovat k podkladům rozhodnutí a namítat nejrůznější skutečnosti zpochybňující závěry Úřadu, jednak je Úřadu dána povinnost se se všemi argumenty subjektu a důvody pro určení jím poskytované služby vypořádat v rámci odůvodnění rozhodnutí. Stejně tak není vyloučena možnost podat proti rozhodnutí Úřadu správní žalobu. Poskytovatel regulované služby má navíc kdykoli možnost podat žádost o výmaz z evidence regulovaných služeb (pokud se domnívá, že kritéria pro zařazení do regulace již nejsou splněna). Možnosti obrany jsou tedy i přes zvýšený zájem státu na rychlém a efektivním rozhodování zachovány. Připomínkové místo s vypořádáním souhlasí.
139. Česká konference rektorů	Z	K návrhu vyhlášky o regulovaných službách Požadujeme vypustit písm. b) v bodě 19.1 U mnoha výzkumných organizací (vč. VŠ a ústavů AV ČR, nebo VO zřízených jinými orgány než MŠMT) je podíl výzkumu na celkovém obratu malý a znamenalo by to, že pokud např. má v.v.i. AV ČR jeden jediný výzkumný projekt, který je financován z více než 50 %	Akceptováno jinak Došlo k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo

		z veřejných prostředků, spadá do režimu vyšších povinností. Je zcela dostatečné, aby tento režim byl definován citlivostí výzkumu (bod (a) v textu prvního odstavce 19.1.).	experimentálnímu vývoji. U vysokých škol se ovšem nedomníváme, že by požadavek byl shodně oprávněný jako u jiných výzkumných organizací. Vysoké školy jsou dlouhodobě diskutovanou skupinou v rámci regulace. V době, kdy se vedly diskuze nad tím, zda vysoké školy jsou orgány veřejné moci a měly by tak některé své systémy zabezpečovat v rámci významných informačních systémů, bylo ze strany vysokých škol opakovaně sdělováno, že by dávalo větší smysl regulovat je pro jejich vědeckou činnost. S tímto se Úřad dlouhodobě ztotožňuje a považuje vysoké školy pro jejich specifickou povahu institucí sloužících k vědě a výzkumu, stejně jako vzdělávání a současně nadaných právem rozhodovat o právech a povinnostech za zástupce skupiny, na kterou by se regulace v režimu vyšších povinností měla vztahovat určitě. Připomínkové místo s vypořádáním souhlasí.
140. Česká konference rektorů	Z	K návrhu vyhlášky o regulovaných službách Požadujeme vypustit bod 19.2 Velké výzkumné infrastruktury, pokud jsou provozovány organizacemi vyjmenovanými v bodě 19.1., s výjimkou eInfra (která je podle bodů l)-o) Vyhlášky strategicky významnou službou, jsou provozovány z definice dle zákona 130/2002 Sb., o podpoře výzkumu a vývoje, v otevřeném režimu a je tedy naprosto dostatečné je provozovat v režimu nižších povinností. Navíc, náklady na jednoho partnera v odhadovaném rozsahu 800-1 500 tis. Kč ročně (viz. důvodová zpráva Zákona) by v znamenaly až 50% růst nákladů na VVI při větším počtu partnerů (až 15, tj. 12-22,5 mil. Kč ročně při současném rozpočtu 40 mil. Kč – viz VVI v oboru SHV). I náklady na nižší povinnosti budou podstatné.	Neakceptováno Partnerské instituce velké výzkumné infrastruktury jsou spolu s hostitelskou institucí stěžejním prvkem zabezpečení fungování velké výzkumné infrastruktury, neboť obě skupiny se podílí na jejím financování a rozhodování o jejím fungování či alespoň strategickém směřování. Nadto je třeba si uvědomit, že i partnerské instituce mají za úkol zaměřit své řízení bezpečnosti na samotnou službu, která je regulována. To znamená, že v případě, že se partnerské organizace podílejí na velké výzkumné infrastruktuře, například pouze prostřednictvím jejího financování, nebude v rámci jejich organizace nalezeno podpůrné aktivum, na které by musely zavádět opatření. Stejně tak, pokud jsou

			vlastníkem pouze malé části samotné infrastruktury a tuto mají oddělenou od své ostatní infrastruktury, která není regulována, zaměřují své řízení bezpečnosti informací pouze na tuto část výzkumné infrastruktury, která představuje aktiva sloužící k poskytování výzkumné činnosti. Náklady na zabezpečení velké výzkumné infrastruktury „na hlavu“ tak budou reálně mnohem nižší, protože několikero institucí bude zabezpečovat pouze jednu sadu aktiv. Skutečnost, že velké výzkumné infrastruktury „jsou provozovány z definice dle zákona 130/2002 Sb., o podpoře výzkumu a vývoje, v otevřeném režimu“ (ačkoli Úřadu není zcela zřejmé, co je tím myšleno), nijak neneguje fakt, že výzkumná infrastruktura tvoří páteřní síť pro provádění excelentního základního a aplikovaného výzkumu a představuje platformu pro vývoj těch nejvyspělejších technologií vykazujících vysokou znalostní náročnost a potenciál pro uplatnění v inovativním zboží a službách s vysokou přidanou hodnotou. S ohledem na skutečnost, že velké výzkumné infrastruktury soustřeďují v rámci svých kapacit nadkritické množství materiálních, lidských a finančních zdrojů potřebných pro dosahování průlomových poznatků, které přinášejí znalostní řešení socioekonomických výzev, je veřejný zájem na zajištění dostatečné úrovně kybernetické bezpečnosti velkých výzkumných infrastruktur zcela zřejmý a odůvodněný. Připomínkové místo s vypořádáním souhlasí.
141. Ministerstvo školství, mládeže a tělovýchovy	Z	K důvodové zprávě, zvláštní část k § 61 na str. 157: V závěrečné větě druhého odstavce na předmětné straně důvodové zprávy požadujeme za slovo „děkan“ vložit slovo „fakulty“ a za slovo	Akceptováno

		„veřejné“ požadujeme vložit slova „či státní“. V čele vysoké školy může totiž stát jen rektor, nikoliv děkan, který stojí v čele fakulty. Úprava děkanů a rektorů vysokých škol je totožná i pro vysoké školy státní, je nutné proto výslovně zmínit i je.	Důvodová zpráva byla upravena. Připomínkové místo s vypořádáním souhlasí.
142. Digitální a informační agentura	Z	K § 27 a § 34 Navrhujeme upravit znění § 27 a § 34 návrhu zákona, popř. § 5 písm. a) ve spojení s částí 1., oddílem 1.1. bodem I. písm. a) přílohy návrhu vyhlášky regulovaných službách, kdy současné <u>navrhované znění těchto může být vykládáno tak, že každá činnost veřejné správy (jak je popsáno ve zmíněných částech vyhlášky) bude považována za strategicky významnou službu a dopadne na ni poskytování služby toliko z území České republiky</u> podle § 34 návrhu zákona. Tento výklad by vedl k výraznému omezení až nemožnosti poskytování řady služeb orgánům veřejné správy.	Akceptováno jinak – nyní § 28 a § 35 Připomínkované ustanovení § 35 bylo v odst. 1 upraveno tak, že "Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby ~~v nezbytném rozsahu, v rozsahu kritické části stanoveného rozsahu~~ ve stanoveném čase a kvalitě z území České republiky.". Tento nezbytný rozsah pak bude stanoven ve vyhlášce Úřadu. V případě veřejné správy budou stanovena kritéria dopadu kybernetického bezpečnostního incidentu v podobě narušení dostupnosti služby a nezbytným rozsahem pak budou jen ty služby veřejné správy, které budou naplňovat tato kritéria. Přičemž ta by měla zhruba odpovídat kritériím dopadu na úrovni kritická podle vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy. Reakce připomínkového místa: Pokud jde o transpozici směrnice NIS2, máme za to, že navrhované územní omezení směrnice NIS2 nepředpokládá, neboť se v této směrnici o tomto omezení nehovoří a předmětné ustanovení tedy zjevně nemá transpoziční povahu a je čistě národní provenience. Předkladatel se ostatně ani na žádné ustanovení směrnice NIS, které by jej podle jeho mínění nutilo předmětné ustanovení do české legislativy vtělit, neodkazuje. Pokud jde o vztah ke směrnici NIS2, tato nejen že předmětné omezení nepředpokládá, ale některá ustanovení této směrnice (např. recitály č. 37, 39, 40, 65 nebo 114) s

		přeshraničním poskytováním služeb a odpovídající spoluprací počítají a nijak se proti ní nevymezují. V recitálu č. 84 se uvádí, že je to právě přeshraniční prvek předmětných služeb, který vyžaduje harmonizaci formou unijního předpisu. Obsahově k ustanovení uvádíme, že na klíčovou námitkou spočívající v tom, že ustanovení by vedlo k výraznému omezení až nemožnosti poskytování řady služeb orgánům veřejné správy, předkladatel nijak nereaguje a ani upravená verze předmětného ustanovení ji neodklízí, protože jsme nuceni na uplatněné připomínce setrvat. Pokud předkladatel hovoří o různých skutečnostech („riziko nedostupnosti dat pro české orgány činné v trestním řízení, rizika spojená s nedostupností dat pro jejich faktickou vzdálenost v případech přírodních katastrof, války, havárie v datovém centru, ztráty konektivity, pandemie či jiných nepředvídatelných událostí na území cizích států“), které jsou podle něj důvodem pro zavedení popsaneého omezení, měl by uvést konkrétní případy těchto událostí, jejich dopadu do poskytování předmětných služeb a popis úvahy ohledně případných řešení a myšlenkou postupu, na jejichž základě dospěl předkladatel k závěru, že tato řešení nejsou možná vhodná či účinná a navrhované omezení je jediným možným řešením. Absence výše popsanych informací je o to palčivější, že mezi vyloučené země patří všechny ostatní země světa včetně jiných členských zemí EU. Absentuje také úvaha, na jejímž základě dospěl předkladatel k závěru, že navrhované omezení nenarušuje předpisy EU, zejména úpravu jednotného trhu. Závěrem spíše podpůrně uvádíme, že navrhované řešení je fakticky nesrozumitelnější než původně

			navrhované znění – územní omezení se sice nově týká jen „nezbytného rozsahu“, avšak tento bude vymezen podzákonným právním předpisem, jehož obsah může zpracován do určité míry arbitrárně a nelze vyloučit, že příliš obecně. To zejména ve spojení se sankčními ustanoveními považujeme za nevhodné. Po vypořádací schůzce: Na základě dohody byly zaslány aktualizované teze vyhlášek a vypořádání připomínky bylo odsouhlaseno.
143. Digitální a informační agentura	Z	<u>Vztah směrnice NIS2 a nařízení eIDAS</u> Směrnice NIS2 na základě jejího čl. 42 s účinkem ode dne 18. října 2024 zrušuje čl. 19 nařízení eIDAS (nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES). Čl. 19 nařízení eIDAS se týká řízení rizik ohrožujících bezpečnost poskytovaných služeb vytvářejících důvěru a notifikační povinnosti poskytovatelů služeb vytvářejících důvěru. Tato problematika se "přesune" ze samotného nařízení eIDAS pod NIS2 jakožto obecného horizontálního předpisu, respektive v ČR pod nový zákon o kybernetické bezpečnosti, který má nabýt rovněž účinnosti 18. října 2024. Nicméně nařízení eIDAS bude nadále obsahovat požadavky zejména pro kvalifikované poskytovatele služeb vytvářejících důvěru (čl. 24) s ohledem na specifika poskytování kvalifikovaných služeb vytvářejících důvěru. V rámci EU se aktuálně rovněž projednává revize nařízení eIDAS, která by měla k požadavkům směrnice NIS2 přidávat další doplňující požadavky týkající se řízení rizik u nekvalifikovaných a kvalifikovaných poskytovatelů služeb vytvářejících důvěru, notifikačních povinností a stanovovat povinnost spolupráce mezi kompetentní autoritou dle NIS2 a orgánem dohledu dle nařízení eIDAS. Pokud jde o poslední stav projednávání revize nařízení	Vysvětleno Vztah novelizovaného eIDAS a směrnice NIS 2 je ve směrnici NIS2 i v návrhu zákona řešen zintenzivněním spolupráce mezi orgány odpovědnými za dozor obou předpisů. Počítá se s tím, že oba orgány budou při dozoru subjektů spadajících do působnosti obou předpisů úzce spolupracovat, sdílet informace a postupovat ve shodě tak, aby byly povinné subjekty co nejméně zatěžovány, avšak současně byly naplňovány cíle obou předpisů. Zrušení čl. 19 eIDAS je ve směrnici NIS 2 stanoveno až k okamžiku uplynutí transpoziční lhůty, do té doby předpokládáme, že nabude účinnosti nový zákon o kybernetické bezpečnosti. Mezera v účinnosti povinností v oblasti zabezpečování informačních systémů poskytovatelů služeb vytvářejících důvěru by tedy neměla nastat. Směrnice NIS 2 reguluje všechny poskytovatele služeb vytvářejících důvěru (kvalifikované i nekvalifikované, viz čl. 2 odst. 2 písm. a bod ii) směrnice + odvětví 8. přílohy I) a rozrazuje je do jednotlivých kategorií následujícím způsobem: kvalifikovaní poskytovatelé všech velikostí jsou

		eIDAS, švédské předsednictví uzavřelo předběžnou politickou dohodu nad klíčovými aspekty revize nařízení eIDAS – viz tisková zpráva: https://www.consilium.europa.eu/en/press/press-releases/2023/06/29/council-and-parliament-strike-a-deal-on-a-european-digital-identity-eid/, přičemž konkrétní text se má dopracovat na technické úrovni. Předpokládáme, že revize nařízení eIDAS vstoupí v účinnost dříve než navrhovaný nový zákon o kybernetické bezpečnosti, což je zřejmě důvodem, že případná spolupráce mezi NÚKIB a DIA jakožto orgánem dohledu v oblasti eIDAS není v tuto chvíli v návrhu zákona o kybernetické bezpečnosti přímo upravena a základní povinnosti spolupráce budou upraveny v připravované revizi nařízení eIDAS. Směrnice NIS2 kategorizuje kvalifikované poskytovatele služeb vytvářejících důvěru jako základní subjekty ("essential entities"), nekvalifikované poskytovatele jako důležité subjekty ("important entities") - viz čl. 2 a 3 směrnice NIS2. Předpokládáme správně, že v budoucím prováděcím právním předpise dle § 4 odst. 2 návrhu zákona, resp. dle § 6 odst. 3 návrhu zákona bude reflektováno, že nekvalifikovaní poskytovatelé jsou v režimu nižších povinností a kvalifikovaní poskytovatelé služeb vytvářejících důvěru v režimu vyšších povinností? Dále podle čl. 21 odst. 5 směrnice NIS2 má Evropská komise přijmout implementační akty do 17. října 2024, kterými stanoví technické a metodické požadavky týkající se opatření k řízení bezpečnostních rizik rovněž pro poskytovatele služeb vytvářejících důvěru. Dovolujeme si Vás požádat, aby Digitální a informační agentura byla informována o průběhu prací na tomto implementačním aktu (filip.bilek@dia.gov.cz, radek.horacek@dia.gov.cz). Zároveň Vás prosíme o průběžnou neformální spolupráci, abychom mohli poskytovatele služeb vytvářejících důvěru průběžně informovat o aktuálním	zařazení do kategorie „essentials“ [viz čl. 3 odst. 1 písm. b) směrnice], velcí nekvalifikovaní poskytovatelé jsou taktéž zařazení do kategorie „essentials“ [viz čl. 3 odst. 1 písm. a) směrnice], střední, malí a mikro nekvalifikovaní poskytovatelé jsou zařazení do kategorie „important“ (viz čl. 3 odst. 2). Toto rozřazení bude reflektováno i v navrhované úpravě (návrhu vyhlášky o regulovaných službách, kde dojde k úpravě stávajícího návrhu služby 16.10). O průběhu příprav prováděcího aktu podle čl. 21 odst. 5 směrnice NIS2 vás budeme informovat samostatným přípisem. Připomínkové místo s vypořádáním souhlasí.
144. Digitální a informační agentura	Z	Důvodová zpráva k těmto paragrafům obsahuje následující informaci „Při zavádění postupů pro ověření totožnosti držitele jména domény mohou subjekty spravující a provozující registry TLD a registrátoři domén využívat prostředky pro elektronickou identifikaci vydané v	Akceptováno Do dotčeného ustanovení byl i s ohledem na připomínku jiného připomínkového místa doplněn

	<i>rámci kvalifikovaného systému elektronické identifikace.</i>“ Nicméně tyto paragrafy podle našeho názoru neobsahují výslovné zmocnění, že subjekty spravující a provozující registry TLD a registrátoři domén jsou oprávněny využívat pro identifikaci a autentizaci uživatelů prostředky pro elektronickou identifikaci vydané v rámci kvalifikovaného systému elektronické identifikace a současně nám není znám právní předpis, který by výslovně stanovil pro tyto subjekty povinnost ověřit totožnost (viz § 2 zákona č. 250/2017 Sb., o elektronické identifikaci). Bez výslovného zmocnění v návrhu zákona využívat prostředky pro elektronickou identifikaci vydané v rámci kvalifikovaného systému elektronické identifikace či bez existence právního předpisu, který by výslovně stanovil pro tyto subjekty povinnost ověřit totožnost jsme toho názoru, že s ohledem na konstrukt § 2 zákona č. 250/2017 Sb. by bylo diskutabilní přiznat právo využívat prostředky pro elektronickou identifikaci vydané v rámci kvalifikovaného systému pro identifikaci a autentizaci uživatelů.	odstavec (§ 37 odst. 4), který pokrývá vámi připomínkové. Reakce připomínkového místa: Pokud jde o vypořádání připomínky č. 144 týkající se možnosti pro subjekt spravující a provozující registry domén nejvyšší úrovně a registrátory domén využívat pro identifikaci a autentizaci uživatelů prostředky pro elektronickou identifikaci vydané v rámci kvalifikovaného systému elektronické identifikace, nesouhlasíme s navrženým zněním § 37 odst. 4. Podle našeho názoru navržené znění (zejména poslední věta zmíněného odstavce) není v souladu se zavedenými pravidly, za kterých se připojují kvalifikovaní poskytovatelé online služeb k Národnímu bodu pro identifikaci a autentizaci („NIA“) dle zákona č. 250/2017 Sb. Pokud by se prostřednictvím jednoho kvalifikovaného poskytovatele online služeb (zde subjekt spravující a provozující registry domén nejvyšší úrovně) připojovaly také další subjekty fakticky v roli kvalifikovaných poskytovatelů (zde registrátoři domén), jde to už mimo rámec „kontroly“ Národního bodu a mimo ustanovení zák. č. 250/2017 Sb. (viz § 18 odst. 1 kdo je kvalifikovaným poskytovatelem). Navrhujeme následující úpravy § 37 odst. 4: a) první část odstavce upravit takto (4) Subjekt spravující a provozující registr domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén mohou je oprávněn při zavedení postupů pro ověření totožnosti držitele jména domény využít přístup s využitím prostředku pro elektronickou identifikaci vydaného v rámci kvalifikovaného systému

		elektronické identifikace podle zákona upravujícího elektronickou identifikaci Odůvodnění: preferujeme využívat textaci, která se již vyskytuje v jiných zákonech (např. zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů) b) Poslední větu („Subjekt poskytující služby registrace jmen domén může přistupovat ke kvalifikovanému systému elektronické identifikace prostřednictvím subjektu spravujícího a provozujícího registr domén nejvyšší úrovně na základě uzavřené smlouvy.“) odstranit s tím, že subjekt poskytující služby registrace jmen domén není v případě přístupu přes jiný subjekt kvalifikovaným poskytovatelem podle zákona o elektronické identifikaci, tím je subjekt spravující a provozující registr domén nejvyšší úrovně. Mezi sebou nechť si tyto subjekty případně další interakce upraví smluvně, jak ostatně sám návrh předpokládá. To ale nemusí být v zákoně. Po schůzce: První věta dotčeného ustanovení byla na základě vyjádření připomínkového řízení přepsána na "Subjekt spravující a provozující registr domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén mohou při zavedení postupů pro ověření totožnosti držitele jména domény využít přístup s využitím prostředku pro elektronickou identifikaci vydaného v rámci kvalifikovaného systému elektronické identifikace podle zákona upravujícího elektronickou identifikaci." Možnost vzniku smluvního vztahu je v návrhu zákona výslovně zmíněna s ohledem na požadavky vyplývající z čl. 6 a 7 nařízení Evropského

		Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES a na základě výsledků konzultací s CZ.NIC z.s.p.o. Připomínkovému místu byl zaslán návrh nového znění § 37. Reakce připomínkového místa Rozumíme důvodům, proč NÚKIB preferuje větu „Subjekt poskytující služby registrace jmen domén může přistupovat ke kvalifikovanému systému elektronické identifikace prostřednictvím subjektu spravujícího a provozujícího registr domén nejvyšší úrovně na základě uzavřené smlouvy.“ v návrhu zákona ponechat. Podle našeho názoru však bude odpovědností správce domény CZ a jednotlivých registrátorů domén, aby byly následně schopni prokázat na základě čeho došlo k předání osobních údajů daného subjektu údajů už podle stávající právní úpravy ochrany osobních údajů včetně účelu zpracování osobních a není třeba toto výslovně upravovat v zákoně. Preferujeme tedy nadále smazání této věty z návrhu. Jsme toho názoru, že vysvětlení stran nutnosti smlouvy může být uvedena v důvodové zprávě. Citovaná věta podle našeho názoru nezakládá sama o sobě žádná práva a žádné povinnosti, nemá žádný normativní charakter. Pokud věta v zákoně nebude, právní stav zůstane stejný. Věta má tedy spíše charakter doporučení, upozornění, nebo vysvětlení a proto navrhuje doplnění jen do důvodové zprávy. V odstavci 3 paragrafu 37 se již teď navrhuje, aby správce domény CZ a jednotliví registrátoři domén zavedli veřejně dostupné zásady a postupy zajišťující

			přesnost a úplnost informací vedených v databázi, včetně postupů ověřování. A dále, že tyto zásady a postupy nesmí vést ke zdvojování shromažďovaných dat a za tímto účelem subjekt spravující a provozující registr domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén vzájemně spolupracují. Zde není uvedena povinnost uzavřené smlouvy mezi správcem domény CZ a jednotlivými registrátory domén ohledně spolupráce, takže nevidíme důvod, proč existenci smlouvy reglementovat v odst. 4. Nicméně jako kompromisní návrh případně dáváme ke zvážení, zda existenci smlouvy nepřesunout do odst. 3. Tj., že spolupráce mezi správcem domény CZ a jednotlivými registrátory domén probíhá na základě smlouvy: [...] „Za tímto účelem subjekt spravující a provozující registr domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén vzájemně spolupracují na základě uzavřené smlouvy.“ Dáváme ke zvážení, zda by neměla být rovněž specifikována případně forma smlouvy (písemná). Závěr Po konzultaci s dalšími připomínkovými místy bylo předmětné ustanovení upraveno a připomínkové místo s úpravou souhlasí. Připomínkové místo s vypořádáním souhlasí.
145. Českomoravská konfederace odborových svazů	Z	oK RIA K části 3.5 (sociální dopady) Žádáme o doplnění RIA o kvalitní vyhodnocení sociálních dopadů. Odůvodnění:	Neakceptováno Co se týče sociální dopadů, podle bodu 10.5 obecných zásad pro hodnocení dopadů regulace (RIA), účinných od 3. 2. 2016, se mezi sociálními dopady uvádějí zejména dopady na rodiny či na specifické sociální

	Národní úřad pro kybernetickou a informační bezpečnost uvádí v shrnutí závěrečné zprávy RIA v části 3.5, že návrh zákona nemá žádné sociální dopady. Toto hodnocení považujeme za nesprávné, protože v části 3.2 hovoří o poměrně zásadním dopadu na mezinárodní konkurenceschopnost, respektive na podnikatelské prostředí: Naopak nelze vyloučit určitý negativní dopad na konkurenční postavení podnikatelských subjektů v ČR v podobě redukce nabídky některých dodávek v důsledku omezení rizikových dodavatelů (tedy zejména dodavatelů pocházejících ze zemí mimo vnitřní trh EU), a tedy i omezený negativní dopad na mezinárodní konkurenceschopnost. Možné omezení okruhu subjektů na trhu může vést k nárůstu cen dodávaných technologií, a tedy i ke zvýšeným nákladům na straně regulovaných subjektů. Vzhledem k možnému snížení počtu dodavatelů technologií může dojít k dočasnému poklesu vzájemného konkurenčního tlaku, a tím pádem i ke snížení motivace k vytváření inovací. Bude však zvýšena celková úroveň bezpečnosti služeb a produktů, čímž dojde ke snížení investičních rizik spojených s dodavatelským řetězcem pro potenciální investory, obzvláště ze zemí, které bezpečnost dodavatelského řetězce již právně regulují. ČMKOS vnímá záměr státu na zajištění bezpečnosti strategicky významné infrastruktury, ale postup, který úřad zvolil, vyvolává značné pochyby o tom, že jde o proporcionální řešení popisovaného problému. V současné době kvůli ekonomické situaci, vládním politikám a vysoké inflaci je Česká republika zemí, kde reálná mzda klesá od čtvrtého čtvrtletí 2021. Průměrná česká mzda v prvním čtvrtletí letošního roku meziročně narostla o 8,6 %, což ovšem po zohlednění inflace, která ve stejném období dosáhla 16,4 %, znamená propad reálné průměrné mzdy o 6,7 %. Aktuálně se reálná průměrná mzda nachází jen mírně nad úrovni prvního kvartálu roku 2017. Kupní síla českých zaměstnanců se vrátila v čase o téměř šest let nazpět. Dvě třetiny zaměstnanců navíc pobírají mzdu nižší než průměrnou.	skupiny obyvatel a jejich práva, tj. např. na sociálně slabé, osoby se zdravotním postižením, národnostní menšiny, sociálně vyloučené nebo na zaměstnance. V rámci hodnocení lze mezi sociálními dopady uvést okolnosti mající dopad na zhoršení sociální rovnosti, dále pak pracovní právní vztahy, sociální začleňování, sdružování nebo kupř. práva menšin. S ohledem na výše uvedené máme za to, že v závěrečné zprávě RIA je správně uvedeno, že návrh zákona nebude mít sociální dopady. Pokud jde o Vámi uvedený případný nárůst cen, tak ve vztahu ke spotřebitelům se jedná o nepřímý dopad, který je již začleněn mezi ekonomické dopady na podnikatelské prostředí. Tyto dopady (společně se všemi zbývajících ekonomickými dopady, včetně těch pozitivních) jsou podrobně popsány v bodě 3.3 závěrečné zprávy RIA. S odkazem na poslední zmíněný bod je nasnadě zopakovat, že přesnou výši finančních dopadů není možné předem stanovit, přičemž veškeré předchozí požadavky na jejich vyčíslení vedly k vytvoření odhadů s nízkou vypovídací hodnotou. Připomínkové místo s vypořádáním souhlasí.

		Česká ekonomika je jednou z nejpomaleji rostoucích v EU a s jednou z nejvyšších inflací v EU, což je smrtící kombinace pro růst disponibilního příjmu domácností a schopnosti domácností dovolit si platit více za služby. Třináct měsíců v řadě už také klesají maloobchodní tržby, což ukazuje, že spotřebitelská důvěra klesá. Úřadem navržený mechanismus má přitom de facto potenciál k růstu cen, což úřad nepřímě přiznává v důvodové zprávě, ale vůbec se dále nezabývá tím, jak a zda se skutečně do cen zvýšené náklady promítnou. Zahraniční zkušenosti přitom ukazují, že podobné mechanismy jsou významně financované státem (USA) nebo vyvolávají tlaky na růst cen a na konsolidaci na trhu (Spojené království). Z důvodové zprávy vyplývá, že NÚKIB nepočítá s tím, že by stát jakkoli rozhodnutí o případném vyřazení dodavatele jakkoli kompenzoval podobně, jako v USA, je na místě analyzovat, zda nepovedou k růstu cen. Ve Spojeném království letos operátoři zdražovali měsíční paušály v rámci inflačních doložek a dalších příplatků o 15 až 17 procent a zároveň dochází k tlaku na konsolidaci na trhu. Analýza toho, jak se regulace projeví na koncových cenách, je tak na místě a NÚKIB by ji měl doplnit do důvodové zprávy / závěrečné zprávy RIA. Konsolidace je navíc častý důsledek zvýšených regulačních nákladů, které vedou k odchodu menších hráčů z trhu. To by mohlo způsobit v ČR zvýšení cen pevného připojení k internetu, které patří mezi nejnížší v EU. Zároveň je otázka, jak se promítne regulace do podnikání velkých mobilních operátorů, jejichž ceny v ČR jsou podle řady srovnání mezi nejvyššími v Evropské unii. ČMKOS tak požaduje, aby NÚKIB provedl pečlivou analýzu sociálních dopadů nového zákona o kybernetické bezpečnosti, především pak na koncové ceny mobilních a pevných služeb elektronických komunikací. Na základě této analýzy je pak třeba znovu vyhodnotit, zda zvolený postup je proporcionální problému, který chce řešit, a zda možné dramatické důsledky v oblasti	

		maloobchodních cen služeb, které vyplynou z takové regulace, nepřevýší benefity, o kterých NÚKIB píše v důvodové zprávě. Minimálně tato analýza musí dát veřejnosti a jejím zástupcům v zákonodárném sboru jasné informace o tom, jaký vliv bude mít výsledek regulace na jejich disponibilní příjmy.	
146. Akademie věd ČR	Z	K materiálu jako celku, k dopadu navrhované úpravy na výzkumné organizace: AV ČR navrhuje, aby výzkumné organizace provádějící pouze nebo převážně základní výzkum nebyly zařazeny mezi poskytovatele regulované služby. Pokud takový návrh nebude akceptován, požaduje AV ČR, aby tyto organizace byly alespoň zařazeny mezi poskytovatele regulované služby v režimu nižších povinností. <u>Zdůvodnění:</u> K návrhu zákona o kybernetické bezpečnosti je navrhováno vydání šesti podzákoných prováděcích předpisů ve formě vyhlášek. Teprve tyto podzákoné právní předpisy fakticky určí okruh povinných osob, na které se nová právní úprava bude vztahovat, a rozsah povinností, který jim bude uložen. Přestože jsou tyto podzákoné předpisy předkládány jako teze, považuje AV ČR za nezbytné se k nim vyjádřit z hlediska jejich dopadu na výzkumné organizace. Konkrétně AV ČR upozorňuje na <u>znění Vyhlášky o regulovaných službách</u>, a to bodu 19 dosud nečíslované přílohy vyhlášky. V tomto bodě je jako regulovaná služba uveden výzkum a vývoj jako jednotná kategorie, aniž by byly dostatečně reflektovány formy výzkumu prováděného různými výzkumnými organizacemi, jeho strategický význam a povaha výzkumné instituce jako takové. Zároveň znění tohoto bodu způsobuje výkladové nejasnosti, když rozlišuje mezi „výzkumnými organizacemi jejímž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj za účelem využití	Akceptováno Došlo k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji. Připomínkové místo s vypořádáním souhlasí.

	<i>tohoto výzkumu pro komerční účely“ a „jinými výzkumnými organizacemi“ s odkazem na seznam výzkumných organizací vedený MŠMT podle §33a zákona č. 130/2002 Sb., o podpoře výzkumu a vývoje.</i> Vyhláška ve své příloze v bodě 19 nijak nezmiňuje výzkumné organizace zabývající se výlučně nebo převážně základním výzkumem. Takové instituce proto zřejmě budou spadat pod zbytkový pojem „<i>jiné výzkumné organizace</i>“ a tedy do režimu vyšších povinností, protože jsou obvykle financovány z veřejných zdrojů z více než 50 %. V prostředí Akademie věd ČR to znamená, že režimu vyšších povinností by se musela podříditi pracoviště, která jsou spíše menší velikosti, pro zajištění požadovaných opatření nedisponují dostatečným finančním ani personálním vybavením, a přitom se zabývají pouze nebo převážně základním výzkumem, který nemá povahu citlivé výzkumné činnosti a jeho dopad na ekonomiku a strategické zájmy státu není zásadní. To není souladné s bodem (15) preambule, který uvádí, že zařazení jednotlivých subjektů do příslušné kategorie (základní nebo důležitý subjekt) by mělo přihlížet ke kritické míře důležitosti a odlišení jednotlivých režimů (vyšších a nižších povinností) má zajistit spravedlivou vyváženost mezi rizikem na jedné straně a správní zátěží na straně druhé. Směrnice NIS 2 v bodu (36) preambule uvádí, že výzkumné organizace by měly být chápány tak, že zahrnují subjekty, které se v <u>podstatné části</u> svých činností zaměřují na provádění aplikovaného výzkumu nebo experimentálního vývoje ve smyslu Frascati manuálu z roku 2015 vypracovaného Organizací pro hospodářskou spolupráci a rozvoj (OECD). V článku 6 bod (41) směrnice NIS 2 je pak výzkumná organizace definována jako subjekt, jehož <u>hlavním cílem</u> je provádět aplikovaný výzkum nebo experimentální vývoj za účelem využití výsledků tohoto výzkumu pro komerční účely, který ovšem nezahrnuje vzdělávací instituce.	

		<u>Z výše uvedeného vyplývá, že směrnice NIS 2 směřuje v oblasti výzkumu pouze na instituce provádějící aplikovaný výzkum nebo experimentální vývoj, zatímco instituce provádějící pouze nebo převážně základní výzkum z regulace vyjímá.</u> Implementující předpis tedy v tomto případě nepřevzal definici povinného subjektu tak, jak ji vymezila směrnice NIS 2, ale významně tento okruh rozšířil. To je z hlediska požadavků unijního práva samozřejmě možné, je ale třeba hodnotit přiměřenost takového opatření. Ostatně v bodě (77) preambule se uvádí, že by měla být prosazována a rozvíjena kultura řízení rizik zahrnující posuzování rizik a provádění opatření k řízení kybernetických bezpečnostních rizik úměrných hrozcím rizikům. Obdobný, důraznější požadavek je obsažen v bodech (81) a (82) preambule: <i>„... aby se zabránilo nepřiměřené finanční a administrativní zátěži pro základní a důležité subjekty, měla by být opatření k řízení kybernetických bezpečnostních rizik úměrná rizikům, kterým jsou dotčená síť a informační systém vystaveny“, a</i> <i>„... opatření k řízení kybernetických bezpečnostních rizik by měla být úměrná míře vystavení základního nebo důležitého subjektu rizikům a společenskému a ekonomickému dopadu, který by měl incident. Při zavádění opatření by měla být náležitě zohledněna rozdílná expozice základních a důležitých subjektů rizikům, jako je kritičnost subjektu, rizika, včetně společenských rizik, jimž je vystaven, velikost subjektu a pravděpodobnost výskytu incidentů a jejich závažnost, včetně jejich společenského a ekonomického dopadu.“</i> V souladu s článkem 21 mají členské státy zajistit, aby povinné subjekty přijaly vhodná a přiměřená opatření, která odpovídají existující míře rizika. Při posuzování přiměřenosti těchto opatření má být náležitě zohledněna míra vystavení subjektu rizikům, pravděpodobnosti výskytu incidentů, jejich závažnosti a případnému společenskému a ekonomickému dopadu.	

	Na řadu výzkumných organizací však navrhovaná právní úprava dopadá způsobem, který v žádném případě nelze považovat za přiměřený. Příkladem může být Slovanský ústav AV ČR, v. v. i., který v roce 2022 zaměstnával pouhých 36 pracovníků, resp. 32,49 FTE, z čehož 26,74 FTE představují vysokoškolsky vzdělání pracovníci výzkumných útvarů. Slovanský ústav AV ČR, v. v. i., se zaměřuje na výzkum v oblasti slavistických disciplín paleoslovenistiky, byzantologie, gramatické a lexikální struktury slovanských jazyků, dějin a teorie slovanských literatur v evropském kontextu, dějin meziválečné emigrace z bývalého Ruského impéria na území ČSR a dějin slavistiky. Případný kybernetický incident by mohl v nejhorším případě omezit činnosti ústavu na několik dní. Důvodová zpráva uvádí, že výše nákladů na zavedení a následné provádění bezpečnostních opatření se předpokládá ve výši mezi 800 000 Kč a 1 500 000 Kč vůči jednomu zabezpečovanému systému. Zároveň se nejedná o náklady jednorázové, další bude třeba každoročně vynakládat na udržování a revizi systému. Režim vyšších povinností zároveň představuje extrémní administrativní zátěž vyžadující potřebnou personální kapacitu. Opatření, která musí poskytovatel regulované služby v režimu vyšších povinností přijmout, jsou v poměru k hrozícím rizikům v tomto případě mimořádně nepřiměřená. Podobných případů lze přitom jen ve struktuře AV ČR najít celou řadu. V situaci, kdy je usilováno o snižování strukturálního deficitu státního rozpočtu a uvažuje se o snižování výdajů na vědu a výzkum, tak <u>nový předpis nutí výzkumné organizace zavádět opatření, která jsou finančně velmi náročná, a ochrana jimi zamýšlená je přitom nepřiměřená aktivům, které jsou předmětem této ochrany.</u> <u>Pokud tedy nová právní úprava zahrne do regulace i výzkumné organizace provádějící základní výzkum, čistě podle kritéria veřejného financování, jedná se o opatření, které je neproporcionální a nevhodné.</u>	

		<u>AV ČR proto navrhuje, aby výzkumné organizace provádějící pouze nebo převážně základní výzkum nebyly zařazeny mezi poskytovatele regulované služby. Pokud takový návrh nebude akceptován, požaduje AV ČR, aby tyto organizace byly alespoň zařazeny mezi poskytovatele regulované služby v režimu nižších povinností.</u> Vzhledem k závažnosti uvedené připomínky požadujeme, aby tato připomínka byla vzata na zřetel při dopracování materiálu.	
147. Státní úřad pro jadernou bezpečnost	D	<u>K § 2 odst. 1 písm. d)</u> Zde doporučujeme rozdělit definici do dvou samostatných písmen. V navrhovaném znění se totiž v rámci jednoho písmene definují rovnou dva pojmy a to „technické aktivum“ i „technické a programové prostředky a vybavení“.	Akceptováno jinak Na základě vícero připomínek směřovaných na znění této definice byla zvolena formulace „technickým aktivem technické a programové prostředky a vybavení, a to včetně průmyslových, řídicích nebo jiných obdobných specifických aktiv,“. Byl odstraněn demonstrativní výčet, kdy současně byla zachována část, kterou povinné osoby často opomíjí při identifikaci technických aktiv, na které se vztahují bezpečnostní opatření vyhlášek, potažmo zákona. Dle Úřadu, nově navrhované znění tak nad rámec velice obecné definice konkretizuje, že OT je součástí technických aktiv, což posiluje právní jistotu. Jsme toho názoru, že při tomto znění již nedochází k definici vícero pojmů v jednom bodu. Připomínkové místo s vypořádáním souhlasí.
148. Státní úřad pro jadernou bezpečnost	D	<u>K § 2 odst. 2 písm. a)</u> V rámci tohoto písmene se definuje „kybernetický prostor“. Tím se dle návrhu zákona rozumí digitální prostředí tvořené aktivy umožňující vznik, výměnu a další zpracování informací a dat. „Aktiva“ jsou pak výše v § 2 odst. 1 písm. a) definována jako primární a podpůrná aktiva a dle § 2 odst. 1 písm. c) se podpůrnými aktivy rozumí například i zaměstnanci, dodavatelé či objekty. Definice tedy do digitálního prostředí vtahuje například i zaměstnance či objekty.	Vysvětleno Z pohledu NÚKIB osoby a objekty do kyberprostoru patří, bez nich by byl kyberprostor nepoužívaný a z našeho pohledu nefunkční. Šlo z naší strany tedy o úmysl. Snažili jsme se inspirovat například výkladovým slovníkem kybernetické bezpečnosti, kde je kybernetický prostor definovaný „Kybernetický prostor – digitální prostředí umožňující vznik,

		To je minimálně z hlediska jazykového velmi zvláštní. Doporučujeme tedy ještě tuto definici nějakým způsobem zúžit nebo přepracovat. Chápeme, že aktivem může být prakticky cokoli relevantního, s čím je potřeba v rámci řízení kybernetické bezpečnosti počítat (a že se zaměstnanci či dodavateli, je potřeba v rámci řízení bezpečnosti informací také počítat), ale je otázka, zda je zařazení osob či objektů do definice kybernetického prostoru skutečně žádoucí. Dle důvodové zprávy to rovněž není zřejmé, jestli šlo v tomto případě o úmysl.	zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“. Je však velmi orientován na systémy a nezahrnuje právě osoby, objekty apod. Chápeme Vaši připomínku, že zařazením osob a objektů do definice není úplně ideální řešení, ale bohužel nás nenapadá jiné vhodnější řešení nebo úprava samotné definice. Pokud Vás napadá konkrétní návrh na úpravu definice budeme za něj rádi a věcně jej vyhodnotíme. Připomínkové místo s vypořádáním souhlasí.
149. Státní úřad pro jadernou bezpečnost	D	<u>K § 4 odst. 1 a 2</u> V případě těchto dvou odstavců se dle našeho názoru zbytečně dubluje zmocnění k vydání prováděcího právního předpisu, když se v odst. 1 říká, že kritéria pro identifikaci regulované služby stanoví prováděcí právní předpis a poté i v odstavci 2 se obdobně stanoví (tentokrát však s ohledem na vypočtená odvětví), že prováděcí právní předpis stanoví kritéria pro identifikaci regulované služby. Tato duplicita ve výsledku vnáší do daného ustanovení mírný zmatek v tom, že není jasné, zda se v prováděcím právním předpise stanoví nějaká obecná kritéria a pak zvláštní pro jednotlivá odvětví nebo ne. Doporučujeme tedy ještě tato dvě zmocnění přeformulovat – například tak, že druhá věta v odstavci 1 bude bez náhrady smazána.	Akceptováno Ustanovení byla na základě připomínek komplexně upravena. Připomínkové místo s vypořádáním souhlasí.
150. Státní úřad pro jadernou bezpečnost	D	<u>K § 5 písm. a)</u> Tento paragraf stanoví, co se dále rozumí regulovanou službou. Slovo „dále“ evokuje to, že se jedná o služby nad rámec těch stanovených podle § 4 a jeho prováděcího právního předpisu. To by bylo pochopitelné v případě, jak je to dále formulováno u § 5 písmen b) až d). Ustanovení § 5 však ale dále v písmeni a) říká, že má jít o službu uvedenou v prováděcím právním předpise stanovujícím kritéria pro identifikaci regulovaných služeb a pak je nutné splnit další podmínku uvedenou v bodech 1. až 4. Odůvodnění tuto problematiku osvětluje v poněkud jiném smyslu, když říká, že míří na orgány a osoby, které	Vysvětleno Pokud rozumíme připomínce správně, pokusíme se ji vysvětlit. Regulovanou službou ve smyslu § 4, resp. vyhlášky o regulovaných službách, je kombinace kritéria „služby“ a „poskytovatele regulované služby“ (tj. naplnění obou sloupců vyhlášky zároveň). V tomto duchu jsou služby v § 5 novými, jinými, regulovanými službami, i když odkazují na první sloupec zmíněné vyhlášky. Máme za to, že uvedení slova "dále" není v tomto smyslu problematické.

		poskytují některou ze služeb uvedených v prováděcím právním předpisu, avšak nedosahují potřebné velikosti v souladu s doporučením Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků nebo nenaplnují jiné kritérium poskytovatele regulované služby stanovené prováděcím právním předpisem (zjednodušeně tedy na orgány a osoby, které nenaplní kritéria pro identifikaci regulované služby). Jsou-li naplněna tato speciální kritéria, může pak NÚKIB rozhodnout, že daná služba je regulovanou službou, byť by její poskytovatel nenaplnil kritéria poskytovatele regulované služby stanovená prováděcím právním předpisem. Toto pravidlo však v textu ustanovení chybí a pouze se stanoví, že jde o službu uvedenou v prováděcím právním předpise stanovujícím kritéria pro identifikaci regulovaných služeb, a navíc musí být splněna alespoň jedna z dále vyjmenovaných podmínek. Takováto služba by ale byla regulovanou službou již na základě § 4. Dle našeho názoru je tedy nutné přidat do návrhu písm. a), že se jedná o subjekty, které nenaplnují některé kritérium dle prováděcího právního předpisu nebo nedosahují velikosti v souladu s doporučením Komise 2003/361/ES.	Připomínkové místo s vypořádáním souhlasí.
151. Státní úřad pro jadernou bezpečnost	D	<u>K § 16 odst. 6</u> V tomto odstavci se stanoví, že hlášením kybernetických bezpečnostních incidentů není dotčena informační povinnost podle jiného právního předpisu nebo přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů. Není zcela jasné, o jaké ustanovení tzv. nařízení GDPR by se mělo jednat. Toto ustanovení tedy zakládá pochybnost, zda by v případě, že kterýkoliv zákon zřizuje informační povinnost nějakých svých regulovaných subjektů, měl explicitně stanovit, že touto informační povinností není dotčeno některé z ustanovení nařízení GDPR. Doporučujeme tedy tuto skutečnost blíže vysvětlit v důvodové zprávě nebo ze zákona tento odstavec bez náhrady vypustit.	Akceptováno Formulace § 16 odst. 6 návrhu zákona vychází z § 8 odst. 1 účinného znění současného zákona o kybernetické bezpečnosti (zákona č. 181/2014 Sb., o kybernetické bezpečnosti, v účinném znění), které podle důvodové zprávy k novelizačnímu zákonu č. 205/2017 Sb. reaguje na čl. 33 nařízení GDPR. Do důvodové zprávy k návrhu zákona byl proto na základě Vaší připomínky doplněn odkaz na uvedené ustanovení nařízení GDPR. Připomínkové místo s vypořádáním souhlasí.
152. Státní úřad pro jadernou bezpečnost	D	<u>K § 62</u> V rámci tohoto ustanovení doporučujeme zcela změnit nadpis.	Akceptováno – nyní § 64

		V navrhovaném znění nadpis zní: „Vztah ke správnímu a kontrolnímu řádu“. V textu tohoto paragrafu se však žádný vztah ke správnímu či kontrolnímu řádu neřeší (jako například § 262 daňového řádu). Ustanovení pojednává o pořádkové a donucovací pokutě. Navíc není z navrhovaného znění jasné, za co by se pořádková pokuta podle odstavce 1 měla udělovat. Doporučujeme tedy formulovat nadpis například takto: „Pořádkové a donucovací pokuty“ a dále alespoň stručně (jak je tomu například v odstavci 2) vymezit, k čemu se tato pořádková pokuta vztahuje. Například za závažné stěžování postupu Úřadu.	Ustanovení bude přejmenováno na „Zajištění účelu a průběhu řízení“ a původní odst. 4, který zní „<i>Exekuce rozhodnutí Úřadu ukládajícího povinnost předat nebo jinak naložit s informacemi a daty se řídí ustanoveními správního řádu upravujícími exekuci odebráním movité věci</i>“, bude přesunut k § 26, ke kterému se vztahuje. Výčet situací, ve kterých je možné uložit pořádkovou pokutu, byl doplněn do důvodové zprávy. Doplnění v návrhu zákona nepovažujeme za nezbytné, neboť ustanovení § 64 odst. 1 až 3 návrhu zákona nestanoví specifické podmínky pro ukládání pokut, naopak se v tomto případě bude Úřad řídit obecnou úpravou obsaženou ve správním a kontrolním řádu, v nichž jsou dotčené instituty upraveny a jimiž bude Úřad při své činnosti vázán. Návrh zákona pouze speciálně upravuje výši pokut, které lze v uvedených případech uložit, a to zejm. z důvodu zjevné zastaralosti částek, se kterými obecné právní předpisy pracují, a naprosté disproporce ve vztahu k pokutám, kterým subjekty čelí za porušení povinností stanovených návrhem zákona. Připomínkové místo s vypořádáním souhlasí.
153. Výbor nezávislého ICT průmyslu	Z	Doplnění závěrečné zprávy z hodnocení dopadů regulace - hodnocení dopadů regulace nebylo provedeno dle závazných metodik a je nedostatečné. Návrh zákona sice obsahuje důvodovou zprávu a závěrečnou zprávu RIA, ta ale neobsahuje měření administrativní zátěže podnikatelů dle platné metodiky Ministerstva průmyslu a obchodu z července 2017. Tato metodika je přitom závaznou pro zpracování RIA tak, jak to uvádí na svých stránkách Úřad vlády. Metodika obsahuje vzorovou tabulku pro výpočet administrativní zátěže v právním předpise, kterou NÚKIB zjevně nepoužil, aniž by zdůvodnil, proč. Stejně tak neodůvodnil, proč nepoužil výše zmíněnou metodiku.	Neakceptováno Jak i samotná připomínka uvádí, hodnocení dopadů obsahuje hodnocení nákladů z několika různých zdrojů. Rozhodně není hodnocení dopadů shrnuto jednou větou, jak se snaží připomínkové místo naznačit. Veškeré zdroje, metodiky i důvody pro nemožnost stanovení konkrétního výpočtu, který připomínkové místo požaduje, jsou uvedeny napříč hodnocením dopadů, zejm. v kapitole 3.1, resp. ve všech odkazovaných metodikách, ze kterých je výpočet složen. Nad to bylo Úřadem provedeno ještě

	Má-li právní předpis dopadnout na přibližně šest tisíc subjektů z podnikatelské i nepodnikatelské sféry, není možné dopad na ně shrnout větou, že „není z pohledu regulátora možné vyčíslit dopady na rozpočty v podobě absolutního čísla, které by bylo dostatečně přesné. Z obdržených vyplněných dotazníků vyplýval extrémní rozptyl těchto předpokládaných nákladů.“ Úřad si mohl v průběhu zpracovávání návrhu zákona provést vlastní reprezentativní průzkum mezi potenciálními subjekty, případně si objednat studii od externího dodavatele, která by pomohla vyčíslit náklady a tak by byla zásadním vodítkem pro to, jak záměr NÚKIB implementovat směrnici a do zákona vložit národní úpravu bezpečnosti dodavatelského řetězce řešit a jakým způsobem. Místo toho bohužel provedl „dotazníkové šetření“ adresované – jak píše v závěrečné zprávě RIA - orgánům a osobám podle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti. To jsou ale v drtivé většině subjekty veřejné správy. NIS 2 přitom dopadne ve většině na subjekty ze soukromé sféry. Pokud úřad uvádí, že „Z obdržených vyplněných dotazníků vyplýval extrémní rozptyl těchto předpokládaných nákladů.“ pak je to důvod k provedení analýzy jiným způsobem, nikoli pouze k prostému konstatování toho, co se stalo. Dovolujeme si upozornit, že například studie think tanku CETA pro Asociaci provozovatelů mobilních sítí odhaduje, že náklady jen v mobilní síti – pokud bude potřeba vyměnit dodavatele v celé části sítě - se mohou vyšplhat až k 17,8 miliardám korun. Není tak možné v Důvodové zprávě říci, že „výši finančních dopadů není možné předem stanovit“. Naopak, je potřeba vytvořit takový analytický podklad, který tyto náklady odhadne. (Shrnutí studie CETA je zde: https://apms.cz/narodni-bezpecnost-chytre-za-stovky-milionu-tupe-iza-18-mld/). Už jen tato částka ukazuje, že dopad nového ZKB může být na podnikatelské prostředí extrémně významný a není možné jej v důvodové zprávě nechat nevyčíslený.	další šetření, na které připomínkové místo odkazuje. Tato metodika nevznikala „na zelené louce“, ale vycházela z metodik dříve prováděných průzkumů NÚKIB a Ministerstva vnitra, které zjišťovaly potřebu finančních zdrojů na kybernetickou bezpečnost pro státní úřady, ministerstva a Úřad vlády ČR. V přípravné fázi byla podoba celého výzkumu včetně teoretických východisek konzultována na jednáních se Svazem průmyslu a dopravy ČR, Svazem měst a obcí a Ministerstvem vnitra ČR. Členové výše zmíněných organizací a státní úřady měli možnost se k celému výzkumu s předstihem dostatečně vyjádřit, což v několika případech rovněž udělali. Četné připomínky byly do podoby dotazníkového šetření implementovány. Nicméně ve fázi provádění samotného průzkumu, zaslalo výsledky jen velmi malé procento subjektů oslovených prostřednictvím výše zmíněných organizací. Použitá metodika byla maximálně zaměřena na novou podobu připravované regulace, zohledňovala jak náklady na jednotlivá bezpečnostní opatření, tak otázku personálií a ve všech podstatných rysech se shoduje s metodikou Ministerstva průmyslu a obchodu, na kterou připomínka odkazuje. Uvedené hodnocení dopadů je dostatečné. Co se týká odkazování na studie CETA, která je reprezentována pouze dvoustránkovým shrnutím, na které připomínkové místo odkazuje, je třeba uvést, že Úřad opakovaně žádal o poskytnutí podkladů k této studii, jakož i metodiky a dalších relevantních informací. I přes opakované žádosti nebyly tyto informace poskytnuty. Na základě toho nelze k této studii přihlížet, neboť chybí podstatné informace o tom, jak a na základě čeho byla tato studie zpracována.

			Připomínka vypořádána.
154. Výbor nezávislého ICT průmyslu	Z	Návrh na doplnění závěrečné zprávy z hodnocení dopadů regulace – doplnění analýzy odůvodnění prověřování dodavatelského řetězce NÚKIB uvádí, že součástí návrhu zákona je zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce do českého právního řádu v souladu s usnesením Bezpečnostní rady státu ze dne 21. června 2022 č. 41. Usnesení ani zájem státu podobný mechanismus zavést nijak nerozporujeme. Zcela ale chybí jakýkoli analytický podklad, ze kterého by bylo patrné, z jakých dat úřad vychází a v jakém rozsahu je daný problém přítomný v České republice, tedy kolik potenciálně rizikových dodavatelů, na které by mechanismus dopadl, je přítomno v jakých částech infrastruktury subjektů, na které má mechanismus dopadnout. Dle zpráv z médií k podobnému kroku přistoupil například německý regulátor a ministerstvo vnitra, které mají na starosti regulaci kybernetické bezpečnosti. NÚKIB přitom v důvodové zprávě tvrdí, že: <i>Nezřídka se navíc stává, že identifikovaná hrozba, před níž Úřad vydal varování podle zákona o kybernetické bezpečnosti, není v analýze rizik povinných osob podle ZKB dostatečně, či dokonce jakkoli, reflektována.</i> <i>Přestože byla vodítka tohoto druhu ze strany správců této infrastruktury dlouhodobě požadována, k reflexi 5G Doporučení jeho adresáty po jeho vydání prakticky nedošlo; mnozí správci kritické informační infrastruktury v sektoru elektronických komunikací nadále uzavírají kontrakty na dodávky technologií do bezpečnostně citlivých částí své infrastruktury s dodavateli, kteří po vyhodnocení kritérií 5G Doporučení na první pohled nevychází jako důvěryhodní.</i> Tato tvrzení patří mezi část zdůvodnění toho, proč chce stát vůbec mechanismus zavést. Z tohoto textu z Důvodové zprávy vyplývá, že	Neakceptováno V rámci analýzy dopadů NÚKIB pracoval s maximálním množstvím dostupných dat, přičemž kontaktoval vybrané povinné osoby a svazy za účelem provedení dotazníkových šetření. Vzhledem k nemožnosti tyto dopady blíže vyhodnotit a specifikovat, což je rovněž způsobeno nemožností předvídat konkrétní dopady navrhované regulace, jsou tyto dopady popsány na určité úrovni obecnosti, kterou však NÚKIB považuje za vhodnou vzhledem k požadavkům na psaní dopadů regulace RIA. Je nasnadě dodat, že konkrétní dopady ke konkrétním subjektům ovšem budou řešeny ve spolupráci s relevantními subjekty (dle § 30 a 31) během projednání s relevantními orgány státu. V této fázi budou řešeny také dopady možného omezení nebo zákazu na daný okruh povinných osob. Připomínka vypořádána.

		úřad má zjevně z vlastní činnosti k dispozici analýzu reflexe Varování a analýzu reflexe 5G Doporučení mezi povinnými subjekty. Požadujeme, aby Úřad doplnil do důvodové zprávy data z těchto analýz. Dále požadujeme, aby Úřad provedl naprosto základní analýzu současného stavu mezi potenciálními budoucími povinnými subjekty mechanismu, ze které vyplýne: • Jaké dodavatele mají potenciální povinné subjekty v aktivech, u nichž ohodnotili dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní vysoká nebo kritická • Zda mají v praxi nasazenou mitigaci rizik spojených s dodavatelem, a případně jakou. • Zda zohledňují rizika spojená s dodavatelem, která úřad identifikoval v tezích prováděcího právního předpisu a která zveřejnil v „5G Doporučení“. Jsme přesvědčeni, že bez úplně základní analýzy statu quo není možné přistupovat k jakékoli další regulaci, protože úřad vůbec nemůže mít informace o tom, jak jsou v současnosti tato rizika potenciálními povinnými subjekty vnímána ve světle vydaných opatření a materiálů úřadu, a případně mitigována. Pouze na základě podobné analýzy (a dalších analýz, které zmiňujeme výše) je možné přistoupit k vhodnému zvolení regulačního nástroje, který má dospět k zamýšlenému efektu při zohlednění zásad proporcionality. Nakonec i v legislativních pravidlech vlády se uvádí, že „Přípravě každého právního předpisu musí předcházet podrobná analýza právního a skutkového stavu.“	
155. Výbor nezávislého ICT průmyslu	Z	Návrh na doplnění závěrečné zprávy z hodnocení dopadů regulace – vliv na plnění aukčních podmínek Některé subjekty na trhu elektronických komunikací jsou zároveň držiteli kmitočtových přidělů z aukcí kmitočtů z let 2017 a 2021. Podmínky spojené s přidělem kmitočtů představují například závazek velkoobchodní nabídky, závazek prioritního BB-PPDR, závazek národního roamingu pro PPDR, závazek pronájmu rádiových	Neakceptováno NÚKIB v rámci analýzy dopadů pracoval s maximálním množstvím dostupných dat, kvůli čemuž kontaktoval vybrané povinné osoby a svazy za účelem provedení dotazníkových šetření. Vzhledem k nemožnosti tyto dopady blíže vyhodnotit a specifikovat, což je rovněž způsobeno nemožností

		kmitočtů pro účely průmyslu 4.0, závazky týkající se pokrytí a podobně. Požadujeme doplnit do důvodové zprávy ve spolupráci s ČTÚ předpokládaný vliv mechanismu na plnění těchto závazků.	předvídat konkrétní dopady navrhované regulace, jsou tyto dopady popsány na určité úrovni obecnosti, kterou však NUKIB považuje za vhodnou vzhledem k požadavkům na psaní dopadů regulace RIA. Konkrétní dopady ke konkrétním subjektům ovšem budou řešeny ve spolupráci s relevantními subjekty (dle § 30 a 31) během projednání s relevantními orgány státu. V této fázi budou řešeny také dopady možného omezení nebo zákazu na daný okruh povinných osob Nutno dodat, že znění závazků je spojeno se strategicky významnými službami, což je taktéž uvedeno v dokumentu RIA. Aukční podmínky tedy neznemožníme a dotčené subjekty by tak měly být schopny plnit nadále. Připomínka vypořádána.
156. Výbor nezávislého ICT průmyslu	Z	K § 6 odst. 3 Požadujeme režim poskytovatele regulované služby stanovit přímo v zákoně (v příloze zákona) z důvodu regulační a právní jistoty. (3) Režim poskytovatele regulované služby je stanoven ~~prováděcím právním předpisem~~ v příloze tohoto zákona. Je-li orgán nebo osoba poskytující regulovanou službu určen rozhodnutím Úřadu podle § 5, je vždy poskytovatelem regulované služby v režimu vyšších povinností.	Neakceptováno. Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech [§ 3 a § 2 písm. d)], tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby [§ 3, ve spojení s § 2 písm. i) a k) a § 22a]. Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon [§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)], a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá [§ 3 a § 2 písm. b)]. Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními

			předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Připomínka vypořádána.
157. Výbor nezávislého ICT průmyslu	Z	K § 10 odst. 2 Je třeba přijmout dostatečnou lhůtu k tomu, aby byl subjekt vůbec schopen plnit požadované povinnosti vyplývající ze zákona tak, aby obstál při případné kontrole. Z tezí vyhlášek vyplývá, že některé povinnosti budou poskytovatelé regulované služby v režimu vyšších povinností muset realizovat pomocí zaměstnanců či kontraktorů s konkrétními znalostmi a dovednostmi, které nemusí být v dané organizaci dosud vůbec přítomni. Navíc musí dojít k revizi smluv s dodavateli a k další řadě plnění, které zajistí compliance. U menších poskytovatelů služeb elektronických komunikací může být velká komplikace vůbec nalézt vhodné lidi – pokud předpokládáme že po datu účinnosti zákona bude podobné subjekty poptávat velká část nově regulovaných subjektů, nemusí se na ně vůbec dostat. Je potřeba si uvědomit, že úřad bude regulovat nově až 2000 subjektů v odvětví elektronických komunikací, z nichž řada jsou mikropodniky v odlehlých venkovských oblastech. Požadujeme změnit text návrhu takto: <i>Poskytovatel regulované služby zapsaný v evidenci poskytovatelů regulovaných služeb je povinen plnit všechny povinnosti plynoucí mu ze zákona vůči zapsaným regulovaným službám nejpozději od</i>	Vysvětleno Den doručení písemného vyrozumění o zápisu do evidence regulovaných služeb je rozhodným datem, se kterým celý zákon pracuje i na jiných místech a počítá se od něj běh některých lhůt. Například jedna z hlavních povinností zavádět bezpečnostní opatření má na zavedení podle § 14 odst. 3 návrhu zákona lhůtu v délce jednoho roku a začíná běžet od tohoto rozhodného data. Neplatí tedy, že by tato povinnost začala platit ihned po doručení vyrozumění o zápisu do evidence. Toto ustanovení pouze říká, že od vyrozumění zápisu do evidence platí, že daná služba je regulovanou službou a poskytovatel regulované služby vůči ní musí plnit své povinnosti. Jednotlivé povinnosti pak vyplývají z dalších ustanovení a mají své samostatné lhůty. Připomínka vypořádána.

		<i>uplynutí šesti měsíců od okamžiku doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb až do okamžiku doručení vyrozumění o výmazu z evidence poskytovatelů regulovaných služeb podle § 11.</i>	
158. Výbor nezávislého ICT průmyslu	Z	K § 21 odst. 1 Směrnice v článku 23 odst 7, ze kterého vychází § 21 „Výstraha“ hovoří pouze o „významných“ incidentech, toto zúžení ale v § 21 chybí, požadujeme jej doplnit. Jinak je oprávnění NÚKIB informovat o kyberbezpečnostních incidentech prakticky bezbřehé. NIS 2 článek 23 odst 7: Pokud je nezbytné informovat veřejnost, aby se významnému incidentu zabránilo nebo aby se probíhající významný incident vyřešil, nebo pokud je zveřejnění významného incidentu jinak ve veřejném zájmu, může tým CSIRT některého členského státu nebo případně jeho příslušný orgán, případně týmy CSIRT nebo příslušné orgány jiných dotčených členských států po konzultaci s dotčeným subjektem informovat veřejnost o významném incidentu nebo požadovat, aby tak učinil daný subjekt. Požadujeme tedy § 21 odst 1 změnit takto: (1) Úřad je po konzultaci s dotčeným poskytovatelem regulované služby z důvodu ochrany vnitřního či veřejného pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn veřejnost informovat o významném kybernetickém bezpečnostním incidentu či o porušování povinností daných tímto zákonem, nebo dotčenému poskytovateli regulované služby rozhodnutím uložit, aby tak učinil sám.	Vysvětleno – nyní § 22 odst. 1 Od použití sousloví "významný incident" bylo upuštěno, protože má v kontextu zákona o kybernetické bezpečnosti jiný obsah (jedná se o incident, který naplňuje kritéria daná vyhláškou pro určení míry významnosti v kontextu hlášení incidentů ze strany poskytovatelů regulované služby v režimu nižších povinností). Významnost incidentu pak indikuje formulace „z důvodu ochrany vnitřního či veřejného pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu“, která stanoví, že Úřad musí mít pro zveřejnění incidentu některý z těchto závažných důvodů a právě zveřejněním incidentu by bylo možné těmto dopadům předejít, což okruh možností, kdy lze zveřejnění incidentu odůvodnit, značně omezuje. Běžně je totiž incident a informace o něm v rozsahu informací, pro které platí i výjimka ze zákona o svobodném přístupu k informacím obsažená v zákoně o kybernetické bezpečnosti, což plyne např. z ustanovení § 38. Jedná se tedy skutečně o prostředek ultima ratio a výjimku z pravidla o neposkytování informací o incidentech a svévoli Úřadu tak zabraňuje množství dalších ustanovení zákona o kybernetické bezpečnosti. Připomínka vypořádána.
159. Výbor nezávislého ICT průmyslu	Z	K § 22 odst. 2 Požadujeme vypustit kompletně celý § 22 odstavec 2. Varování je instrument, který je v ZKB nad rámec směrnice. V původním ZKB je	Vysvětleno – nyní § 23 odst. 2 Úřad nikdy neměl v úmyslu rozšiřovat okruh subjektů, kterých se varování týká, nad zákonem stanovenou

		Varování upraveno tak, že jeho obsahem není nic ekvivalentního tomuto odstavci. Jde tedy o typický gold-plating. V důvodové zprávě není nijak zdůvodněno, proč tento odstavec úřad do § 22 vložil. Navíc pokud úřad může „stanovit jinak“ jak poskytovatel regulované služby v režimu vyšších povinností Varování zohlední, znamená to významný prostor k širokému zásahu úřadu do svobody podnikání fakticky dle libosti. Úřad v důvodové zprávě správně píše, že <i>„Varování je ve svém důsledku závazné pro poskytovatele regulovaných služeb v režimu vyšších povinností, jelikož ti v rámci svého systému řízení bezpečnosti informací a řízení rizik jsou schopni zohlednit hodnotu dané hrozby či zranitelnosti.“</i>, pro existenci odstavce 2 tohoto paragrafu tedy neexistuje žádný logický důvod. Požadujeme změnit § 22 takto: § 22 Varování (1) Úřad vydá varování, dozví-li se o závažné kybernetické hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti. ~~(2) Poskytovatel regulované služby v režimu vyšších povinností zohlední varování v rámci stanoveného rozsahu, pokud Úřad nebo jiný právní předpis nestanoví jinak.~~ (23) Varování Úřad oznámí dotčeným poskytovatelům regulované služby a zveřejní jej na úřední desce Úřadu. Úřad varování nezveřejní, pokud by jeho zveřejnění mohlo ohrozit zajišťování kybernetické bezpečnosti, účinnost protiopatření vydaného podle tohoto zákona, jiné oprávněné zájmy státu nebo by na jeho základě bylo možné identifikovat orgán nebo osobu, která kybernetickou hrozbu, zranitelnost nebo s tím související kybernetický bezpečnostní incident ohlásila.	úroveň, tedy ani globálně, ani vůči poskytovatelům regulovaných služeb v režimu nižších povinností. Úřad toto ustanovení zahrnul pouze proto, aby v případech, kdy je zejména hrozba relevantní pouze pro některé odvětví, mohl navázat varování vůči naopak úžeji vymezenému počtu subjektů. Rozšířit varování na subjekty mimo zákon o kybernetické bezpečnosti pouhým rozhodnutím Úřadu by nebylo legální a rozšíření na poskytovatele regulované služby v režimu nižších povinností je neúčelné, jelikož tito neprovádějí povinně analýzu rizik, do které by mohli tuto změnu hodnoty hrozby či zranitelnosti implementovat. Tedy tato varianta není rovněž z pozice Úřadu relevantní. Toto je také příslušně doplněno do důvodové zprávy, aby o úmyslu Úřadu s použitím tohoto ustanovení nebylo pochyb. Co se týká jiného právního předpisu, který může subjekty zavázat k aplikaci varování, to vychází z faktu, že vzrůstá trend sektorové regulace, která zahrnuje mimo regulaci sektorovou i regulaci kybernetické bezpečnosti. Při její implementaci ze strany sektorových regulátorů zaznává, že by těmto regulátorům připadalo účelné ve svých předpisech zavázat některé subjekty, u kterých to systém řízení bezpečnosti umožňuje (jde o řízení prostřednictvím rizik) a jsou zároveň postaveni mimo dosah zákona o kybernetické bezpečnosti k tomu, aby se tyto organizace řídily varováními vydanými Úřadem. Z tohoto důvodu je tu ponechán prostor pro jiný právní předpis stejné právní síly, tedy zákon, k tomu, aby zavázal další povinné osoby k dodržování varování. Připomínka vypořádána.
160. Výbor nezávislého ICT průmyslu	Z	K dílu 5	Vysvětleno

	Požadujeme vynětí Dílu 5 z NZKB (a odstranění odkazů na ustanovení Dílu 5 v celém zákoně). Alternativně požadujeme minimálně schvalování mechanismu v podobě zvláštního zákonného předpisu mimo implementaci NIS 2. Mechanismus s NIS 2 nijak zásadně věcně nesouvisí a není nutné ho schvalovat současně. Navíc na evropské úrovni se zjevně připravuje podobná právní úprava v podobě Telecoms Act, který avizoval v rozhovoru pro deník Les Echos evropský komisař pro vnitřní trh Thierry Breton (https://www.lesechos.fr/tech-medias/hightech/thierry-breton-la-commission-soutient-les-etats-membres-qui-bannissent-huawei-1952702), je tak potřeba pečlivě zvážit (i s ohledem na naše další připomínky), zda je vhodná forma prověřování dodavatelů čistě národní úprava a zda není vhodné postupovat na úrovni celé EU. Zároveň samotná směrnice NIS 2 předpokládá celoevropské hodnocení dodavatelů v článku 22 „Koordinované posouzení bezpečnostních rizik kritických dodavatelských řetězců na unijní úrovni“ Ten předpokládá, že Skupina pro spolupráci může ve spolupráci s Komisí a agenturou ENISA provést koordinované posouzení bezpečnostních rizik dodavatelských řetězců u specifických kritických služeb IKT, systémů IKT nebo produktů IKT, přičemž zohlední technické, případně netechnické rizikové faktory. Dle našeho přesvědčení je vhodné postupovat v tomto ohledu na evropské a nikoli národní úrovni. Úřad sám v důvodové zprávě uvádí na straně 69, že kritéria jsou fakticky totožná, jaká navrhuje v mechanismu. Navíc tvrdí, že v podobě § 23 má k dispozici nástroj (reaktivní protiopatření) kterým může povinným osobám nařídít zohlednění výsledků koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců: <i>„Reaktivní protiopatření je zároveň v této podobě i nástrojem odrážejícím požadavek, který směrnice NIS 2 na členské státy klade</i>	Prověřování dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS 2 je procesně i pojmově spjato. Vyčlenění mechanismu mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České republice pro stát i soukromé subjekty. Koordinované posouzení rizik dle čl. 22 NIS 2 představuje proces posouzení rizik spojených s dodavateli na úrovni Evropské unie, kdežto mechanismus prověřování bezpečnosti dodavatelských řetězců, obsažený v aktuálním návrhu zákona o kybernetické bezpečnosti, představuje vnitrostátní proces hodnotící kritéria důležitá pro bezpečnost České republiky. Z tohoto důvodu se tyto dva systémy posuzování rizik, resp. hrozeb, procesně i co do kritérií posuzování liší. Konečně dodáváme, že využití reaktivního protiopatření jakožto nástroje odrážejícího požadavek stanovený v čl. 21 odst. 3 je možné v situacích, kdy bude koordinované posouzení dopadat na jiné subjekty, než jsou poskytovatelé strategicky významné služby. Připomínka vypořádána.

		<i>ve svém článku 21 odst. 3. Ten stanovuje členským státům povinnost disponovat nástrojem prostřednictvím kterého zajistí, aby povinné osoby, tedy poskytovatelé regulovaných služeb museli zohlednit výsledky koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců podle čl. 22 směrnice NIS 2.“</i> Pokud má NÚKIB k dispozici evropskou úpravu posouzení bezpečnostních rizik kritických dodavatelských řetězců fakticky se stejnými kritérii, jaké plánuje do národní úpravy, a nástroj kterým dokáže donutit povinné osoby zohlednit výsledky tohoto posouzení, pak je na místě otázka, k čemu je mechanismus na národní úrovni vlastně potřeba.	
161. Výbor nezávislého ICT průmyslu	Z	K dílu 5 Alternativně, pokud NÚKIB neakceptuje připomínku č. 8, požadujeme: • Pečlivé odůvodnění v Důvodové zprávě a Závěrečné zprávě RIA, proč se stát nerozhodl jít v tomto případě kroky, které předpokládá směrnice NIS 2. Ta v článku 22 kodifikuje přesně to, čeho chce stát dosáhnout vlastním mechanismem - tedy posouzení bezpečnosti rizik dodavatelských řetězců u specifických kritických služeb ICT, systémů ICT nebo produktů ICT, a to se zohledněním technických, případně netechnických faktorů. V souladu se zásadou proporcionality by měl NÚKIB zdůvodnit, z jakého důvodu není toto ustanovení dostatečné a nevede k cíli, kterého chce stát dosáhnout. Je zcela legitimní otázka, zda článek není dostatečnou implementací mechanismu, jehož přípravu zadala NÚKIB Bezpečnostní rada státu ještě před tím, než bylo známo finální znění směrnice NIS 2, zvláště když Úřad sám v důvodové zprávě tvrdí, že v podobě § 23 NZKB má k dispozici nástroj (reaktivní protipatření) kterým může povinným osobám nařídít zohlednění výsledků	Neakceptováno Koordinované posouzení rizik dle čl. 22 směrnice NIS 2 představuje proces posouzení rizik spojených s dodavateli na úrovni Evropské unie, kdežto mechanismus prověřování bezpečnosti dodavatelských řetězců, obsažený v aktuálním návrhu zákona o kybernetické bezpečnosti, představuje vnitrostátní proces hodnotící kritéria důležitá pro bezpečnost České republiky, přičemž druhý z uvedených není implementací toho prvního. Tyto dva systémy posuzování rizik, resp. hrozeb, se proto procesně i co do kritérií posuzování liší, byť v obecnosti míří ke stejnému cíli. Z tohoto důvodu nelze při zachování potřeby omezování hrozeb specifických pro Českou republiku spoléhat pouze na posouzení dle čl. 22 směrnice NIS 2 a odkazovaný díl návrhu zákona vypustit. Co se týče odůvodnění výše naznačeného postupu, odkazujeme na zpracované odůvodnění návrhu zákona, závěrečnou zprávu hodnocení dopadů regulace a na rozdílovou tabulku.

		koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců. • Koordinované posouzení rizik dodavatelských řetězců na evropské úrovni by dle našeho pohledu odstranilo mnoho nejasností, které jsou bohužel přítomné v současném návrhu. Protože dle článku 22 specifické služby, systémy a produkty ICT určí Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA, nedojde k závažnému narušení jednotného trhu, kdy dnes reálně hrozí, že operátoři v jedné zemi (a v jedné podnikatelské skupině) budou moci využívat větší množství dodavatelů, než v zemi jiné. Tím se operátoři v zemi, kde stát úředně omezí množství dostupných dodavatelů, dostanou do konkurenční nevýhody, protože se jim logicky zvýší náklady - tím se stanou méně atraktivní pro potenciální investory a sníží se valuace jejich společností, což bude mít vliv na případný exit majitelů nebo na získání strategických investorů. NÚKIB by měl tyto aspekty zhodnotit podrobně v analýze RIA, kde zcela absentují. • Upozorňujeme, že existuje „Metodická pomůcka pro prevenci nadbytečné regulační zátěže při implementaci práva EU“ dostupná na stránkách Úřadu vlády. Podle kapitoly II „Předcházení nadbytečné regulační zátěži při neminimalistické implementaci“ by měl NÚKIB vždy posoudit, zda zvolen varianta implementace nepředstavuje nadbytečnou regulační zátěž a posouzení provést při hodnocení dopadů regulace. Požadujeme, aby NÚKIB dle této metodické pomůcky vyhodnotil, proč zvolil mechanismus prověřování dodavatelského řetězce jako národní variantu a nikoli společný postup v rámci EU a jeho uplatnění na regulované subjekty v ČR pomocí § 23 NZKB. • Případné omezení dodavatelů významně ovlivní investiční kapacitu a schopnosti především menších a středních firem investovat do rozvoje svých sítí. Pokud budou NÚKIB nějací dodavatelé omezení nebo zakázáni, pochopitelně to sníží	Přípomínka vypořádána.

		úroveň konkurence a zvýší ceny. Tento faktor musí NÚKIB zhodnotit v RIA v oddílu týkajícího se sociálních dopadů. • NÚKIB by měl také zhodnotit vliv na malé a střední podniky v RIA tak, jak to předpokládají příslušná pravidla.	
162. Výbor nezávislého ICT průmyslu	Z	K § 28 odst. 3a) Úřad sám pojmenoval onu část stanoveného rozsahu, kterou chce prověřovat, jako „kritickou část stanoveného rozsahu“. Přitom aktiva, která mají být předmětem prověřování jejich dodavatelů, jsou taková, u kterých bylo ohodnocené poskytovatelem strategicky významné služby jejich případné ohrožení bezpečnosti informací na úrovni vysoká nebo kritická. Dle našeho přesvědčení postačí, když budou předmětem prověřování pouze aktiva, u nichž poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotí dopad narušení bezpečnosti informací na stanovených rozsah strategicky významné služby na úroveň kritická. Zároveň jsme přesvědčeni, že identifikace podle prováděcího právního předpisu postačuje k tomu, aby NÚKIB dosáhl zamýšleného cíle, tedy že mechanismus bude prověřovat dodavatele aktiv, která jsou kritickou částí stanoveného rozsahu. Je to patrné i z toho, že v tezích vyhlášky jsou nepominutelné funkce stanovené pro síť a služby elektronických komunikací, ale nikoli pro subjekty v ostatních odvětvích stanovených v §27 odst 1. Požadujeme tak zrušit zákonné zmocnění úřadu vydat prováděcí právní předpis stanovující nepominutelné funkce stanoveného rozsahu. Rozsah mechanismu je navíc nutné zaměřit pouze na taková aktiva, u nichž má jejich nedostupnost přímý okamžitý dopad na nedostupnost strategicky významné služby, což je nejvýznamnější hrozba. Úřad by měl mít možnost zakázat rizikového dodavatele pro aktiva, jejichž výpadek může způsobit nedostupnost strategicky významné služby. Tento postup je s ohledem na princip proporcionality přiměřený. Odst 3a) tak požadujeme změnit takto:	Neakceptováno Nejprve bychom se rádi vyjádřili k úpravě nepominutelných funkcí na úrovni vyhlášky. Zde je nutno uvést, že úprava nepominutelných funkcí ve vyhlášce představuje proporcionální řešení konfliktu mezi širokým správním uvážením NÚKIB, obdobně zákona č. 34/2021 Sb., o prověřování zahraničních investic, a vymezením daných funkcí na úrovni zákona. Obdobný postup navíc již funguje v případě tzv. cloudové vyhlášky NÚKIB, tj, vyhláška č. 316/2021 Sb. Znovu uvádíme, že úprava kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, tak daná vyhláška bude procházet řádným legislativním procesem, v rámci kterého k ní mohou relevantní subjekty uplatnit své připomínky, jež je předkladatel povinen řádně vypořádat. Obdobný postup NÚKIB zvolil v případě zmíněné úpravy vyhlášky o zápisu do katalogu cloud computingu, kde toto nečiní žádné aplikační potíže. Nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu. Zároveň musíme poznamenat, že vyhláška o nepominutelných funkcích cílí na vše, co je v rámci fungování veřejných komunikačních sítí kritické, a to nehledě na pozici jednotlivých funkcí v topologii sítě. To znamená, že z pohledu kybernetické bezpečnosti je kritická funkčnost jak jádra sítě, tak také vybraných

		kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovni vysoká nebo kritická a jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby, ~~kritickou částí stanoveného rozsahu jsou vždy alespoň aktiva stanoveného rozsahu strategicky významné služby, která zajišťují nepominutelné funkce stanoveného rozsahu stanovené prováděcím právním předpisem,~~	funkcí ostatních částí sítě, jako například funkce v rádiové přístupové síti, bez nichž by jádro sítě nemohlo být propojeno s koncovými zařízeními, čímž by došlo k znefunkčnění takové sítě. Vzhledem ke komplexitě telekomunikačních sítí, ale také vysoké úrovni zpracování architektur těchto sítí na úrovni mezinárodních standardizačních organizací, má právě toto odvětví vlastní vyhlášku. V případě kompromitace těchto nepominutelných funkcí může být narušeno či porušeno nejen poskytování služeb koncovým uživatelům, ale také dalších strategicky významných služeb, které jsou na telekomunikacích závislé. Co do ochrany aktiv stanoveného rozsahu, která poskytovatel ohodnotil úrovní vysoká (v rámci připomínky se jedná o část „vysoká nebo“), tak zde, na základě předešlých zkušeností a zkoumání, NÚKIB konstatuje, že tato aktiva jsou kritická pro fungování strategicky významných služeb. Byť by se striktně jazykovým výkladem dalo dovodit, že je možné do kritického rozsahu sítě zahrnout pouze aktiva s dopadem „kritická“, nelze tak učinit. Co se týče ochrany aktiv stanoveného rozsahu, u kterých poskytovatel tyto ohodnotil úrovní vysoká, tak zde, na základě předešlých zkušeností a zkoumání (vyplývajících zejména z kontrolní činnosti NÚKIB), NÚKIB konstatuje, že tato aktiva jsou velmi důležitá až kritická pro fungování strategicky významných služeb. Aktiva ohodnocena jako vysoká mají podstatné dopady na primární aktiva, a tím pádem na chod celé strategicky významné služby. Ochrana pouze kritických aktiv by nebyla v plném rozsahu

			schopna pokrýt bezpečnost strategicky významné služby v doménách důvěrnost, integrita i dostupnost. Připomínka vypořádána.
163. Výbor nezávislého ICT průmyslu	Z	K § 28 odst. 3b) Úřad zde uvádí, že „pro potřeby mechanismu (...) se rozumí: <i>b) bezpečnostně významnou dodávkou plnění směřující do kritické části stanoveného rozsahu spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu</i> <i>1. technického prostředku nebo vybavení s výpočetní kapacitou,</i> <i>2. programového prostředku nebo vybavení, nebo</i> <i>3. informační či komunikační služby,</i> Požadujeme, aby v § 2 byly vymezeny všechny pojmy z tohoto odstavce, především pak bod 3, který není nijak vymezen. „Informační či komunikační služba“ je přitom extrémně vágní pojem, který je potřeba definovat zcela jasně. Nesplnění požadavků vyplývajících ze zákona s sebou nese vysoké riziko pokut, takže předpokládáme, že povinné subjekty by v rámci regulační opatrnosti NÚKIB informovali o všech dodavatelích, kteří se mohou být jen dotknout kritické části stanoveného rozsahu, mezi nimiž by při extenzivním výkladu pojmu „informační či komunikační služba“ mohly být třeba poskytovatelé služeb Public Relations (poskytují „komunikační“ služby managementu organizace, který může být „kritickou součástí stanoveného rozsahu“). I při méně extenzivním výkladu pojmu „informační či komunikační služba“ může do těchto služeb spadat například pronájem nenasvíceného vlákna, jejichž riziko narušení bezpečnosti informací může být ohodnoceno na úroveň vysoká nebo kritická, ale nikoli z důvodů kyberútoku, ale fyzického přerušení, což ale vůbec nesouvisí s tím, kdo je dodavatelem onoho vlákna.	Neakceptováno – nyní § 29 odst. 3 písm. b) Bližší vymezení pojmů § 29 odst. 3 písm. b) není žádoucí pro účel právní úpravy. Informační či komunikační služby je běžně zaužívaným neurčitým pojmem, se kterým pracovalo i předchozí znění zákona, a doposud se tento pojem nejevil jako problematický. Informační nebo komunikační službou jsou pak například služby cloud computingu nebo řízené služby. Informování úřadu o všech dodavatelích, kteří se mohou podílet na dodávání služby do kritické části stanoveného rozsahu, ať už sebemenším dílem, je cílem úpravy proto, aby Úřad měl informace o těchto dodavatelích a mohl vyhodnocovat rizika s nimi související. V případě pochybností s plněním povinnosti hlášení dodavatelů se pak mohou povinné subjekty obracet na Úřad. Obdobných pojmů také užívá například i zákon č. 127/2005 Sb., o elektronických komunikacích. Připomínka vypořádána.
164. Výbor nezávislého ICT průmyslu	Z	K § 28 odst. 3c)	Neakceptováno – nyní § 29 odst. 3 písm. c)

	Úřad zde uvádí, že „<i>dodavatelem bezpečnostně významné dodávky ten, kdo poskytovateli strategicky významné služby poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku.</i>“ V současné podobě návrhu bude subjektem mechanismu prakticky každý lokální a regionální subjekt, který poskytuje provozovateli „kritické součásti stanoveného rozsahu“ velkoobchodně jakoukoli bezpečnostně významnou dodávku podle § 28 odstavce 3b), což je ale fakticky jakákoli služba, protože NÚKIB definuje aktiva natolik široce, že „kritickou částí stanoveného rozsahu“ je podle návrhu fakticky celá síť poskytovatele sítě či služby elektronických komunikací. Důsledkem toho je, že mechanismus nedopadne jen na subjekty, u kterých to NÚKIB dle důvodové zprávy předpokládá, ale na stovky dalších subjektů. Úřad nebere v úvahu fakt, že sektor elektronických komunikací je extrémně propojen řadou dodavatelsko-odběratelských vztahů. Protože mechanismus úřad definuje extrémně široce fakticky jako celou síť, budou regulovanými subjekty i stovky malých a středních regionálních a lokálních operátorů, kteří poskytují velkoobchodní služby velkým národním operátorům. Zjevně jim neposkytují „kritickou“ službu (typicky pronájem vlákna či propoj základnové stanice s nějakým koncentračním bodem), ale přesto budou předmětem tlaku na změnu dodavatele od svých větších obchodních partnerů, protože budou součástí „kritické části stanoveného rozsahu“. To bude mít zásadní vliv na podnikání malých a středních regionálních firem, který není zohledněný v RIA (která má dle obecných zásad pro hodnocení dopadů regulace hodnotit dopad na podnikatelské prostředí „zejména s ohledem na osoby samostatně výdělečně činné a malé a střední podniky“). I z tohoto důvodu požadujeme změnit § 28 odst 3a skutečně jen na kritické části sítě, jak píšeme v připomínce č. 10	Z hlediska strategických hrozeb pro kybernetickou bezpečnost státu a strategicky významných služeb je nutno posuzovat jak dodavatele, tak také poddodavatele, jelikož skrz tyto může dojít k provedení stejného vektoru útoku, jelikož mají stejné možnosti v rámci možného ovlivnění dodavatelského řetězce. Co se týče kritické součásti stanoveného rozsahu a veřejné komunikační sítě, tak zde NÚKIB skrz vyhlášku o nepominutelných funkcích cílí na to skutečně nejkritičtější z hlediska fungování těchto sítí, nehledě na postavení jednotlivých funkcí v rámci architektury sítě. Kritické jsou jak funkce jádra sítě, tak také vybrané funkce rádiové přístupové sítě, bez kterých nemůže například dojít k propojení mezi koncovým zařízením a jádrem sítě. Obdobná ochrana navíc není v rámci EU ojedinělá, podobně kritické části sítě chrání také Dánsko, Belgie, Finsko či Lotyšsko. Co se týče ochrany aktiv stanoveného rozsahu, který poskytovatel ohodnotil úrovní vysoká (v rámci připomínky se jedná o část „vysoká nebo“), tak zde, na základě předešlých zkušeností a zkoumání, NÚKIB konstatuje, že tato aktiva jsou kritická pro fungování strategicky významných služeb. Byť by se striktně jazykovým výkladem dalo dovodit, že je možné do kritického rozsahu sítě zahrnout pouze aktiva s dopadem „kritická“, nelze tak učinit. Co se týče ochrany aktiv stanoveného rozsahu, u kterých poskytovatel tyto ohodnotil úrovní vysoká (v rámci připomínky se jedná o část „vysoká nebo“), tak zde, na základě předešlých zkušeností a poznání (vyplývajících zejména z kontrolní činnosti NÚKIB), NÚKIB konstatuje, že tato aktiva jsou velmi důležitá

			až kritická pro fungování strategicky významných služeb. Aktiva ohodnocena jako vysoká mají podstatné dopady na primární aktiva, a tím pádem na chod celé strategicky významné služby. Ochrana pouze kritických aktiv by nebyla v plném rozsahu schopna pokrýt bezpečnost strategicky významné služby v doménách důvěrnost, integrita i dostupnost. Připomínka vypořádána.
165. Výbor nezávislého ICT průmyslu	Z	K § 28 odst. 4 Úřad by neměl stanovovat „nepominutelné funkce stanoveného rozsahu“ (viz připomínka č. 10). Zároveň by kritéria rizikosti dodavatele neměly být v prováděcím právním předpise, ale přímo v zákoně (případně v příloze k zákonu). Pokud by byla tato kritéria stanovená pouze úřadem, reálně hrozí, že jakékoli příští vedení úřadu jmenované jakoukoli příští vládou bude mít naprosto odlišný názor na to, jaká mají tato kritéria být a bude je daleko snáze a rychleji moci měnit, což může způsobit zásadní regulační nejistotu. § 28 odst 4 tak požadujeme zcela vymazat. ~~Nepominutelné funkce stanoveného rozsahu a k~~ ~~Kritéria rizikosti~~ ~~dodavatele a způsob jejich vyhodnocení stanoví prováděcí právní~~ ~~předpis.~~	Neakceptováno - nyní § 29 odst. 5 Nejprve k úpravě nepominutelných funkcí na úrovni vyhlášky je potřeba říct, že úprava nepominutelných funkcí ve vyhlášce představuje proporcionální řešení konfliktu mezi širokým správním uvážením NÚKIB, obdobně jako v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, či zákona č. 34/2021 Sb., o prověřování zahraničních investic, a vymezením kritérií jednotlivých nepominutelných funkcí na úrovni zákona. Obdobný postup navíc již funguje v případě tzv. cloudové vyhlášky NÚKIB, tedy vyhlášky č. 316/2021 Sb. Nutno poukázat na argument, že úprava obdobných kritérií formou podzákoného právního předpisu je běžnou legislativní praxí, tak jak tomu bylo mimo jiné například v případě zmíněné vyhlášky č. 316/2016 Sb. V případě, že by mělo dojít ke změně této vyhlášky, tak taková změna bude procházet řádným legislativním procesem, v rámci kterého k ní mohou připomínková místa uplatnit své připomínky, které je předkladatel povinen řádně vypořádat. Případné nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu.

			Připomínka vypořádána.
166. Výbor nezávislého ICT průmyslu	Z	K § 28 odst. 4 V kritériích rizikovosti dodavatele nejsou nijak zohledněna kritéria technické a organizační povahy zajišťování kybernetické bezpečnosti. Zahnutí technických kritérií do hodnocení důvěryhodnosti dodavatelů byla přitom doporučena samotným úřadem v Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice z února 2022. Technické a organizační zajištění kybernetické bezpečnosti může být přitom vhodnou mitigací rizik vyplývajících ze „strategického“ posouzení dodavatele – minimálně by měl úřad a další orgány brát tato technická a organizační opatření v úvahu při rozhodování o rizikovosti dodavatele. Požadujeme tak do kritérií rizikovosti dodavatele doplnit technická a organizační kritéria a výslovně uvést do §4 vyhlášky (nebo do příslušného ustanovení zákona), že technická a organizační kritéria musí být brána v úvahu při vyhodnocování rizikovosti dodavatele a jako mitigační opatření.	Neakceptováno - nyní § 29 odst. 5 Technická kritéria by měla být dle názoru NÚKIB ponechána na posouzení povinných osob, jež tyto dokáží nejlépe vyhodnotit. Z toho důvodu je na státu a jeho organizačních složkách, včetně NÚKIB, posuzovat rizika na strategické rovině, tedy na základě strategických kritérií, ke kterým mají jednotlivé orgány státu relevantní informace. Obdobně se tak děje i v jiných zemích, včetně Spojených států amerických či Estonska. Zároveň je důležité zdůraznit, že nedůvěryhodnost dodavatele nelze v žádném případě mitigovat žádnými technickými ani organizačními opatřeními. Připomínka vypořádána.
167. Výbor nezávislého ICT průmyslu	Z	K § 30 Dle našeho přesvědčení není možné, aby do procesu omezování dodavatele, což je fakticky velmi zásadní a závažný zásah do svobody podnikatelského prostředí, byl zapojen pouze NÚKIB a ostatní státní orgány, především ty s politickou odpovědností, byly zapojené v procesu pouze okrajově poskytováním součinnosti či poskytováním informací. Problematika mechanismu prověřování bezpečnosti dodavatelského řetězce už jde daleko za hranice kybernetické bezpečnosti, ale směřuje k obecnému prověřování hrozeb pro bezpečnost České republiky její vnitřní a veřejný pořádek. V samotném návrhu se píše v § 28 odst. 1: <i>“Úřad shromažďuje a vyhodnocuje informace a data spojené s orgánem či osobou, které se týkají možné hrozby pro bezpečnost</i>	Neakceptováno - nyní § 31 Do procesu je zapojena Bezpečnostní rada státu, která je stálým pracovním orgánem vlády pro koordinaci problematiky bezpečnosti České republiky a přípravu návrhů opatření k jejímu zajišťování, ve které jsou členové vlády zastoupeni. V případě potřeby může samozřejmě problém eskalovat až na vládní úroveň. S tím také plyne procesní stránky věci, kdy Bezpečnostní rada státu může návrh opatření obecné povahy v případě, že je jí předložen, neprojednat, přerušit jeho projednávání, vrátit jej k přepracování, případně s ním vyjádřit nesouhlas. Jakékoliv rozhodnutí je pro Úřad samozřejmě závazné.

	<i>České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele“.</i> I kritéria pro hodnocení rizikovosti dodavatelů určená ve vyhláškách se vůbec nezaměřují na kybernetickou bezpečnost, na technologie nebo služby, ale čistě na vyhodnocení právního a politického prostředí země mající vliv na dodavatele a na osobu dodavatele. Pro oblast vnitřního a veřejného pořádku a bezpečnosti České republiky je ústředním orgánem státní správy Ministerstvo vnitra. Problematika prověřování bezpečnosti dodavatelského řetězce se dotýká i pravomocí dalších ústředních orgánů státní správy - zahraničního obchodu, hospodářské soutěže, bezpečnosti a integrity služeb veřejných komunikačních sítí a služeb elektronických komunikací. Omezení dodavatele je vysoce politickým krokem, který může mít zahraničněpolitické i ekonomické dopady a spolurozhodovat by tak měly orgány s politickým mandátem. Do procesu posuzování dodavatele požadujeme tak analogicky k zákonu o prověřování zahraničních investic zapojit vládu (odstavec 1-4) a sektorové regulátory (odstavec 5-6) Obdobně je tato problematika řešena na Slovensku v rámci § 27a odst. 3 zák. č. 69/2018 Z.z. o kybernetické bezpečnosti. Podle slovenské právní úpravy Národní bezpečnostní úřad Slovenska před vydáním rozhodnutí o omezení dodavatele, produktu, služby nebo procesu vyhotoví analýzu rizik na základě a v součinnosti s ostatními ústředními orgány státní správy, zpravodajskými službami a připraví návrh rozhodnutí. Návrh rozhodnutí potom předloží Bezpečnostní radě Slovenska a vládě. Od stanoviska vlády se potom Národní bezpečnostní úřad nemůže odchýlit. Navrhuje se řešit tuto problematiku v rámci českého návrhu zákona obdobně. Námi navrhovaný § 30 obsahuje navíc další bezpečnostní opatření, kterými poskytovatel strategicky významné služby musí pro aktiva nezařazená jím do kritické části stanoveného rozsahu provést analýzu rizik. V nich musí zohlednit rizika, která NÚKIB uvedl v OOP a	Úřad při vydávání opatření obecné povahy spolupracuje se všemi orgány státní správy, které jsou relevantní pro získání všech informací potřebných k tomu, aby byla dosažena maximální kvalita výsledného opatření obecné povahy, která se skládá z mnoha faktorů, například zvýšení bezpečnosti, dopady na poskytovatele strategicky významných služeb, dopady na hospodářskou soutěž, dopady na mezinárodní dohody, lhůta pro zohlednění opatření, dopady na další zákonné povinnosti poskytovatelů strategicky významných služeb a mnoho dalších. Toto v návrhu zákona ošetřeno v § 30 a nadto to vyplývá z obecných principů dobré správy. Připomínka vypořádána.

	vypracovat plán zvládání rizik, jehož součástí jsou i bezpečnostní opatření minimalizující rizika spojená s dodavatelem. Navrhujeme tak následující nové znění § 30: § 30 Omezení rizik spojených s dodavatelem 1. Zjistí-li Úřad na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, předloží věc k projednání Vládě České republiky (dále jen "Vláda"). 2. Vláda přijme do 45 dnů ode dne, kdy jí byla věc předložena k projednání, usnesení o tom, zda plnění dodavatele může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Při posuzování věci Vláda zohlední možný dopad plnění dodavatele na principy demokratického právního státu, ochranu života a zdraví obyvatel, obranu státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku. 3. V návaznosti na usnesení Vlády, že plnění dodavatele představuje významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, vydá Úřad opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu. 4. Usnesení Vlády je pro Úřad závazné a vydání opatření obecné povahy omezující či zakazující plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu je vydáním usnesení Vlády podmíněno. 5. Zakáže-li nebo omezí-li Úřad opatřením obecné povahy dle odstavce 3 plnění dodavatele, určí zároveň v opatření obecné povahy přiměřenou lhůtu zákazu nebo zohlednění podmínek plnění dodavatele. Lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy stanoví Úřad s přihlédnutím k jejich	

		dopadům na poskytovatele strategicky významné služby. Úřad vždy musí lhůtu předem konzultovat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele. 6. Před vydáním opatření obecné povahy je Úřad povinen projednat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele, zda návrh opatření obecné povahy a jeho možné dopady neohrozí plnění povinností stanovených a vyplývajících ze zvláštních právních předpisů. Úřad je povinen při vydání opatření obecné povahy stanovisko ústředního orgánu státní správy zohlednit. 7. Jestliže zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle odstavce 3 může ohrozit poskytování strategicky významné služby anebo představuje bezprostřední hrozbu kybernetického bezpečnostního incidentu, který podstatným způsobem ohrožuje poskytování strategicky významné služby, je poskytovatel strategicky významné služby povinen plnit opatření obecné povahy až po pominutí takové hrozby. 8. Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu opatření obecné povahy podávali připomínky. Lhůta pro podání připomínek činí 30 dnů, nestanoví-li Úřad jinak. Ustanovení § 172 odst. 1 a 5, § 173 odst. 1 věty první, část věty za středníkem, a § 173 odst. 1 věty druhé správního řádu se pro postup podle tohoto ustanovení nepoužijí. 9. V případě vydání opatření obecné povahy odstavce 3 musí poskytovatel strategicky významné služby provést analýzu rizik spojených s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3 pro aktiva strategicky významné služby, která nezařadil do kritické části stanoveného rozsahu podle § 28 odst. 3 písm. a). 10. Na základě analýzy rizik vypracuje poskytovatel strategicky významné služby plán zvládání rizik dle odstavce 9, v němž uvede bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3. Plán zvládání	

		rizik je poskytovatel strategicky významné služby povinen aktualizovat alespoň jednou za kalendářní rok. 11. Úřad přezkoumá alespoň jednou za 3 roky trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 3. Zjistí-li Úřad, že tyto skutečnosti pominuly, opatření obecné povahy zruší.	
168. Výbor nezávislého ICT průmyslu	Z	K § 55 odst. 1 Požadujeme změnu příslušného paragrafu ve světle připomínek výše (zrušení zákonného zmocnění k vydání prováděcích právních předpisů k ustanovením, která mají být v zákoně, případně mají být zcela vypuštěna). Prováděcí právní předpis stanoví a) kritéria pro identifikaci regulované služby (§ 4), ~~b) způsob stanovení režimu poskytovatele regulované služby (§ 6 odst. 3),~~ c) bezpečnostní opatření odpovídající režimu poskytovatele regulované služby a míru a způsob jejich zavedení a provádění (§14 odst. 2 a 4), d) způsob stanovení významného dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby v režimu nižších povinností (§ 16 odst. 3), e) obsahové náležitosti, formát a způsob oznámení provedení protiopatření a jeho výsledku (§ 20 odst. 3), ~~f) kritéria pro identifikaci strategicky významné služby (§ 27 odst. 1),~~ ~~g) nepominutelné funkce stanoveného rozsahu (§ 28 odst. 4),~~ ~~h) kritéria rizikovosti dodavatele a způsob jejich vyhodnocení (§ 28 odst. 4),~~ i) způsob hlášení údajů subjektem poskytujícím služby registrace jmen domén (§ 35 odst. 1) a j) technické a organizační podmínky používání Portálu NÚKIB, obsahové náležitosti, formát, strukturu a způsob provádění úkonů	Akceptováno jinak Celý § 55 byl zrušen s tím, že zmocnění k vydání prováděcích právních předpisů je uvedeno u jednotlivých ustanovení, kterých se týkají. Režim poskytovatele a strategicky významná služba byly upraveny tak, aby základní pravidla byla již v návrhu zákona. Prováděcí právní předpis ke kritériím rizikovosti dodavatele byl zrušen. Nepominutelné funkce stanoveného rozsahu bude dále stanovovat vyhláška; zmocnění k jejímu vydání je přímo v textu ustanovení, které se týká prověřování rizik spojených s dodavatelem. Připomínka vypořádána.

		uvedených v § 44 odst. 2 (§ 44 odst. 3).“	
169. Výbor nezávislého ICT průmyslu	Z	<u>K příloze k Vyhlášce o regulovaných službách - Kritéria pro identifikaci regulované služby</u> Požadujeme ve vyhlášce o regulovaných službách v Příloze v bodě 16.1 a 16.2 sjednotit kritéria na 350 000 SIM karet nebo pevných přípojek. Alternativně obě tato kritéria zrušit a ponechat pouze dělení vyplývající ze směrnice. Odůvodnění: Na českém trhu je běžné, že řada operátorů provozuje své sítě jako holding menších společností. Jde o reziduum toho, že některé operátorské skupiny zvláště regionálních hráčů vznikly tak, že provedly akvizice menších hráčů. Protože operátoři mají různé využití technologie, různé dodavatele, různé topologie sítí a různou praxi v nasazování technologií do sítě, má smysl docházet k nějakému sjednocování až v určitém čase, případně - pokud tak operátorské holdingy seznají, že je to vhodné - k technologické unifikaci nedojít vůbec. Takto vzniklé skupiny mohou překonat NÚKIBem stanovený limit 100 tisíc aktivních pevných přípojek, ačkoli de facto jde o malé podniky. Vzhledem k této běžné praxi jsme přesvědčeni, že by NÚKIB měl ustoupit od stanovení objemových kritérií v oblasti pevných sítí, nebo je sjednotit se stanoveným limitem pro mobilní sítě (350 tisíc aktivních přípojek). Dobrou orientaci pro tržní poměry na trhu pevného internetu má Český telekomunikační úřad, který vydává přehled o trhu ve svých výročních zprávách https://www.ctu.cz/vyrocní-zpravy. Objemový požadavek, pokud by měl být zachován, by měl kvantifikovat nikoliv počet přípojek celkem, ale počet přípojek v rámci jedné infrastruktury. Zároveň žádáme o upřesnění toho, jak bude NÚKIB postupovat v případě operátorů, kteří nabízejí své služby formou tzv. Fixed Wireless Access (FWA) na kmitočtech, které jsou určené pro služby IMT	Neakceptováno Teze prováděcích právních předpisů jsou sice již teď součástí předkládaného materiálu, ale budou následně předmětem samostatného připomínkového řízení při procesu jejich vydávání. Nelze předpokládat, že jedna pevná přípojka (typicky jedna domácnost) odpovídá jedné osobě (tj. jedné SIM kartě), z pohledu účelu právní úpravy tedy není vhodné uvedená kritéria sjednocovat. Pokud jde o konkrétní počty SIM karet a pevných přípojek, uvedený minimální počet aktivních přípojek byl stanoven tak, aby pokryl subjekty poskytující společně podle posledních dostupných dat Českého telekomunikačního úřadu (za rok 2021) většinu všech aktivních přípojek (cca 60 %). Minimální počet SIM karet pokrývá subjekty, které společně poskytují veřejně dostupné služby elektronických komunikací uživatelům většiny všech aktivních mobilních SIM karet na maloobchodním trhu (cca 92 %). V případě SIM karet je současně zohledněna skutečnost, že uvedené výrazně nadpoloviční většině poskytují veřejně dostupné služby elektronických komunikací pouze tři subjekty. Na subjekty poskytující tzv. Fixed Wireless Access (FWA) služby bude Úřad nahlížet obdobně jako ČTÚ, tedy podřazením FWA služeb pro regulační účely pod pevné služby. Důvodem je předpoklad, že FWA služby rovněž odpovídají potřebě spíše domácností než jednotlivců. Připomínka vypořádána.

			(3400-3800 MHz). Tito operátoři nabízí službu, kterou pro některé regulační účely ČTÚ označuje jako pevnou službu, ale zároveň ji nabízí na zařízeních, které mohou mít v sobě SIM kartu a služba je nabízena na kmitočtech harmonizovaných pro pohyblivou službu. Potenciálně mohou mít tito operátoři časem více než 100 tisíc zákazníků.	
170. Ministerstvo místní rozvoj	pro	D	K nadpisu návrhu V nadpisu návrhu zákona doporučujeme slova „Vládní návrh“ nahradit slovem „Návrh“ a slova „ze dne dd.mm.rrrr“ nahradit slovy „ze dne 2024“.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
171. Ministerstvo místní rozvoj	pro	D	K označení hlav a paragrafů Označení hlav a paragrafově značky včetně čísla paragrafu v návrhu zákona doporučujeme uvést netučně. Tučně doporučujeme ponechat pouze nadpisy hlav a paragrafů (např. nadpis hlavy Základní ustanovení , nadpis paragrafu Vymezení pojmů).	Akceptováno Připomínkové místo s vypořádáním souhlasí.
172. Ministerstvo místní rozvoj	pro	D	K nadpisu části třetí Z nadpisu části třetí doporučujeme vypustit slova „A ÚČINNOST“ a ponechat jen nadpis „ZÁVĚREČNÁ USTANOVENÍ“.	Akceptováno jinak. Část třetí byla zrušena a došlo k jejímu spojení s Částí druhou. Připomínkové místo s vypořádáním souhlasí.
173. Ministerstvo místní rozvoj	pro	D	V závěru návrhu zákona doporučujeme slova „V Praze dne dd.mm.rrrr“ a slova „Předseda vlády“ vypustit.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
174. Ministerstvo místní rozvoj	pro	D	K § 2 V § 2 odst. 1 písm. d) doporučujeme slovo „řídící“ nahradit slovem „řídící“.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
175. Ministerstvo místní rozvoj	pro	D	K § 65 V § 65 odst. 1 doporučujeme text „§ 8, § 9, § 10“ nahradit slovy „§ 8 až 10“.	Akceptováno jinak. § 65 byl zrušen Připomínkové místo s vypořádáním souhlasí.
176. Ministerstvo místní rozvoj	pro	D	K § 66 V § 66 doporučujeme slova „§ 30 a § 31“ nahradit slovy „30 a 31“.	Akceptováno Připomínkové místo s vypořádáním souhlasí.

177. Ministerstvo místní rozvoj	pro	D	K § 69 V § 69 odst. 1 písm. a) doporučujeme slova „ustanovení § 8, § 9, § 10, § 11, § 12“ nahradit slovy „§ 8 až 12“ a text „§ 13, § 14, § 15“ nahradit slovy „§ 13 až 15“.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
178. Ministerstvo místní rozvoj	pro	D	K § 70 V § 70 odst. 2 písm. a) a b) doporučujeme obdobnou úpravu jako v § 66 (vizte připomínku č. 7).	Akceptováno Připomínkové místo s vypořádáním souhlasí.
179. Ministerstvo místní rozvoj	pro	D	K § 72 Ve smyslu čl. 52 Legislativních pravidel vlády doporučujeme ve zrušovacím ustanovení výslovně uvést všechny právní předpisy (resp. jejich části), které obsahují novelu zákona, která se novým právním předpisem zrušuje. Doporučujeme tedy výslovně uvést všechny novely, které měnily zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Obdobnou úpravu doporučujeme i u prováděcích předpisů (vyhlášek).	Akceptováno Připomínkové místo s vypořádáním souhlasí.
180. Ministerstvo místní rozvoj	pro	D	K poznámkám pod čarou č. 7, 8 a 14 Ve výše uvedených poznámkách pod čarou doporučujeme slovo „Nařízení“ nahradit slovem „nařízení“.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
181. Ministerstvo místní rozvoj	pro	D	Ke zvláštní části důvodové zprávy – části šesté S ohledem na skutečnost, že účinnost zákona je navrhována dnem 18. října 2024, doporučujeme v odůvodnění ustanovení o nabytí účinnosti vysvětlit a zdůvodnit naléhavý obecný zájem ve smyslu § 3 odst. 4 zákona č. 309/1999 Sb., o Sbírce zákonů a o Sbírce mezinárodních smluv, ve znění pozdějších předpisů.	Akceptováno Ve zvláštní části odůvodnění byl k ustanovení týkající se účinnosti návrhu zákona doplněn následující text: "Vzhledem k tomu, že zde existuje naléhavý obecný zájem, spočívající v nutnosti implementace směrnice NIS 2 do určeného termínu, lze podle § 3 odst. 4 zákona č. 309/1999 Sb., o Sbírce zákonů a o Sbírce mezinárodních smluv, ve znění pozdějších předpisů, stanovit dřívější den nabytí účinnosti, než který je stanovený v odst. 3 tohoto ustanovení, tedy k 1. lednu nebo k 1. červenci kalendářního roku, nejdříve však počátkem dne následujícího po dni vyhlášení právního předpisu. V případě, že by nebyla směrnice NIS 2 implementována v řádném termínu, může Evropská

			komise zahájit s Českou republikou řízení o nesplnění povinnosti podle čl. 258 a násl. Smlouvy o fungování EU." Připomínkové místo s vypořádáním souhlasí.
182. Svaz průmyslu a dopravy ČR	Z	§ 2 Vymezení pojmů, odst. 2 písm f) a g), § 16 Hlášení kybernetických bezpečnostních incidentů odst. 1 a 2 Úprava definice ve smyslu vyloučení úmyslného zavinění Např: <i>kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v rámci aktiv v případě, že nelze vyloučit úmyslné zavinění</i> Rozumíme správně, že poskytovatelé v režimu vyšších povinností nemají povinnost hlásit NÚKIB tzv. provozní incidenty, které z povahy věci pod jeho působnost nespádají a incidenty, u kterých lze s jistotou vyloučit úmyslné zavinění a nemají pro vyhodnocování ze strany NÚKIB a další mapování bezpečnostní situace v kybernetickém prostoru zásadnější význam. Takto je i uvedeno v důvodové zprávě. Jak je nyní definováno v § 16, odst. 1, subjekty mají povinnost hlášení incidentů, které vznikly v kyberprostoru. Tato definice i na základě proběhlých jednání vyčleňuje z povinnosti incidenty, které vznikly neúmyslným zaviněním a případnou chybou samotného subjektu, např. při plánovaných pracích. V tomto smyslu hovoří i důvodová zpráva k Zákonu. Bylo by tedy vhodné upravit formulace samotného pojmu „kybernetický bezpečnostní incident“. NCSC definuje kybernetický incident jako porušení bezpečnosti aktiva (systému) s cílem ovlivnit jeho integritu nebo dostupnost nebo neoprávněný přístup nebo pokus o neoprávněný přístup k aktivu (systému) s cílem porušit jeho důvěrnost. Doporučujeme využít Metodiku k hlášení kybernetického bezpečnostního incidentu NÚKIB https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni-incidentu_1.1.pdf, která uvádí:	Akceptováno jinak Definice kybernetického bezpečnostního incidentu zůstala v návrhu zachována, na základě Vaší připomínky došlo nicméně k úpravě formulace § 16 odst. 1 na „<i>Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a nejsou způsobeny vlastní provozní činností.</i>“ Povinnost poskytovatele regulované služby v režimu vyšších povinností se proto nově nevztahuje na kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru, a zároveň jsou způsobeny vlastní provozní činností. Pokud jde o doporučení ohledně uvedené metodiky, k obsahu doporučení bude přihlédnuto při tvorbě nové metodiky, která bude připravena po přijetí návrhu zákona. Připomínkové místo s vypořádáním souhlasí.

		Rozumíme správně, že poskytovatelé v režimu vyšších povinností nemají povinnost hlásit NÚKIB tzv. provozní incidenty, které z povahy věci pod jeho působnost nespádají a incidenty, u kterých lze s jistotou vyloučit úmyslné zavinění a nemají pro vyhodnocování ze strany NÚKIB a další mapování bezpečnostní situace v kybernetickém prostoru zásadnější význam. Takto je i uvedeno v důvodové zprávě. Jak je nyní definováno v § 16, odst. 1, subjekty mají povinnost hlášení incidentů, které vznikly v kyberprostoru. Tato definice i na základě proběhlých jednání vyčleňuje z povinnosti incidenty, které vznikly neúmyslným zaviněním a případnou chybou samotného subjektu, např. při plánovaných pracích. V tomto smyslu hovoří i důvodová zpráva k Zákonu. Bylo by tedy vhodné upravit formulace samotného pojmu „kybernetický bezpečnostní incident“. NCSC definuje kybernetický incident jako porušení bezpečnosti aktiva (systému) s cílem ovlivnit jeho integritu nebo dostupnost nebo neoprávněný přístup nebo pokus o neoprávněný přístup k aktivu (systému) s cílem porušit jeho důvěrnost. Doporučujeme využít Metodiku k hlášení kybernetického bezpečnostního incidentu NÚKIB https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni-incidentu_1.1.pdf, která uvádí:	
183. Svaz průmyslu a dopravy ČR	Z	Důvodová zpráva Zákona o kybernetické bezpečnosti, § 17 Náležitosti hlášení kybernetických bezpečnostních incidentů V odst. 5 vypustit slova „nebo svévolným“ z věty <i>"Prvotní hlášení obsahuje informace o tom, zda existuje podezření, že incident byl způsoben nezákonným nebo svévolným zásahem, a zda je pravděpodobné, že bude mít přeshraniční dopad."</i> Incident, který vznikl svévolným způsobem nenaplnuje podmínky vzniku takového incidentu v kyberprostoru, jak zakládá znění § 16 odst. 1.	Neakceptováno Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnicí NIS 2, pokud bychom do návrhu zákona tuto úpravu nezahrnuli, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Obsahem prvotního hlášení podle čl. 23 odst. 4 písm. a) směrnice NIS 2 (ve směrnici označen jako včasné varování) je uvedení toho, "zda se [subjekty] domnívají, že byl významný incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad".

			Úřad tedy není oprávněn zasahovat v navrženém smyslu do znění dotčeného ustanovení návrhu zákona, nadto informace o případné svévolnosti incidentu představuje pro Úřad cennou informaci pro potřebu následné analýzy. Také pro incident vzniklý v kyberprostoru platí, že může být způsoben nesvévolně. Připomínkové místo s vypořádáním souhlasí.
184. Svaz průmyslu a dopravy ČR	Z	Zákon o bezpečnosti kybernetické -§ 4 Kritéria pro identifikaci regulované služby, Vyhláška o regulovaných službách Změnit formu prováděcího předpisu na nařízení vlády. V § 4 odstavec 1 nahradit slova „<i>prováděcí předpis</i>“ slovy „<i>vláda nařízením</i>“. V § 4 odstavec 2 nahradit slova „<i>Prováděcí předpis</i>“ slovy „<i>Vláda nařízením</i>“. Původní znění umožňuje NÚKIB, aby na základě vlastního uvážení rozhodoval o okruhu jím regulovaných subjektů, přičemž zákon nevylučuje, aby tento okruh byl rozšířen na libovolný subjekt v rámci vyjmenovaných odvětví. Taková míra koncentrace pravomocí v rukou jednotlivého orgánu veřejné správy je v demokratickém a právním státě nepřijatelná. Navrhovaná změna má za cíl přenést pravomoc určování rozsahu působnosti zákona o kybernetické bezpečnosti na Vládu ČR obdobně jako v případě nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které v současnosti určuje prvky infrastruktury, na něž dopadá nejprísrnější režim regulace dle zákona o kybernetické bezpečnosti.	ROZPOR Neakceptováno Právní forma nařízení vlády není pro danou regulaci odpovídající. Stanovení okruhu povinných osob, jejich režimu a dalších ustanovení pro něž je vydáván prováděcí právní předpis je analogicky nejpodobnější současnému nastavení vyhlášky č. 437/2017 Sb., o kritériích pro stanovení provozovatelů základní služby, což je spolu s § 22a současného zákona o kybernetické bezpečnosti způsob stanovení osobní působnosti transpozičních ustanovení předchozí směrnice NIS 1. Stejným způsobem je tedy přistupováno k transpozici směrnice NIS 2 - podstata věci se i přes rozdílnost směrnic v tomto případě nijak nemění. Stanovení okruhu povinných osob prostřednictvím prováděcího právního předpisu na základě a v mezích zákona (jak vyplývá z čl. 79 odst. 3 Ústavy) je v působnosti Úřadu. Z tohoto důvodu také není využito nařízení vlády, které má být využito jen v situacích, kdy se věc týká působnosti více než dvou orgánů nebo je dán naléhavý obecný zájem, což v tomto případě provedení běžného ustanovení zákona není. Stejně jako v případě dříve zaslaných podnětů v rámci neoficiálního podnětového řízení je potřeba opět upozornit, že domněnka navrhovatele, že je Úřadu

			dána pravomoc „na základě vlastního uvážení rozhodoval o okruhu jím regulovaných subjektů, přičemž zákon nevylučuje, aby tento okruh byl rozšířen na libovolný subjekt v rámci vyjmenovaných odvětví“, je mylná, protože přijímání každého právního předpisu je podmíněno řádně provedeným legislativním procesem, který umožňuje zapojení široké skupiny připomínkových míst, stejně jako v tomto případě, a také Legislativní rady vlády.
185. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 12 Hlášení údajů poskytovatelem regulované služby, odst. 2a a 2c , Vyhláška o portálu NÚKIB Vynechat požadované údaje, které má NÚKIB dostupné v základních registrech (například informace o vlastnické struktuře viz požadavek § 3 Vyhlášky o portálu NUKIB) Portál NÚKIB by měl být napojen na základní registry, tudíž by registrační a doplňující údaje měly být z velké části, ne-li všechny, z těchto registrů vyčteny.	Vysvětleno Počítáme s tím, že dojde k napojení na základní registry a k čerpání maximálního množství údajů z nich, tak aby docházelo k minimální administrativní zátěži regulovaných organizací. Nicméně náležitosti formulářů musí být v prováděcím právním předpise specifikovány tak či tak (vyplývá to z judikatury Ústavního soudu, která je zmíněna v důvodové zprávě). Takto je navíc transparentní, které údaje NÚKIB ze základních registrů získává a dále zpracovává. Výčet potřebných údajů je nezbytné ve vyhlášce v této podobě zachovat také pokud by se Portál NÚKIB nepodařilo napojit na základní registry k okamžiku účinnosti návrhu zákona. Připomínkové místo s vypořádáním souhlasí.
186. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 19 Informační povinnost poskytovatele regulované služby odst. 1 Doporučujeme doplnit následovně <i>„V rozhodnutí o uložení této povinnosti stanoví Úřad rozsah informační povinnosti. Zveřejnění informace nesmí ohrozit bezpečnost nebo provoz regulované služby a povinné osoby.“</i>	Akceptováno jinak – nyní § 20 odst. 1 Do dotčeného ustanovení bylo doplněno: „<i>po konzultaci s tímto poskytovatelem regulované služby</i>“. Uložení a rozsah informační povinnosti je po této konzultaci náležitě zvážen ze strany Úřadu. Úřad při rozhodování o zveřejnění informací o kybernetickém bezpečnostním incidentu vezme v rámci správního uvážení do úvahy potřebu zachování rovnováhy mezi

		Rozsah informační povinnosti není nijak upřesněn/omezen. NÚKIB tak může vyzvat ke zveřejnění informací bez znalosti celkového kontextu incidentu. Přílišná transparentnost může být v některých případech ohrozit bezpečnost regulovaných služeb a kritické infrastruktury.	zájmem uživatelů být informovanými o hrozbách a incidentech, a možném poškození pověsti poskytovatele regulované služby či ohrožení bezpečnosti regulované služby zasažené incidentem. Připomínkové místo s vypořádáním souhlasí.
187. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 21 Výstraha Doplnit následující formulaci: <i>Zveřejnění informace nesmí ohrozit bezpečnost nebo provoz regulované služby.</i> Zveřejnění klasifikovaných informací a případného nesouladu s tímto zákonem může vést k narušení bezpečnosti informací a samotného smyslu zákona zajistit bezpečnost regulovaných služeb.	ROZPOR Neakceptováno - nyní § 22 Nedomníváme se, že toto doplnění je nutné. Úřad v rámci správního uvážení bere do úvahy, jak informace získané při konzultaci s daným poskytovatelem regulované služby, tak i míru dopadu výstrahy na daného poskytovatele regulované služby a právě veřejný zájem musí v rámci testu proporcionality převážit nad dopady, které by to mohlo mít na danou organizaci. Běžně je incident a informace o něm navíc v rozsahu informací, pro které platí i výjimka ze zákona o svobodném přístupu k informacím obsažená v zákoně o kybernetické bezpečnosti. Jedná se tedy skutečně o prostředek <i>ultima ratio</i> a výjimku z pravidla o neposkytování informací o incidentech a svévoli Úřadu tak zabraňuje množství dalších ustanovení zákona o kybernetické bezpečnosti. Rovněž lze říci, že se jedná o institut, který již v obdobném znění byl součástí institutu varování i v současném znění zákona o kybernetické bezpečnosti a Úřad k takovému zveřejnění doposud nikdy neshledal dostatek důvodů.
188. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 25 Speciální úprava předání informací a dat od významného dodavatele odst. 1. Doporučujeme přeformulovat nebo upřesnit spojení „...hrozícího kybernetického bezpečnostního incidentu...“.	Akceptováno – nyní § 26 Definice hrozícího kybernetického bezpečnostního incidentu byla upřesněna. Úřad bude při zvažování

		Z textu zákona není zřejmé, jakou metrikou bude vyhodnocována míra hrozby incidentu, která se nelehko kvantifikuje, pokud takový incident ještě nenastal. Není zřejmé, kdo určí, že se jedná o hrozící incident, a tedy oprávněnost žádosti. Jedná se podle definice o Událost? O jaká data a informace se jedná, pokud incident ještě nenastal? Bez vyjasnění může docházet ke zneužití a nepřesným interpretacím.	dopadu incidentu brát v rámci správního uvážení v potaz vždy konkrétní okolnosti každého případu. V každém případě se bude jednat o informace a data související s provozem aktiv sloužících k poskytování regulované služby. Připomínkové místo s vypořádáním souhlasí.
189. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 25 Speciální úprava předání informací a dat od významného dodavatele odst. 1 <i>Za větu „Úřad může v rozhodnutí určit formát, rozsah, způsob a lhůtu předání a stanovit povinnost po provedení předání tyto informace a data a jejich kopie bezpečně zlikvidovat.“</i> doplnit: Formát, rozsah, způsob a lhůta předání informací nesmí jít nad rámec smluvních závazků. Je nutné respektovat smluvní ujednání.	Neakceptováno – nyní § 26 Toto ustanovení míří na krajní situace, kdy by hrozící či probíhající kybernetický bezpečnostní incident mohl mít závažný vliv na poskytování regulované služby s dopadem na zachování základních funkcí státu, hospodářských činností, bezpečnosti, veřejného zdraví, majetku nebo životního prostředí. V takovém případě převládá zájem státu na odvrácení incidentu s takto významným dopadem nad soukromoprávní dohodou o předání dat. Povinnost zanechat do smlouvy specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání povinnou osobou je součástí bezpečnostních opatření, která bude poskytovatel regulované služby v režimu vyšších povinností povinen zavádět. Vzhledem k tomu, že příslušná ujednání by měla být součástí smluvního vztahu mezi poskytovatelem regulované služby a významným dodavatelem, měl by institut předání dat podle § 26 sloužit jako <i>ultima ratio</i> až poté, co selžou jednání mezi dotčenými stranami. Do situace, kdy je smlouva jasně ujednána, vyhovuje oběma stranám a významný dodavatel se jejím plněním nebrání, Úřad nikdy zasahovat nebude. Připomínkové místo s vypořádáním souhlasí.

190. Svaz průmyslu a dopravy ČR	a Z	Zákon o kybernetické bezpečnosti - § 25 Speciální úprava předání informací a dat od významného dodavatele odst. 1 Na konec odstavce 1 § 28. doplnit větu „Úřad využívá data výhradně za účelem vyhodnocování rizikivosti dodavatelů“. Původní znění explicitně neomezuje účel sběru informací, účel žádostí ani charakter sbíraných a vyžadovaných informací. Absence těchto omezení vytváří zjevně nezamýšlený prostor pro zneužití institutu sběru údajů a součinnosti k neodůvodněnému shromažďování údajů o právnických i fyzických osobách. Původní znění by bylo možné vykládat např. tak, že zakládá povinnost poskytovatele služeb elektronických komunikací poskytnout NÚKIB na vyžádání shromažďované provozní a lokalizační údaje, ačkoli takové poskytnutí by ve většině případů bylo neproporcionálním zásahem do ústavně chráněného základního práva na soukromí.	ROZPOR Neakceptováno - nyní § 26 Úřad shromažďuje informace a data primárně za účelem zajištění fungování mechanismu bezpečnosti dodavatelského řetězce. Tato data a informace se musí týkat možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikivosti dodavatele. Úřad také zaručuje, že v žádostech o součinnost bude postupovat v souladu s principem proporcionality, jak je zakotveno v nynějším znění návrhu. Soulad s tímto principem pak bude náležitě kontrolován i dotazovanými orgány a osobami, které nemusí žádosti o součinnost vyhovět, pokud nebude dostatečně odůvodněna. Nelze však vyloučit, jak plyne i ze samotné povahy činnosti správních orgánů, že získané informace budou využity i při jiných činnostech Úřadu nebo jiných správních orgánů veřejné moci. Bylo by v rozporu se základními zásadami činnosti správních orgánů, pokud by Úřad tyto informace nepředal, respektive nevyužil při výkonu ostatních pravomocí. Účel sběru informací a žádostí, jakožto i charakter sbíraných a vyžadovaných informací je tedy, jak plyne z výše uvedeného, omezený.
191. Svaz průmyslu a dopravy ČR	a Z	Zákon o kybernetické bezpečnosti - § 28 odst. 4 „... kritéria rizikivosti dodavatele a způsob jejich vyhodnocení stanoví prováděcí právní předpis.“ Nevydávat Vyhlášku o kritériích rizikivosti dodavatele a její obsah přenést do zákona o kybernetické bezpečnosti (přílohu vyhlášky, která stanovuje kritéria rizikivosti, doplnit jako přílohu samotného zákona).	ROZPOR Neakceptováno - nyní § 29 odst. 4 Byť jsou teze prováděcích právních předpisů součástí předkládaného materiálu, tyto budou předmětem samostatného připomínkového řízení při procesu jejich vydávání. Vaši připomínku bereme na vědomí a určitě doporučujeme veškeré připomínky směřující k prováděcím předpisům uplatnit v rámci

		Původní znění zakládá právní nejistotu pro poskytovatele strategicky významných služeb i bezpečnostně významné dodavatele, protože kritéria hodnocení rizikovosti se mohou v budoucnu významně a snadno změnit změnou vyhlášky. Původní znění v tomto směru pro obsah vyhlášky nestanoví žádné limity. Ponechání této kompetence v rukou moci výkonné, nikoli zákonodárné, by vedlo k nepřiměřené koncentraci pravomocí v rukou jednoho z orgánů veřejné moci. Nelze přitom akceptovat vypořádání připomínky z veřejné konzultace, dle kterého je úprava kritérií formou podzákoného právního předpisu běžnou legislativní praxí. Podstata hodnocení bezpečnosti dodavatelského řetězce a dostupná opatření se závažností dopadu blíží opatřením podle zákona č. 34/2021 Sb. o prověřování zahraničních investic, přičemž zde jsou základní parametry hodnocení rovněž stanoveny zákonem. Současně již nyní navrhovaná kritéria jsou svou povahou obecná, lze proto očekávat minimum jejich změn. K jejich vyčlenění do prováděcího právního předpisu tedy není racionální důvod. S ohledem na závažný ekonomický i provozní dopad na poskytovatele regulované služby tedy nelze akceptovat model, kdy by kritéria byla stanovena vyhláškou.	připomínkového řízení k vyhláškám k navrhovanému zákonu, aby tyto mohly být řádným způsobem vypořádány. Nutno dodat, že zmíněná kritéria posuzování rizikovosti dodavatele v rámci vyhlášky sloužila primárně jako vodítko/metodika k určení hrozby, přičemž vyhláška o kritériích rizikovosti dodavatele byla, také z důvodů uvedených v připomínkách směřujících k jejich smyslu a formě, zrušena. Kritériem tudíž zůstává bezpečnost ČR a její vnitřní či veřejný pořádek.
192. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 28 Prověřování rizik spojených s dodavatelem odst. 3 písm. a) „...u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní vysoká nebo kritická; ...“ Vypustit slova „vysoká nebo“. Poskytovatelé strategicky významných služeb, kteří jsou povinnými osobami podle zákona č. 181/2014 Sb., mají klasifikovaná aktiva a u řady těchto aktiv může být dopad narušení bezpečnosti informací	ROZPOR Neakceptováno – nyní § 29 odst. 3 písm. a) Co se týče ochrany aktiv stanoveného rozsahu, u kterých poskytovatel tyto ohodnotil úrovní vysoká (v rámci připomínky se jedná o část „vysoká nebo“), tak zde, na základě předešlých zkušeností a zkoumání, NÚKIB konstatuje, že tato aktiva jsou kritická pro fungování strategicky významných služeb. Byť by se striktně jazykovým výkladem dalo dovodit, že je možné do kritického rozsahu sítě zahrnout pouze

		ohodnocen úrovni vysoká, aniž by přitom bylo přiměřené u těchto aktiv aplikovat mechanismus prověřování. Přijetí nového zákona přitom nebude odůvodňovat samo o sobě změnu hodnocení dopadu narušení bezpečnosti informací na tato aktiva. Je proto namístě aplikovat tento mechanismus pouze na aktiva s hodnocením dopadu úrovni kritická. Omezení kritické části stanoveného rozsahu pouze na aktiva s hodnocením dopadu úrovni kritická přitom nevytváří riziko nedostatečného zahrnutí klíčových aktiv.	aktiva s dopadem „kritická“, nelze tak učinit. Co se týče ochrany aktiv stanoveného rozsahu, u kterých poskytovatel tyto ohodnotil úrovni vysoká (v rámci připomínky se jedná o část „vysoká nebo“), tak zde, na základě předešlých zkušeností a poznání (vyplývajících zejména z kontrolní činnosti NÚKIB), NÚKIB konstatuje, že tato aktiva jsou velmi důležitá až kritická pro fungování strategicky významných služeb. Aktiva ohodnocena jako vysoká mají podstatné dopady na primární aktiva, a tím pádem na chod celé strategicky významné služby. Ochrana pouze kritických aktiv by nebyla v plném rozsahu schopna pokrýt bezpečnost strategicky významné služby v doménách důvěrnost, integrita i dostupnost.
193. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 29 odst. 1 a 2 Mezi orgány, které mají poskytovat Úřadu informace a součinnost, doplnit Český telekomunikační úřad (ČTÚ). Návrh zákona o kybernetické bezpečnosti a související předpisy významně dopadají na poskytovatele regulovaných služeb v oblasti služeb elektronických komunikací, přesto původní znění výslovně nezmiňuje mezi orgány poskytujícími součinnost ČTÚ (jakkoli jej lze považovat za „orgán“ podle odst. 3). ČTÚ má přitom ve vztahu k oblasti služeb elektronických komunikací největší odbornost, dohlíží nad bezpečností a integritou komunikačních sítí a ukládá opatření k řešení hrozeb (§ 98 zákona č. 127/2005 Sb., o elektronických komunikacích), díky čemuž disponuje řadou informací významných z hlediska technologií, které je pro zajištění bezpečnosti dodavatelského řetězce třeba zohlednit (zejména z hlediska nepominutelných funkcí stanoveného rozsahu).	Neakceptováno - nyní § 30 Dle navrhované úpravy NÚKIB v rámci získávání informací spolupracuje s relevantními orgány státu, přičemž v případě jednotlivých sektorů pak návrh zákona v podobě, jaké je dnes, tuto spolupráci předpokládá s regulátory jednotlivých sektorů, je-li to pro daný případ možné. Toto je zaručeno mimo jiné § 8 odst. 2 zákona č. 500/2004 Sb, správního řádu. Dále je tento postup dán principem dobré správy, kdy NÚKIB pro co nejlepší vyhodnocení situace a možných dopadů počítá s dožádáním informací od relevantních orgánů státu v rámci jednotlivých odvětví. Důvodem, proč jsou v navrhovaném zákoně popsány orgány, které jsou obsaženy v § 30, je ten, že tyto fungují napříč jednotlivými sektory a jejich spolupráce je tak pro správné posouzení rizik, včetně vyhodnocení pro případné omezení či zákaz, žádoucí. Po vypořádání:

			Návrh § 31 byl v rámci vypořádání přepracován a upraven. Připomínkové místo s tímto způsobem vypořádání souhlasí.
194. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 29 odst. 3 Vypustit odst. 3 Původní znění explicitně neomezuje okruh dalších orgánů a osob, které jsou povinny poskytnout Úřadu informace a součinnost. To vytváří potenciál k zatížení povinných osob mechanismu prověřování dodatečnými povinnostmi k poskytování údajů, typicky v reakci na hlášení podle § 32 odst. 1 písm. b), a tak faktické rozšiřování výčtu údajů podle § 4 odst. 4 Vyhlášky o portálu NÚKIB. Okruh osob a orgánů povinných k součinnosti vůči NÚKIB v této oblasti by měl být stanoven taxativně.	ROZPOR Neakceptováno - nyní § 30 odst. 3 Úřad shromažďuje informace a data primárně za účelem zajištění fungování mechanismu bezpečnosti dodavatelského řetězce. Tato data a informace se musí týkat možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele. Běžný rozsah těchto dat a informací od povinných osob, které Úřad potřebuje ke shora uvedené činnosti, je vymezen v § 32 odst. 1 návrhu; dle konkrétního případu však může být nezbytné zjištění také dalších, předem nespecifikovaných údajů. Úřad nicméně zaručuje, že v žádostech o součinnost bude postupovat v souladu s principem proporcionality, jak je zakotveno v nynějším znění návrhu. Soulad s tímto principem pak bude náležitě kontrolován i dotazovanými orgány a osobami, které nemusí žádosti o součinnost vyhovět, pokud nebude dostatečně odůvodněna. Nelze také vyloučit, jak plyne i ze samotné povahy činnosti správních orgánů, že získané informace budou využity i při jiných činnostech Úřadu, nebudou pro ně však primárně sbírány. Bylo by v rozporu se základními zásadami činnosti správních orgánů, pokud by Úřad tyto informace nevyužil při výkonu ostatních pravomocí. Účel sběru informací a žádostí, jakožto i charakter sbíraných a vyžadovaných informací je tedy, jak plyne

			z výše uvedeného, omezený a vypustit předmětný § 30 odst. 3 návrhu při zachování stanoveného účelu nelze.
195. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 29 Prověřování rizik spojených s dodavatelem odst. 3 písm. c) „... dodavatelem bezpečnostně významné dodávky každý, kdo poskytovateli strategicky významné služby poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku.“ Ve spojení s § 32 odst. 1 písm. a) „... zjišťovat s vynaložením přiměřeného úsilí informace o dodavatelích bezpečnostně významných dodávek a...“ Doplnit úroveň poddodavatelského řetězce, která má být předmětem zjišťování povinné osoby mechanismu prověřování dle § 32 odst. 1 písm. a), nebo způsoby pro její stanovení (např. odkaz na prováděcí právní předpis a zmocnění k jeho vydání). Je třeba blíže specifikovat úroveň dodavatelského řetězce, do které jsou poskytovatelé strategicky významných služeb povinni zjišťovat informace dle § 32 odst. 1 písm. a). V souladu s cílem a účelem předmětné úpravy je přiměřené, aby poskytovatel strategicky významné služby zjišťoval informace nejen o primárním dodavateli, kterým bude často pouze distributor, ale také o přímém výrobcí daného produktu nebo poskytovateli služby ve vztahu, ke kterým je stěžejní prověřit rizikovost. Původní znění však lze vykládat i jako povinnost zjišťovat informace i o dodavatelích jednotlivých komponent daného výrobku (polovodičových prvků) nebo dodavatelích dílčích programových prostředků (licencí), pomocí kterých je poskytována služba přímým dodavatelem. Taková povinnost pro poskytovatele strategicky významných služeb by byla nepřiměřená a není opodstatněna bezpečnostními riziky, která jednotlivé komponenty či programové	Neakceptováno NÚKIB je přesvědčen, že současný návrh úpravy umožňuje poskytovateli strategicky významné služby dostatečnou volnost uvážení, zda zjištění a nahlášení určitého poddodavatele je pro něj přiměřené z pohledu vynaloženého úsilí. Je však na poskytovateli, aby si tento krok dokázal obhájit během kontroly ze strany NÚKIB. Nelze však <i>a priori</i> říci, že dodavatel licence nebo jednotlivých komponentů nemá z pohledu kybernetické bezpečnosti význam. Stejně tak není možné pevně stanovit úroveň, do které mají být informace o dodavatelích zjišťovány. Neurčitost a navázání na přiměřené úsilí je kompromisem, který zajistí správné a efektivní fungování mechanismu a zároveň nebude neadekvátně zatěžovat poskytovatele strategicky významné služby. Připomínkové místo s vypořádáním souhlasí.

		vybavení představují pro kybernetickou bezpečnost regulované služby. Tato hloubka prověřování by naopak byla přiměřená v případě služeb elektronických komunikací, kde by poskytovatelé strategicky významných služeb měli zjišťovat informace o dodavatelích použité infrastruktury, jakožto bezpečnostně významných dodavatelích, přičemž by měli promítnout opatření obecné povahy spočívající v zákazu nebo stanovení podmínek využívání plnění bezpečnostně významného dodavatele i na dodavatele infrastruktury pro využívané služby elektronických komunikací. Vypořádání připomínky z veřejné konzultace nevyrovnává s různorodou povahou poddodavatelů popsanou výše (dodavatelé software vs. komponent). Ze skutečnosti, že hloubka prověřování musí být přiměřená, neplyne možnost některé dodavatele, kteří nemají význam z hlediska kybernetické bezpečnosti, zcela ignorovat.	
196. Svaz průmyslu a dopravy ČR	Z	Vyhláška o nepominutelných funkcích stanoveného rozsahu, bod 1.11 a 1.14 přílohy „1.11 Systémy řízení veřejné komunikační sítě a monitorování této sítě, včetně řízení a monitoringu kybernetické bezpečnosti, pokud se tyto systémy týkají řízení nebo monitorování nepominutelných funkcí veřejné komunikační sítě nebo pokud mohou mít významný dopad na přístup k síti nebo na síťový provoz.“ „1.14 Funkce řízení rádiové přístupové sítě 2., 4. a 5. generace a řízení základnových stanic.“ Vypustit body 1.11 a 1.14 Uvedené typy aktiv nepovažujeme za nezbytné pro zajištění fungování jádra sítě elektronických komunikací, a proto by neměly tvořit součást nepominutelných funkcí stanoveného rozsahu.	ROZPOR Neakceptováno Nejprve je třeba uvést, že teze prováděcích právních předpisů jsou sice součástí předkládaného materiálu, ale budou předmětem samostatného připomínkového řízení při procesu jejich vydávání. Vaši připomínku tak bereme na vědomí a doporučujeme ji uplatnit v rámci připomínkového řízení k předmětné vyhlášce, aby mohla být řádným způsobem vypořádána. Již nyní se však můžeme vyjádřit k dotčeným bodům 1.11 a 1.14 vyhlášky. Konkrétně u bodu 1.11 NÚKIB uvádí, že tyto tzv. monitorovací/dohledové funkce jsou jednoznačně kritické. Principiálně se jedná o jediné nástroje, které mají za úkol dohled nad dostupností sítě. To, že jádro sítě funguje i bez těchto nástrojů, lze považovat za samozřejmost. Pokud ale v rámci jádra dojde k poruše či znefunkčnění jádra nebo

			jinému, obdobnému problému, tak tyto monitorovací systémy představují první bod interakce, a tudíž jsou absolutně stěžejní z pohledu tzv. telekomunikačních business modelů. Z hlediska důležitosti bodu 1.14, tj. řízení stanic rádiové přístupové sítě jednotlivých generací, uvádíme, že tyto funkce by měly být považovány za kritické (také dle německého přístupu k určení kritických částí či EU 5G Toolboxu). Řízení základnových stanic je kritické také z toho důvodu, že v případě kompromitace těchto stanic může dojít přímo ke kompromitaci provozu v dané oblasti nebo omezení dostupnosti sítě. Přestože se nejedná o kritické funkce z pohledu jádra, z pohledu koncových zařízení/zákazníků jsou tyto skutečně rozhodující.
197. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 30 Omezení rizik spojených s dodavatelem Za odstavec 3 vložit nový odstavec 4 ve znění „Ukládá-li opatření obecné povahy povinnost poskytovateli služeb elektronických komunikací, má Český telekomunikační úřad v řízení o vydání opatření obecné povahy postavení dotčeného orgánu. Dotčený orgán uplatňuje v řízení stanoviska, která nejsou rozhodnutím ve správním řízení a jejichž obsah je závazný pro vydání opatření obecné povahy podle odst. 1.“ ČTÚ disponuje nejširší expertízou v oblasti trhu služeb elektronických komunikací a dohlíží nad bezpečností a integritou veřejných komunikačních sítí a služeb elektronických komunikací. Závažné zásahy do trhu poskytování služeb elektronických komunikací nelze efektivně provádět bez informací, jimiž disponuje pouze sektorový regulátor, který je ze zákona eviduje a zpracovává.	ROZPOR Neakceptováno - nyní § 31 Nejprve je nutno uvést, že NÚKIB v rámci získávání informací, dle navrhovaného zákona, spolupracuje s relevantními orgány státu, v případě jednotlivých sektorů pak zákon v podobě, v jaké je dnes, tuto spolupráci předpokládá též s regulátory jednotlivých sektorů (např. telekomunikace, doprava, energetika), pokud je to v daném případě možné. Uvedenou spolupráci se sektorovými regulátory mimo jiné zaručuje § 8 odst. 2 zákona č. 500/2004 Sb, správního řádu. Dále je tento postup zaručen principem dobré správy, kdy NÚKIB pro co nejlepší vyhodnocení situace a možných dopadů počítá s dožádáním informací od relevantních orgánů státu v rámci jednotlivých odvětví. Důvodem, proč jsou v navrhovaném zákoně popsány orgány, které jsou

		ČTÚ ze zákona náleží dohled nad trhem se službami elektronických komunikací, který nelze účinně provádět, bude-li do trhu zasahovat jiný správní orgán bez nutnosti vyžádání stanoviska, potenciálně i bez vědomí ČTÚ. Současně musí mít sektorový regulátor k dispozici informace o připravovaných zásadních zásazích do jím regulovaného trhu. Spolupráce s dotčeným orgánem také snižuje zátěž povinných osob z hlediska poskytování obdobné součinnosti jak NÚKIB, tak ČTÚ. Návrh má za cíl vytvořit obdobný mechanismus stanovisek dotčeného orgánu k mechanismu stanovisek dotčených orgánů podle § 54 zákona č. 283/2021 Sb., stavebního zákon (a obdobně podle zákona č. 183/2006 Sb.), přičemž kromě ČTÚ by dotčenými orgány mohli být také ostatní sektorový regulátoři (např. ERÚ, ÚCL apod.). Takový mechanismus zároveň sníží koncentraci pravomocí NÚKIB, který má v původní podobě návrhu možnost významně zasáhnout do téměř všech odvětví národního hospodářství bez ohledu na existenci a stanovisko regulační autority příslušného sektoru. Vypořádání připomínky z veřejné konzultace nepovažujeme za dostatečné. Argumenty vznesené ve vztahu k NÚKIB lze analogicky uvést i u obce či kraje jako pořizovatelů územně plánovací dokumentace, přesto jsou obec i kraj při pořizování územně plánovací dokumentace vázány stanovisky dotčených orgánů a nadřízeného orgánu.	obsaženy v § 30, je ten, že tyto fungují napříč jednotlivými sektory a jejich spolupráce je tak pro správné posouzení rizik, včetně následujícího vyhodnocení pro případné omezení či zákaz, velmi žádoucí. Po vypořádání: Návrh § 31 byl v rámci vypořádání přepracován a upraven. Připomínkové místo s tímto způsobem vypořádání u této připomínky nesouhlasí.
198. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 32 Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce odst. 1 písm. a) a b) „... zjišťovat s vynaložením přiměřeného úsilí informace o dodavatelích bezpečnostně významných dodávek a dokumentovat tyto informace alespoň v rozsahu identifikace všech bezpečnostně významných dodávek a dodavatelů bezpečnostně významných dodávek, kteří je poskytují,“	Akceptováno jinak - nyní § 33 Souhlasíme, že v případě, kdy se dílčí plnění z rámcové smlouvy nijak nezmění, bylo by nadbytečné každé toto plnění hlásit. Úprava této problematiky na úrovni zákona je však s ohledem na její specifickou nevhodná. Z těchto důvodů byla upravena důvodová zpráva k § 33 návrhu zákona následujícím způsobem: „<i>Úřad specifikuje, že vzhledem k účelu ustanovení není v případě rámcových smluv na dodávku určitého</i>

		Upřesnit, že bezpečnostně významnou dodávkou plynoucí z rámcové smlouvy je uzavření rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb jako celku (se specifikací rozsahu rámcové smlouvy), nikoli jednotlivé dílčí plnění (objednávky). V případě, že by každé jednotlivé dílčí plnění (realizovaná objednávka) z rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb, mělo být hlášeno jako samostatná bezpečnostně významná dodávka, byla by na poskytovatele strategicky významné služby kladena neúměrně vysoká administrativní zátěž a stejně tak NÚKIB by byl zatížen řadou nadbytečných hlášení bez přidané informační hodnoty. Účel tohoto ustanovení bude naplněn i ve znění navrhované změny, dle které se plnění plynoucí z rámcové smlouvy budou hlásit jako jedna bezpečnostně významná dodávka s určením možného rozsahu plnění. Vypořádání připomínky z veřejné konzultace nereflektuje že návrh se vztahuje k opakovanému objednávání stejného plnění (zboží) tedy nezměněného bezpečnostního rizika.	<i>výrobku nebo služby žádoucí, aby byla opakovaně hlášena jednotlivá dílčí plnění. Postačí hlášení rámcové smlouvy jako celku. Výjimkou jsou však situace, kdy dojde ke změně v dodavatelském řetězci. Pak je povinností poskytovatele strategicky významné služby, aby tuto změnu Úřadu nahlásil."</i> Připomínkové místo s vypořádáním souhlasí.
199. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 32 Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce odst. 2 „Poskytovatel strategicky významné služby začne plnit povinnost hlásit informace podle odstavce 1 pro každou strategicky významnou službu nejpozději do 1 roku ode dne doručení písemného vyrozumění o jejím zápisu do evidence poskytovateli regulovaných služeb podle § 10 odst. 1.“ Doplnit, že doba 1 roku ode dne doručení písemného vyrozumění o zápisu se vztahuje také na povinnost zjišťovat informace podle § 32 odst. 1 písm. a).	Neakceptováno - nyní § 33 Úprava směřuje k tomu, aby povinná osoba začala zjišťovat informace o svých dodavatelích co nejdříve. Povinnost zjišťování informací pak v prvotních fázích může mít podobu pouhých kroků, které budou vést ke schopnosti povinné osoby požadované informace následně sbírat. Jelikož je povinnost hlášení těchto informací stanovena na jeden rok ode dne doručení písemného vyrozumění o zápisu služby, nebudou tak v tomto přechodném období ukládány žádné sankce. Povinnost zjišťovat informace o svých dodavatelích je navázána na povinnost je hlásit, a až ta může být po uplynutí přechodného období Úřadem sankcionována.

		Přechodné období by se nemělo uplatnit pouze pro povinnost hlásit NÚKIB informace, ale i pro povinnost je zjišťovat. Není přiměřené požadovat, aby poskytovatelé strategicky významných služeb zahájili sběr informací bezprostředně po účinnosti zákona, bez stanovení přechodného období. Vypořádání připomínky z veřejné konzultace nereflektuje skutečnost, že plnění povinnosti zjišťovat informace nelze zahájit okamžitě. K okamžiku zápisu do evidence poskytovatelů regulované služby nebude mít poskytovatel strategicky významné služby nastaveny odpovídající smluvní a compliance mechanismy a v případě kontroly bezprostředně po tomto zápisu bude čelit riziku významných sankcí ze strany NÚKIB. I proto povinnost je tak třeba nastavit odložené plnění, aby bylo možné zavést příslušné smluvní a compliance mechanismy.	Doba jednoho roku pro sběr informací je tedy implicitně v zákoně již stanovena a není ji proto potřeba doplňovat. Připomínkové místo s vypořádáním souhlasí.
200. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 33 Omezení rizik spojených s dodavatelem ve veřejných zakázkách Odstranit z § 32 slova „v postavení zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek“ a slova „na veřejnou zakázku“. I soukromý subjekt, který není zadavatelem podle zákona o zadávání veřejných zakázek, může mít sjednaný dlouhodobý závazek, při jehož sjednávání nemohl vědět, že jeho dodavatel bude shledán rizikovým dodavatelem. Řada takových závazků může být sjednána před účinností navrhovaného zákona. Pro takové případy je třeba stanovit mechanismy umožňující i takovému soukromému subjektu ukončit sjednaný závazek. Vypořádání připomínky z veřejné konzultace nereflektuje skutečnost, že některé kontrakty na bezpečnostně významné dodávky jsou dlouhodobé a mohly být sjednány před přijetím navrhované právní úpravy a tedy ji nemohly předvídat a nemusí v ní být obsažen adekvátní výpovědní důvod.	Akceptováno - nyní § 34 Připomínkované ustanovení předkládaného návrhu zákona bylo upraveno podle požadavků připomínky. Možnost ukončení dlouhodobých závazků tak bude přiznána i soukromým subjektům, které nejsou zadavateli podle zákona o zadávání veřejných zakázek. Připomínkové místo s vypořádáním souhlasí.

201. Svaz průmyslu a dopravy ČR	a	Z	Zákon o kybernetické bezpečnosti - § 40 Opatření k řešení stavu kybernetického nebezpečí odst. 1 g) Vypustit Zákon nedefinuje rozsah ani metodiku provedení skenu zranitelností a penetračního testu. Sken zranitelností a penetrační test technických aktiv provedený na jejich produkční části může zásadně narušit funkčnost technických aktiv až do míry ekvivalentní reálnému kybernetickému útoku, může způsobit nestabilitu, dlouhodobé selhání, případně přímo usnadnit budoucí kybernetický útok. Provedení skenu zranitelností a penetračního testu musí být vždy v odpovědnosti vlastníka nebo provozovatele technických aktiv a musí být prováděno v rámci plánovaných výlukových oken, a to v definovaném rozsahu s odhadnutelným dopadem.	Neakceptováno - nyní § 41 Na tuto povinnost je navázána povinnost součinnosti vyzvaných orgánů a osob právě za tím účelem, aby nebylo zasaženo do funkčnosti technických aktiv a to provedením zpravidla méně invazivního skenu zranitelností nebo penetračním testováním. Ohledně rozsahu a metodiky je proto nezbytné konzultovat s příslušnými odpovědnými pracovníky orgánů a osob, u nichž se znalost informačního systému předpokládá a skrze jejichž součinnost by tam mělo být zamezeno narušení funkčnosti technických aktiv. Primárně není v zájmu řešení dané situace, aby došlo k narušení fungování dalších organizací a je tak v zájmu Úřadu, aby tyto testy proběhly pokud možno bez dalšího narušení kybernetické bezpečnosti. Připomínkové místo s vypořádáním souhlasí.
202. Svaz průmyslu a dopravy ČR	a	Z	Zákon o kybernetické bezpečnosti - § 53 Zpracování osobních údajů odst. 1 Vypustit slovo „úkolů“ a přidat slovo „oprávněným“ z/do věty „Tyto údaje Úřad a provozovatel Národního CERT předávají oprávněným orgánům veřejné moci nebo osobám, je-li to nezbytné pro plnění jejich ~~úkolů~~ – zákonných povinností a nedojde-li tím k porušení povinnosti mlčenlivosti podle tohoto zákona.“ Zajistit soulad s účinnými právními normami, jako je GDPR, která specifikují pravomoci a zmocnění oprávněných orgánů při plnění jejich zákonných povinností.	Akceptováno jinak - nyní § 56 Připomínkované ustanovení (§ 53 odst. 1) bude z návrhu zákona zcela vypuštěno. Připomínkové místo s vypořádáním souhlasí.
203. Svaz průmyslu a dopravy ČR	a	Z	Zákon o kybernetické bezpečnosti - § 53 Zpracování osobních údajů odst. 3 a), 3 b), 3 c) Doplnit soulad s GDPR a dalšími právními předpisy	Neakceptováno - nyní § 56 Odepření práv subjektu údajů je možné pouze po dobu plnění povinností podle tohoto návrhu zákona při řešení kybernetického bezpečnostního incidentu nebo

		V případě, kdy mají být subjektům údajů odepřena jejich práva, je nutné zákonem vymezit konkrétní účely a podmínky zpracování osobních údajů, a to včetně retenčních povinností. Současně je nutno zakotvit zákonný mechanismus kontroly oprávněnosti a zpracování takovýchto osobních údajů.	kybernetické bezpečnostní události, při prevenci kybernetických hrozeb nebo rizik anebo při výkonu kontroly. Po odpadnutí důvodu zpracování osobních údajů při řešení kybernetického bezpečnostního incidentu nebo kybernetické bezpečnostní události, při prevenci hrozeb nebo rizik anebo při výkonu kontroly, postupuje Úřad nebo provozovatel Národního CERT dle přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů. Připomínkové místo s vypořádáním souhlasí.
204. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 28 Prověřování rizik spojených s dodavatelem odst. 3 písm. a) „... aktiva stanoveného rozsahu strategicky významné služby, která zajišťují nepominutelné funkce stanoveného rozsahu stanovené prováděcím právním předpisem,“ odst. 3 písm. c) c) dodavatelem bezpečnostně významné dodávky ten, kdo poskytovateli strategicky významné služby poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku. písm. a) Vypustit „<i>... která zajišťují nepominutelné funkce stanoveného rozsahu stanovené prováděcím právním předpisem</i>“ a nahradit „<i>úrovní kritická; a jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby,</i>“ písm. c) Vypustit „<i>či jako poddodavatel.</i>“ Navrhované ustanovení ponechává pravomoc NÚKIB provádět prověřování rizik spojených s dodavatelem, tak jak předpokládá návrh	ROZPOR Neakceptováno - nyní § 29 Níže se vyjadřujeme k Vaším bodům: Ad písm. a) Nepominutelné funkce představují množinu kritických funkcí, která nutně nepředpokládá vstup do analýzy rizik. Na základě analýzy rizik lze zkontrolovat zařazení aktiv, tedy zdali tato aktiva odpovídají také seznamu nepominutelných funkcí. Nepominutelné funkce stanoví, společně s aktivy určenými samotnou povinnou osobou, množinu aktiv, na kterou dopadají povinnosti mechanismu prověřování bezpečnosti dodavatelského řetězce. Nepominutelné funkce nicméně do analýzy rizik, resp. řízení aktiv dle vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, nezasahují, ale pouze ji doplňují. Tyto funkce jsou důležité z důvodu značné komplexity veřejných komunikací a jejich tzv. kaskádovitého efektu, tedy přímého dopadu na další strategicky významné služby, které jsou na telekomunikacích

	ZKB, odlišně však vymezuje některé pojmy spojené s touto pravomocí. Vzhledem k odlišné koncepci pojmu kritické části stanoveného rozsahu (viz níže), je obsolentní zakotvení vydání vyhlášky o nepominutelných funkcích stanoveného rozsahu, jak předpokládá návrh ZKB, proto byla ze znění tohoto návrhu vypuštěna. Pravomoc NÚKIB má být realizována, v souladu s návrhem ZKB, prostřednictvím shromažďování a vyhodnocování informací, jež mohou přispět k vyvození závěrů o existenci hrozby pro bezpečnost ČR, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovitosti dodavatele stanovených prováděcím právním předpisem, a které jsou spojeny s plněním konkrétního dodavatele. Kritéria rizikovitosti dodavatele stanoví prováděcí právní předpis – vyhláška, k jejímuž vydání je zmocněn NÚKIB v § 55 návrhu ZKB. Jak je uvedeno v důvodové zprávě k návrhu ZKB, cílem mechanismu prověřování BDŘ je umožnit státu identifikovat a vyhodnocovat hrozby spojené jak s orgány nebo osobami, které již jsou dodavateli do infrastruktury poskytovatelů strategicky významné služby, tak s orgány nebo osobami, u nichž se lze domnívat, že by svá plnění do této infrastruktury dodávat mohly, a to s cílem odhalit hrozbu ještě dříve, než bude u strategicky významné služby moci způsobit narušení bezpečnosti informací. S ohledem na velké množství orgánů a osob, které mohou být předmětem prověřování, je stanovena možnost NÚKIB prioritizovat činnosti spojené s prověřováním stávajících a potenciálních dodavatelů, tak jak to předpokládá i návrh ZKB, a to s ohledem na možná rizika a dostupné kapacity NÚKIB. Odst. 3 předmětného ustanovení vymezuje pojmy, které navrhovaná právní úprava dále užívá v souvislosti s mechanismem. Pojem „bezpečnostně významná dodávka“, který vymezuje plnění, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů, a „dodavatel bezpečnostně významné dodávky“, který vymezuje okruh orgánů a osob, na jejichž plnění se mohou vztahovat omezení využití v důsledku prověření rizik s nimi spojených, je dle tohoto návrhu	závislé. Z toho důvodu NÚKIB ve vyhlášce určuje funkce, které musí být považovány za kritické z hlediska jejich dopadu na funkčnost sítí, a to neohledně na jejich umístění v rámci architektury sítí. Ad písm. c) Zákon definuje pouze dodavatele bezpečnostně významné dodávky, jež je důležitý pro určení rozsahu mechanismu bezpečnosti dodavatelského řetězce. Dodavatel na obecné rovině, včetně poddodavatele, je již definován jinými zákony, jako je například zákon č. 134/2016 Sb., o zadávání veřejných zakázek, přičemž se v obecném pojetí NÚKIB nechce odchýlit od již fungujících definic. Co se týče pojmu poddodavatel, tak poddodavatelé jsou rovněž kritičtí z hlediska posuzování jejich rizikovitosti, jelikož mají v rámci strategického posuzování kybernetické bezpečnosti obdobné až stejné možnosti působit na dodavatelský řetězec, jako dodavatel. Co se pak týče kritičnosti jednotlivých funkcí upravených vyhláškou o nepominutelných funkcích, tak zde platí, že tyto skutečně představují to, co je v rámci veřejných komunikačních sítí kritické, neohledně na jejich umístění v rámci síťové architektury. To znamená, že některé funkce rádiové přístupové sítě jsou rovněž kritické pro to, aby mohl dojít k propojení koncových zařízení s nejkritičtějším jádrem sítě. Bez uvedených funkcí by takové propojení nebylo možné ani v případě, kdy by jádro sítě bylo zcela funkční.

	shodný se zněním uvedeným v návrhu ZKB, proto se mu text zde nebude věnovat. Změny však v tomto předkládaném návrhu doznal pojem „kritická část stanoveného rozsahu“, který vymezuje aktiva poskytovatele strategicky významné služby, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů. NÚKIB opakovaně deklaroval, že mechanismus se má vztahovat pouze na tu nejkritičtější část strategické infrastruktury. V návrhu ZKB je však vymezen rozsah mechanismu formou vyhlášky o nepominutelných funkcích, která je výrazně širší než bylo deklarováno, a např. pro oblast telekomunikací obsahuje jak ty nejkritičtější části sítě (jako je jádro sítě – „core“), tak i méně kritické části sítě (jako je např. rádiová přístupová síť) nebo aktiva, které nemají přímý vliv na nedostupnost regulovaných služeb (např. fakturační systém). V návrhu ZKB i důvodové zprávě k němu zcela chybí odůvodnění, proč jsou kritické části stanoveného rozsahu aktiv definovány tak široce. Ve zde předkládaném návrhu je stanovena nová úprava kritické části stanoveného rozsahu aktiv tak, aby se jednalo pouze o aktiva ohodnocená povinnými subjekty na úrovni kritická, jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby. Předkládaný návrh vychází z předpokladu, že kritická část stanoveného rozsahu se skládá z podmnožiny aktiv strategicky významných služeb, u kterých si poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu upravujícího bezpečnostní opatření poskytovatele regulované služby v režimu vyšších povinností sám v rámci plnění povinností podle § 13 návrhu ZKB ohodnotil dopad narušení bezpečnosti informací úrovní kritická. Kritické části strategické infrastruktury jsou transparentně rozděleny dle úrovně hrozby a dopadů její případné realizace. Nejvýznamnější hrozbou je výpadek regulované služby – rozsah mechanismu tak byl v návrhu omezen výlučně na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické	

		úrovni. Pro příklad – pro oblast telekomunikací se jedná zejména o jádro sítě, případně části přenosové sítě. Úprava je formulována obecněji, aby se vztahovala na všechny oblasti, nejen telekomunikace. Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je přiměřené, aby byla dána možnost státu okamžitým zásahem omezit či zakázat vybraného dodavatele, u kterého identifikuje významnou hrozbu. Pro zbylé části aktiv strategicky významné služby, které nemohou ze své podstaty způsobit nedostupnost služby na kritické úrovni, je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika, která v rámci opatření obecné povahy identifikoval NÚKIB. Ten by přitom jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Úpravou písm. c) se tento mechanismus omezí pouze na přímé dodavatele povinných osob, a nikoliv i dalších nepřímých poddodavatelů. Tímto zúžením počtu subjektů, na něž bude dopadat předmětná úprava, dojde k omezení této zásadní administrativní zátěže. Zároveň se předejde situaci, kdy např. povinnosti z předmětné úpravy budou muset plnit také dodavatelé poddodavatelů apod.	
205. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 30 Omezení rizik spojených s dodavatelem Navrhujeme nové znění § 30 ve znění: 1. Zjistí-li Úřad na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, předloží věc k projednání Vládě České republiky (dále jen “Vláda”). 2. Vláda přijme do 45 dnů ode dne, kdy jí byla věc předložena k projednání, usnesení o tom, zda plnění dodavatele může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Při posuzování věci Vláda zohlední možný dopad plnění dodavatele na principy	ROZPOR Připomínka velmi obsáhle reaguje na celou řadu principů mechanismu prověřování BDŘ, které jsou v návrhu obsažené a současně s tím předkladatel připomínky navrhuje mnoho nových bodů. Ve vypořádání připomínky se s nimi vypořádáme tematicky. Zapojení vlády ČR do procesu prověřování. Neakceptováno. Do procesu je zapojena Bezpečnostní rada státu, která je stálým pracovním orgánem vlády pro koordinaci problematiky

		demokratického právního státu, ochranu života a zdraví obyvatel, obranu státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku. 3. V návaznosti na usnesení Vlády, že plnění dodavatele představuje významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, vydá Úřad opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu. 4. Usnesení Vlády je pro Úřad závazné a vydání opatření obecné povahy omezující či zakazující plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu je vydáním usnesení Vlády podmíněno. 5. Zakáže-li nebo omezí-li Úřad opatřením obecné povahy dle odstavce 3 plnění dodavatele, určí zároveň v opatření obecné povahy přiměřenou lhůtu zákazu nebo zohlednění podmínek plnění dodavatele. Lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy stanoví Úřad s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby. Úřad vždy musí lhůtu předem konzultovat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele. 6. Před vydáním opatření obecné povahy je Úřad povinen projednat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele, zda návrh opatření obecné povahy a jeho možné dopady neohrozí plnění povinností stanovených a vyplývajících ze zvláštních právních předpisů. Úřad je povinen při vydání opatření obecné povahy stanovisko ústředního orgánu státní správy zohlednit.	bezpečnosti České republiky a přípravu návrhů opatření k jejímu zajišťování, ve které jsou členové vlády zastoupeni. V případě potřeby může samozřejmě problém eskalovat až na vládní úrovni. S tím také plyne procesní stránky věci, kdy Bezpečnostní rada státu může návrh opatření obecné povahy v případě, že je jí předložen, neprojednat, přerušit jeho projednávání, vrátit jej k přepracování, případně s ním vyjádřit nesouhlas. Jakékoliv rozhodnutí je pro Úřad samozřejmě závazné. Konzultace s orgány státní správy Neakceptováno v navržené podobě. Úřad při vydávání opatření obecné povahy spolupracuje se všemi orgány státní správy, které jsou relevantní pro získání všech informací potřebných k tomu, aby byla dosažena maximální kvalita výsledného opatření obecné povahy, která se skládá z mnoha faktorů, například zvýšení bezpečnosti, dopady na poskytovatele strategicky významných služeb, dopady na hospodářskou soutěž, dopady na mezinárodní dohody, lhůta pro zohlednění opatření, dopady na další zákonné povinnosti poskytovatelů strategicky významných služeb a mnoho dalších. Toto v návrhu zákona ošetřeno v § 30 a nadto to vyplývá z obecných principů dobré správy. Analýza rizik Neakceptováno. Byť lze navržený postup poskytovatelům strategicky významných služeb v mnoha případech doporučit, připomínka jako taková nebude akceptována. Úřad cílí mechanismem na kritickou část stanoveného rozsahu a ukládání povinností nad tento rámec není žádoucí.

	7. Jestliže zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle odstavce 3 může ohrozit poskytování strategicky významné služby anebo představuje bezprostřední hrozbu kybernetického bezpečnostního incidentu, který podstatným způsobem ohrožuje poskytování strategicky významné služby, je poskytovatel strategicky významné služby povinen plnit opatření obecné povahy až po pominutí takové hrozby. 8. Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu opatření obecné povahy podávali připomínky. Lhůta pro podání připomínek činí 30 dnů, nestanoví-li Úřad jinak. Ustanovení § 172 odst. 1 a 5, § 173 odst. 1 věty první, část věty za středníkem, a § 173 odst. 1 věty druhé správního řádu se pro postup podle tohoto ustanovení nepoužijí. 9. V případě vydání opatření obecné povahy odstavce 3 musí poskytovatel strategicky významné služby provést analýzu rizik spojených s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3 pro aktiva strategicky významné služby, která nezařadil do kritické části stanoveného rozsahu podle § 28 odst. 3 písm. a). 10. Na základě analýzy rizik vypracuje poskytovatel strategicky významné služby plán zvládání rizik dle odstavce 9, v němž uvede bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3. Plán zvládání rizik je poskytovatel strategicky významné služby povinen aktualizovat alespoň jednou za kalendářní rok. 11. Úřad přezkoumá alespoň jednou za 3 roky trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 3. Zjistí-li Úřad, že tyto skutečnosti pominuly, opatření obecné povahy zruší. A nový § 31 ve znění:	Náhrada účelně vynaložených nákladů Neakceptováno. Navrhovaná právní úprava je ve své současné podobě ústavně konformní, kvůli čemuž není důvod přidávat ustanovení o náhradě škod. Vzhledem k charakteru navrhované právní úpravy, převážně v oblasti mechanismu bezpečnosti dodavatelského řetězce, která se snaží vyjít vstříc povinným osobám například v otázkách životních cyklů technologií nebo zamezení možné závislosti na jedné technologii skrz systém výjimek, není nutné, aby možnost kompenzací byla upravena přímo v zákoně; přirozeně tím však nejsou dotčena např. práva na náhradu škody či kompenzace podle jiných právních předpisů. Zároveň platí, že pro vydání omezení či zákazu formou opatření obecné povahy budou posuzovány veškeré okolnosti a reálné dopady na trh a podnikatelské prostředí. Z toho důvodu by NÚKIB posuzoval jak životnost jednotlivých technologií, tak například možnosti jednotlivých povinných subjektů či postavení dodavatele na českém trhu apod. Cílení na nedostupnost. Neakceptováno. Rozsah mechanismu je stanoven na aktiva ohodnocena jako vysoká a kritická. Ta mají podstatné dopady na primární aktiva, a tím pádem na chod celé strategicky významné služby. Ochrana pouze kritických aktiv by nebyla v plném rozsahu schopna pokrýt bezpečnost strategicky významné služby v doménách důvěrnost, integrita i dostupnost. Není zcela jasné, proč by měla být doména dostupnosti na úrovni zákona vyzdvížena nad doménu důvěrnosti a integrity, když z pohledu strategického

	§31 Náhrada účelně vynaložených nákladů 1. V případě, že lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle §30 odstavce 3 je kratší, než životní cyklus bezpečnostně významné dodávky, nejdéle však 7 let, má každý poskytovatel strategicky významné služby vůči státu právo na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností podle odstavce 3 a to včetně nákladů na náhradu dlouhodobého majetku, který poskytovatel strategicky významné služby v důsledku opatření obecné povahy podle odstavce 3 nemůže dále využívat. Výši účelně vynaložených nákladů podle věty první určí Úřad na základě znaleckého posudku, pro jehož vyhotovení poskytne poskytovatel strategicky významné služby součinnost. 2. Životní cyklus bezpečnostně relevantní dodávky bude znalcem určen na základě účetních odpisů zařízení. 3. Zrušením opatření obecné povahy podle odstavce 11 nezaniká právo na náhradu nákladů podle tohoto odstavce. Ve věci náhrady nákladů podle tohoto odstavce jménem státu jedná Úřad. Jak je uvedeno ve zprávě o hodnocení dopadů, cílem prověřování rizik spojených s dodavatelem je minimalizace ekonomických dopadů a omezení pouze na kritickou část síťové infrastruktury. Pokud je cílem vymezit pouze kritickou část strategické infrastruktury, mělo by se jednat o aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je tedy vhodné, aby byla možnost státu okamžitým zásahem zakázat vybraného dodavatele, u kterého identifikuje významné hrozby. Pro zbylé části aktiv strategicky významné služby je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika,	významu mají všechny tři domény svoji nezastupitelnou roli pro bezpečnost státu.

		kteřá v rámci opatření obecné povahy identifikoval regulátor. Regulátor by jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by nově byla upravena zvlášt' v bezpečnostní dokumentaci, kterou by poskytovatel měl povinnost ročně aktualizovat. Nově je navrženo zapojení Vlády ČR do procesu vydávání OOP. Je nezbytné, aby v případě vyhodnocování hrozeb měla Vláda možnost posoudit dopady úkonů Úřadu na principy demokratického právního státu, ochranu života a zdraví obyvatel, obrany státu, zahraničně-politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Lhůta plnění povinností poskytovatele z OOP navrhuje stanovovat na základě délky životního cyklu aktiv bezpečnostně významné dodávky, které jsou vyjádřeny účetními odpisy jednotlivých aktiv. V případě, že je taková lhůta zkrácena, znalec stanoví výši náhrady.	
206. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - Aktuální § 31 Výjimky z omezení rizik spojených s dodavatelem, Nový odst.5 Doplnit nový odstavec „(5) Informace týkající se výjimky je v souladu s právními předpisy¹⁾ označována jako utajovaná informace.“ ¹⁾ Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Udělované výjimky jsou citlivou informací, která může poskytovatele regulované služby významně ohrozit. Domníváme se, že je vhodné klasifikovat informace o procesu udělení výjimky i obsah samotné výjimky, zahrnující subjekty, jichž se výjimka týká jako tajné.	ROZPOR Neakceptováno - nyní § 32 Požadavek na doplnění předmětného ustanovení nemůže být akceptován. Problematika utajení informací je již řešena v § 67 návrhu zákona - informace o výjimkách se uchovávají jako neveřejné mimo spis. Pokud by výjimka obsahovala informace klasifikované jako utajované, pak bude takto nakládáno i s celým rozhodnutím.
207. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 34 Zajištění dostupnosti strategicky významné služby, Využívání cloudových a dalších inovativních služeb	Akceptováno jinak - nyní § 35 Připomínkové ustanovení § 35 bylo v odst. 1 upraveno tak, že „Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky

	Navrhujeme: - úpravu odst. 1, 2 a 4, jednak úpravu směřující k vypuštění referencí na případná aktiva směřující k vyjasnění, že dostupnost služby musí být zajištěna v omezeném a pouze nezbytném rozsahu. Pojem „nezbytný“ rozsah, čas a kvalita považujeme za vhodnější, než pojem „stanovený“. Zároveň navrhujeme odkázat na „rozsah“, protože pro některé agendy orgánů veřejné správy nebo jejich části nemusí být nezbytné zajistit dostupnost vůbec. Odkaz na kvalitu a čas implikuje, že je nutné zajistit dostupnost všech agend, bez ohledu na jejich strategický význam, byť případně v omezené kvalitě. - vyjasnění vztahu mezi informačními systémy veřejné správy a požadavky na dostupnost služby, kde zároveň navrhujeme omezení aplikovatelnosti požadavku dostupnosti na informační systémy veřejné správy v bezpečnostní úrovni 4 (kritická). Alternativně by rovněž bylo možné zvažovat úplné vyloučení aplikaci požadavku dostupnosti z území České republiky na veřejnou správu, protože informační systémy veřejné správy v bezpečnostní úrovni 4 mohou být poskytovány výhradně ve státním cloudu umístěném na území České republiky a požadavek zajištění dostupnosti z území České republiky je pro ně tudíž zjevně nadbytečný. Požadavek dostupnosti z území České republiky by se pak uplatnil pouze na ostatní strategicky významné služby v sektoru energetiky, dopravy a digitální infrastruktury. <u>Navrhovaná úprava:</u> § 34 (1) Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby ~~v rozsahu kritické části stanoveného rozsahu ve stanoveném~~ nezbytném ~~časem a kvalitě~~ a rozsahu z území České republiky.	významné služby v nezbytném rozsahu, ~~v rozsahu kritické části stanoveného rozsahu~~ <i>ve stanoveném čase a kvalitě z území České republiky</i>". Tento nezbytný rozsah pak bude stanoven vyhláškou Úřadu. V případě veřejné správy budou stanovena kritéria dopadu kybernetického bezpečnostního incidentu v podobě narušení dostupnosti služby a nezbytným rozsahem pak budou jen ty služby veřejné správy, které budou naplňovat tato kritéria dopadu. Přičemž ta budou zhruba odpovídat kritériím dopadu na úrovni kritická podle teze vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy. Po vypořádání: Nad rámec výše uvedeného byl současně upraven také § 35 odst. 4 návrhu zákona a byly upraveny též Teze vyhlášek, konkrétně teze vyhlášky o o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, kde byl doplněn nový § 29 a byla upravena Příloha č. 9. Připomínkové místo s vypořádáním souhlasí.

		(2) Poskytovatel strategicky významné služby je povinen testovat schopnost zajištění poskytování strategicky významné služby ~~z rozsahu kritické části stanoveného rozsahu~~ z území České republiky nejméně jednou za dva roky. (3) Poskytovatel strategicky významné služby začne plnit povinnosti uvedené v odst. 1 a 2 pro každou strategicky významnou službu nejpozději do jednoho roku ode dne doručení vyrozumění o zápisu strategicky významné služby do evidence poskytovatelů regulovaných služeb nebo od doručení rozhodnutí o určení strategicky významné služby podle § 27 odst. 2. (4) ~~Stanovený~~ Nezbytný čas, a kvalitu a rozsah služby stanoví poskytovatel regulované služby v závislosti na cílech řízení kontinuity činností podle prováděcího právní předpisu. (5) Pro potřeby tohoto ustanovení je kritická část stanoveného rozsahu vymezena v § 28 odst. 3 písm. a). <u>Pokud je pro strategicky významnou službu orgánu veřejné správy využíván informační systém veřejné správy^[1], pro který je využíván cloud computing, musí být dostupnost takového informačního systému státní správy na území České republiky pro účely zajištění dostupnosti strategicky významné služby dle odst. 1 zajištěna pouze pro informační systémy veřejné správy zařazené do nejvyšší bezpečnostní úrovně.</u> Ustanovení § 34 návrhu zákona stanoví povinnosti na zajištění dostupnosti strategicky významných služeb z území České republiky. Pro veřejnou správu je strategicky významná služba definovaná jako „výkon svěřených pravomocí“ ze strany vymezených orgánů státní správy a samosprávy. Vymezený okruh orgánů je velmi široký a zahrnuje, mimo jiné, všechny ústřední orgány státní správy, správní úřady s celostátní působností, kraje, větší obce s rozšířenou působností, vysoké školy, orgány soudní moci a policejní útvary a dalších orgány (dále označovány také jako „orgány veřejné moci“). Dostupnost na území České republiky musí být podle navrhované právní úpravy zajištěna pro všechna aktiva, u kterých by narušení	

^[1] Ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů.

		bezpečnosti informací mělo kritický a vysoký dopad na výkon kterékoli agendy svěřené těmto orgánům¹. Tato povinnost by se tak v praxi vztahovala na převážnou většinu informačních systémů v české státní správě a samosprávě. Ačkoliv hlavním cílem nového zákona o kybernetické bezpečnosti má být implementace směrnice NIS 2, požadavek na zajištění dostupnosti služeb z území České republiky nemá ve směrnici žádnou oporu a jde nad rámec její implementace do českého právního řádu. Lze i dovozovat, že tento požadavek může být v rozporu s přeshraniční spoluprací v rámci Evropské unie, kdy elektronizace některých agend veřejné správy probíhá ve vzájemné koordinaci jednotlivých zemí. Zdá se, že se jedná o požadavek, které nebyl v navrhované podobě zatím implementován v žádném jiném členském státě EU. Z praktického hlediska to znamená, že orgány veřejné moci by musely mít zajištěnou dostupnost veškerých informačních systémů používaných pro výkon svých agend z území České republiky. Pro tyto informační systémy by tak musela existovat záložní varianta, která by byla za všech okolností dostupná výhradně z území České republiky (dle výkladu NÚKIB se musí jednat o variantu, která umožní výkon svěřených pravomocí výhradně s využitím aktiv umístěných na území České republiky a nelze ji zajistit např. dvěma zahraničními poskytovateli či privátním připojením). Tyto požadavky mají zásadní dopad na možnost využívání cloudových služeb v české veřejné správě. Orgány veřejné moci by při využití globálních cloudových služeb musely vytvářet paralelní infrastrukturu na území České republiky (tj. zajistit veškerá aktiva paralelně i na území České republiky, tak aby výkon jejich agend byl možný jen s využitím těchto aktiv). To by vedlo k extrémnímu	

¹ Definice dotčených aktiv je v navrhovaném textu zákona o kybernetické bezpečnosti v § 28 odst. 3 písm. a) částečně nejasná, nicméně NUKIB předběžně potvrdil výše popsany výklad. Definice dotčených aktiv dle navrhované právní úpravy je následující (s tím, že „strategicky významnou službou“ je ve státní správě „výkon svěřených pravomocí“: „kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní vysoká nebo kritická; kritickou částí stanoveného rozsahu jsou vždy alespoň aktiva stanoveného rozsahu strategicky významné služby, která zajišťují nepominutelné funkce stanoveného rozsahu stanovené prováděcím právním předpisem“;

		navýšení nákladů na informační systémy. Tato paralelní infrastruktura by musela být trvale udržována, aktualizována, testována a zabezpečena. Pro některé komplexní SaaS a PaaS služby nemusí být zajištění řešení dostupného výhradně z území České republiky vůbec reálné a tyto služby by tak v české veřejné správě nemohly být vůbec využívány. Tento požadavek by velmi pravděpodobně znemožnil využívání zejména vysoce inovativních služeb s prvky umělé inteligence, které není reálné zajistit výhradně z území České republiky, a to ani s vynaložením vysokých nákladů. Požadavek na zajištění dostupnosti služeb (z lokálního území) považujeme za opodstatnitelný pro nejkritičtější infrastrukturu státu. Pro veřejnou správu byla tato nejkritičtější informační infrastruktura státu již vymezena prostřednictvím bezpečnostních úrovní (bezpečnostní úroveň 4 – kritická) ve smyslu vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (která má být nově vydaná ve stejném znění na základě nově předvídaného zmocnění v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy). Pro tyto systémy je již v souladu s § 6m odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy, možné využívat cloudové služby pouze, pokud jsou poskytovány státním poskytovatelem cloud computingu (tj. je zajištěna dostupnost i poskytování z území České republiky). Rozšiřování těchto povinností na jakékoliv další systémy veřejné správy tak popírá smysl této úpravy a je nepřiměřené. Dopady takového rozšíření by zahrnovaly několikanásobné navýšení nákladů na informační systémy veřejné správy a výrazné zpomalení rozvoje služeb eGovernmentu a digitalizace státní správy.	
208. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 34 Zajištění dostupnosti strategicky významné služby, Služby elektronických komunikací Mezi aktuální odst. 1 a 2 přidat nový odst. 2. Následující odstavce přechíslovat	Akceptováno jinak Připomínkované ustanovení § 35 bylo v odst. 1 upraveno tak, že „Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v nezbytném rozsahu, ~~v rozsahu kritické části stanoveného rozsahu~~ ve stanoveném čase

	„(2) Poskytovatel strategicky významné služby v odvětví 16.1 Poskytování veřejně dostupných služeb elektronických komunikací a 16.2. Zajišťování veřejně dostupné komunikační sítě elektronických komunikací podle přílohy Vyhlášky o regulovaných službách je povinen zajistit dostupnost strategicky významné služby uvedené v odst. 2 písm. a) až c), v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky. a) poskytování veřejně dostupné mobilní služby elektronických komunikací b) zajišťování veřejné mobilní komunikační sítě elektronických komunikací c) Poskytování veřejně dostupné služby elektronických komunikací v pevném místě“ v nově číslovaném odst. 3 doplnit za slova „zajištění poskytování strategicky významné služby“ slova „podle odst. 1 a 2“. v nově číslovaném odst. 4 doplnit za slova „v odst. 1 a 2“ slova „a 3“. NÚKIB na základě připomínek veřejnosti upustil od požadavků na lokalizaci dat na území České republiky nebo spřátelených států. Zároveň však navrhl nahradit lokalizaci povinností zajistit dostupnost strategicky významných služeb z České republiky, pokud jsou k jejich poskytování využívána zahraniční aktiva. Povinnost má zajistit dostupnost nejkritičtějších služeb pro občany České republiky v případě mimořádných událostí (přírodní katastrofy, pandemie, války atp.), které by mohly omezit možnosti využití zahraničních aktiv, ať už z důvodu faktické vzdálenosti, nebo nemožnosti uplatňovat státní moc na území jiných států. NÚKIB však prostřednictvím strategicky významných služeb spojil mechanismus zajišťování minimální úrovně dostupnosti s mechanismem prověřování bezpečnosti dodavatelského řetězce	a kvalitě z území České republiky.“. Tento nezbytný rozsah bude stanoven vyhláškou o nezbytném rozsahu dostupnosti strategicky významných služeb. V této vyhlášce bude blíže rozvedeno, co se v telekomunikačním sektoru rozumí nezbytným rozsahem při zajištění dostupnosti těchto služeb z území ČR. Po vypořádání: Nad rámec výše uvedeného byl současně upraven také § 35 odst. 4 návrhu zákona a byly upraveny též Teze vyhlášek, konkrétně teze vyhlášky o o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, kde byl doplněn nový § 29 a byla upravena Příloha č. 9. Připomínkové místo s vypořádáním souhlasí.

	(dále jen „BDŘ“), přičemž se jedná o odlišné instituty jak z hlediska cíle právní úpravy, tak z hlediska způsobu jeho dosahování. Účelem stanovení minimální úrovně dostupnosti by mělo být zabezpečení dostupnosti nejkritičtějších služeb na „minimální“ úrovni potřebné k fungování společnosti a státu. Navrhovaná právní úprava se však nesoustředí na stanovení této minimální úrovně, které částečně ponechává na povinných osobách, nýbrž se věnuje konkrétním funkcím technických aktiv stanovených ve vyhlášce o nepominutelných funkcích stanoveného rozsahu. Ponechává tedy v nejistotě ohledně zabezpečení minimální úrovně dostupnosti jak poskytovatele, tak uživatele regulovaných služeb. Z výše uvedených důvodů se navrhuje oddělení mechanismu BDŘ od stanovování minimální úrovně dostupnosti. Minimální úroveň dostupnosti jednotlivých kritických služeb by měla být určena zákonem, přičemž způsob zajištění její dostupnosti by měl být ponechán na poskytovatelích. Zároveň se navrhuje konkrétní výčet služeb pro sektor telekomunikací, která respektuje přiměřenou úroveň služeb elektronických komunikací v souladu se zákonem č. 127/2005 Sb., o elektronických komunikacích (dále jen „ZEK“). Poskytovatelé a zajišťovatelé veřejně dostupných služeb elektronických komunikací by měli mít povinnost zajistit dostupnost hlasové komunikace v mobilní síti a připojení k internetu v mobilní síti v takovém rozsahu tak, aby byla při mimořádné situaci umožněna základní komunikace mezi občany a orgány veřejné moci. Minimální úroveň by tak měla zabezpečit komunikaci během mimořádné situace, aniž by kladla nadměrné technické nároky na poskytovatele, protože se nepočítá s nutností zajišťovat služby, které vyžadují vysokou rychlost internetového připojení, jako např. streamování videí nebo videohovory. Pokud by měla být zachována povinnost zabezpečit dostupnost regulované služby v celém rozsahu, k čemuž vede stávající podoba	

		návrhu, museli by poskytovatelé služeb elektronických komunikací budovat infrastrukturu výlučně na území České republiky, neboť by nedávalo ekonomický smysl budovat jakoukoli infrastrukturu v zahraničí, pokud by zároveň musela existovat její plnohodnotná „záložní kopie“ v České republice. Taková povinnost by tudíž byla nepřipustným omezením volného trhu v rámci EU.	
209. Svaz průmyslu a dopravy ČR	Z	Důvodová zpráva k Zákonu o kybernetické bezpečnosti - § 34 Zajištění dostupnosti strategicky významné služby Odst. 1 vypustit V odst. 2 doplnit za slova „cíle na rizika spojená s dostupností“ doplnit slova „poskytované služby.“ V odst. 2 doplnit za slova „Nicméně je limitován nutností zajistit tuto dostupnost“ slova „řídícím systémem“ Znění prvního odstavce navazuje na předchozí návrh paragrafu týkajícího se lokalizace a zpracování dat, nicméně nový návrh ve znění podle § 34 je již výhradně zaměřen na zajištění dostupnosti služby z území ČR, proto je neodůvodněné se nadále zabývat tématem dostupnosti a zpracování dat. Zároveň je nutné zdůraznit, že dostupnost služby a její obnova znamená realizaci takového opatření, aby v případě obnovy bylo možné takovou obnovu zajist z území České republiky a nejedná se o reálné poskytování služby z území České republiky. Předpokládáme vytvoření metodického pokynu ze strany NÚKIB, který dále upřesní plnění tohoto ustanovení.	Akceptováno jinak – nyní § 35 Znění důvodové zprávy k předmětnému ustanovení bylo upraveno ve smyslu připomínky. Odstavec 1 nebyl zcela vymazán, byl pouze upraven s ohledem na změny provedené v legislativním textu. Sousední „řídícím systémem“ nebylo na navrhované místo doplněno, z připomínky není patrný smysl či důvod takové změny. Možnost vydání podpůrného či metodického materiálu není třeba do důvodové zprávy explicitně zmiňovat. Připomínkové místo s vypořádáním souhlasí.
210. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 2 Vymezení pojmů odst. 1 písm. a) Navrhujeme doplnit za slovo „zpracování“ slova „a likvidaci“	Akceptováno jinak, neakceptováno, vysvětleno. -K písm. a) tohoto ustanovení: akceptováno jinak - bude doplněno „včetně likvidace“. -K písm. b) neakceptováno - s ohledem na došlé připomínky došlo k návratu k původní definici jakou používáme v aktuální právní úpravě „<i>primárním</i>“

		odst. 1 písm. b) Navrhujeme za slovo „provozních“ doplnit slova „a lokalizačních“. Dále požadujeme v důvodové zprávě vymezit, o jaké procesy se jedná. odst. 1 písm. h) Navrhujeme upřesnit definici významného dodavatele. odst. 1 písm. a) Likvidace informací a dat je jednou z klíčových oblastí správy informačních aktiv. odst. 1 písm. b) Vedle provozních údajů jsou lokalizační údaje důležitým atributem dat a informací. Navíc je zde vazba na zákon o elektronických komunikacích. Dále jasné vymezení pomůže aplikační praxi. Z textu návrhu není jasné, o jaké procesy se jedná, např. procesy vedoucí k zajištění DDI regulované služby. odst. 1 písm. h) Pokud definice upřesňuje významného dodavatele, jako toho, kdo je „významný“, dochází k jistému pojmovému zacyklení, z něhož není pro aplikační praxi návodné, o jaké dodavatele se má jednat.	<i>aktivem informace a služby</i>" došlo také k upřesnění výkladu této definice v důvodové zprávě. -K písm. h) vysvětleno - Chápeme, že definice je velmi obecná, což znamená, že je to je na povinné osobě zda vyhodnotí, že se jedná o významného dodavatele z pohledku kybernetické bezpečnosti či nikoliv. Vztahuje se na něj speciální úprava obsažená v § 26 návrhu zákona a dále se s ním pracuje v návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. Nicméně se nebráníme novým návrhům, pokud vás nějaká vhodnější definice významného dodavatele napadá budeme za ní rádi, ale již dříve jsme se snažili definici upřesnit, ale vždy jsme se nakonec vrátili k obecné formulaci, jelikož každému subjektu definice významného dodavatele ve vyšší míře detailu vyhovuje rozdílně a nepokrývá potom všechny možné alternativy. Připomínkové místo s vypořádáním souhlasí.
211. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 9 Změna registrace poskytovatele regulované služby, odst. 1 Navrhujeme výslovně stanovit, že za změnu se považuje i výmaz, resp. ukončení regulované služby. Alternativně navrhujeme nastavení podmínek a lhůty v § 11. Ustanovení § 9 odst. 1 nestanovuje, jak provést změnu registrace poskytovatele regulované služby směrem k podání oznámení výmazu (ukončení) regulované služby. Obecně § 9 řeší pouze registraci dalších služeb a změny režimu, avšak nezabývá se možností oznámení změn ukončení regulované služby. Navazující § 11 sice	Akceptováno jinak Na základě této, ale i dalších souvisejících připomínek, došlo k tomu, že bude umožněn výmaz z evidence na žádost poskytovatele regulované služby. Subjekty však záměrně samy nemohou přes portál službu z evidence smazat, musí o tom rozhodnout vždy Úřad. Do výmazu regulované služby z evidence pak platí fikce, že se na službu zapsanou v evidenci vždy hledí jako na regulovanou službu. Poskytovatel

		stanovuje postup výmazu z evidence poskytovatelů regulovaných služeb z pohledu NÚKIB, ale nestanovuje proces (postup) podání oznámení změn z pohledu poskytovatele, pokud již nejsou plněna příslušná kritéria. Cílem je umožnit, aby činnost, která odpadne, mohla být formálně ihned zrušena a poskytovateli nevznikaly další náklady.	regulované služby tudíž musí plnit vůči této službě všechny povinnosti plynoucí mu ze zákona. Připomínkové místo s vypořádáním souhlasí.
212. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - §13 Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby, odst. 3 Vymazat část věty „, a odůvodnění jejich vyjmutí“ Důvodová zpráva v prvním odstavci daného paragrafu udává, že subjekty, které již nyní postupují podle platného a účinného zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti v procesu stanovování rozsahu řízení, budou mít situaci výrazně ulehčenou, jelikož nový postup pouze zpřesňuje již zavedenou praxi. Tuto tezi však vyvrací nová povinnost, kterou poskytovatelům ukládá právě odst. 3, § 13, který nad rámec popsaného a standardního procesu jednotlivých kroků identifikace, nastavuje povinnost naprosto opačnou, a to popsání a zdokumentování argumentace, proč daná aktiva nebyla zařazena. V krocích, které vyžaduje návrh nového zákona a prováděcí právní předpisy, však stanovuje jasně popsat i předchozí kroky, které k zařazení aktiva vedou. Pro dokumentaci a doložení argumentů, proč dané aktivum nebylo zařazeno, tedy dostačuje interpretace popisu aktiva v předchozích krocích celého procesu. Popis nad rámec tohoto přináší administrativní zátěž subjektům a nepřináší přidanou hodnotu NÚKIB.	ROZPOR Neakceptováno Dle směrnice NIS 2 měl být rozsah řízení kybernetické bezpečnosti stanoven na celou organizaci. Aby NÚKIB neúměrně nezatěžoval povinné subjekty, rozhodl se umožnit vyjmout z rozsahu primární aktiva, která s regulovanou službou nesouvisí. Definice řízení kybernetické bezpečnosti podle písm. g) říká, že je to činnost směřující k zajištění kybernetické bezpečnosti regulované služby, tzn. zajištění regulované služby je hlavním cílem, neznamená to však, že by rozsah nemohl být stanoven na celou organizaci, pokud to povinná osoba vyhodnotí jako vhodné, aby mohla kybernetickou bezpečnost regulované služby řádně zajistit. Dále § 13 odst. 1 říká následující: „je nutné identifikovat všechna primární aktiva [písm. a)], následně identifikovat ta, která souvisí s regulovanou službou [písm. b)] a nakonec identifikovat podpůrná aktiva související s primárními aktivy potřebnými pro regulovanou službu [písm. c)]. Rozsah je stanoven pouze na aktiva dle písm. b) a c), tedy na primární aktiva související s regulovanou službou a na ně navázána podpůrná aktiva. Není tedy pravda, že by dle § 13 odst. 2 rozsah tvořila všechna aktiva. Nesouhlasíme s tím, že to bude administrativně zatěžující, bude se jednat o primární aktiva v množství jednotek a jednoduchého zdůvodnění (např. nesouvisí

			s regulovanou službou). Je pracováno s typovými aktivy, nikoliv s každou službou/informací jako takovou zvlášť. Jde o základní identifikaci služeb, které organizace poskytuje (za jakým účelem je vytvořena a co jsou její core služby). Vše slouží k tomu, aby bylo možné ověřit, zda byl rozsah stanoven správně. Ze zkušeností z kontrol vyplývá, že povinné osoby mají rozsah stanoven nesprávně, proto bylo ustanovení zpřesněno. Hodnocení aktiv a rizik se vždy provádí ve stanoveném rozsahu.
213. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 14 Bezpečnostní opatření, odst. 1 Navrhujeme vypustit druhou větu: „(1) Bezpečnostními opatřeními se rozumí úkony, jejichž cílem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv. ~~Bezpečnostními opatřeními jsou organizační a technická opatření.~~“ Dle § 14 jsou bezpečnostními opatřeními organizační a technická opatření. Vnímáme argumentaci předkladatele, že pro režim vyšších povinností jsou nastavena přísnější pravidla, zároveň není jasné, proč nelze – minimálně fakultativně – nastavit organizační a technická opatření i pro služby v režimu nižších povinností. V případě holdingu může totiž dojít k situaci, kdy některé společnosti spadnou do režimu vyšších a jiné do režimu nižších povinností. Zpravidla se však pro celý holding zpracovává jednotná řídicí dokumentace a bude poměrně náročně vést dvojkolejnou dokumentaci – organizační a technická opatření pro vyšší režim a bezpečnostní opatření pro režim nižší. Ideální by bylo zachovat možnost stejného rozdělení pro oba režimy, ale věcný rozsah upravit dle typu režimu.	Neakceptováno Jednotlivé ustanovení návrhu vyhlášky pro režim nižších povinností kombinují oba typy bezpečnostních opatření, z toho důvodu nebylo účelné je rozdělovat na organizační a technická. Toto řešení nemění podstatu bezpečnostních opatření, dále bylo cílem regulátora zpracovat přehledný a srozumitelný předpis, kdy bude na první pohled jasné, jaká všechna bezpečnostní opatření se váží k dané oblasti (např. BCM, obsahuje jak organizační, tak technická bezpečnostní opatření) - všechna bezpečnostní opatření k BCM jsou tak přehledně uvedena v jednom ustanovení. Je jedno, jak bude dokumentace označena, podstata opatření zůstává stejná, pro plnění zákonných povinností není důležité, zda jsou jednotlivá bezpečnostní opatření definována v interní dokumentaci jako technická nebo organizační, ale je důležité, zda jsou fakticky zaváděna. Pro lepší pochopení byl upraven § 15 odst. 2 aby bylo jasné, že bezpečnostní opatření pro režim nižších povinností jsou organizačního a technického typu, i když nejsou rozděleny samostatně, jako je tomu v režimu vyšších povinností, z důvodů uvedených výše. Praktičností

			nastavení jednotného přístupu v rámci holdingu rozumíme a nevidíme to v tom v budoucnu aplikační problém. Rádi bychom i k této problematice vydali samostatnou metodiku, která bude porovnávat jaké ustanovení vyhlášky z režimu vyšších povinností lze podřadit pod ustanovení vyhlášky pro režim nižších povinností, tak aby bylo možné jednotné řízení ISMS pro lepší efektivnost a hospodárnost procesů v rámci holdingu. Připomínkové místo s vypořádáním souhlasí.
214. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 15 Seznam bezpečnostních opatření, odst. 2 písm. c) Navrhujeme doplnit za slovo „řízení“ slova „aktiv a“ Řízení rizik je možné pouze tehdy, jsou-li identifikována aktiva. Teprve po identifikaci aktiv lze definovat rizika. Teze prováděcích právních předpisů k navrhované právní úpravě řízení aktiv vůbec v nižším režimu. Naopak vyhláška o bezpečnostních opatřeních poskytovatele služby v režimu vyšších povinností v § 8 výslovně stanoví řízení aktiv a v § 9 řízení rizik. Původní návrh právní úpravy, který NÚKIB předložil k veřejné konzultaci (dokument 1a str. 10 – odst. 3 písm. v) „řízení aktiv“ obsahoval. Pokud tedy nedojde k doplnění samostatného bodu týkajícího se řízení aktiv, navrhujeme spojení řízení aktiv a řízení rizik do jednoho bodu.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
215. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 16 Navrhujeme znění zákona přizpůsobit znění a záměru NIS2 a zachovat povinnosti pro subjekty, které odpovídají označení “essential” a “important” ve smyslu NIS2. Jiná úprava by mohla být v rozporu s NIS2 a vytvořit nerovnoměrné zatížení subjektů.	ROZPOR Neakceptováno Nová úprava podle směrnice NIS 2 reflektuje snahu EU o zajištění vysoké společné úrovně kybernetické bezpečnosti napříč celou EU, proto jsou mezi povinné osoby ve vysoce kritickém odvětví nad rámec stávající

	Článek 23 směrnice NIS 2 stanoví ohlašovací povinnosti základních a významných subjektů. Podle tohoto ustanovení musí základní a významné subjekty hlásit každou událost, která má významný dopad na poskytování jejich služeb. Návrh zákona implementuje článek 23 směrnice NIS 2 ve svém § 16. V porovnání se směrnicí NIS 2 stanoví § 16 pro základní subjekty přísnější pravidla než pro významné subjekty. Podle tohoto ustanovení musí významné subjekty hlásit každou událost bez ohledu na její dopad na poskytování svých služeb. NÚKIB v této souvislosti odkazuje na článek 5 směrnice NIS 2, který členským státům umožňuje přijmout nebo zachovat ustanovení zajišťující vyšší úroveň kybernetické bezpečnosti, pokud jsou tato ustanovení v souladu s právem EU. To potvrzuje i relevantní část důvodové zprávy. NÚKIB odůvodňuje tuto úpravu odkazem na stávající zákon o kybernetické bezpečnosti a uvádí, že takový přístup se v současné době uplatňuje. To nepokládáme za zcela vypovídající. Ustanovení § 8 zákona o kybernetické bezpečnosti rozlišuje oznamovací povinnosti většiny regulovaných subjektů a dále pak poskytovatelů digitálních služeb. Poskytovatelé digitálních služeb hlásí pouze takový incident, který má významný dopad na poskytování jejich služeb. Na základě výše uvedeného a s ohledem na nové rozlišení základních a významných subjektů by se na poskytovatele cloudových služeb mohla vztahovat mnohem přísnější pravidla ve srovnání se současným stavem, neboť by mohli být považováni rovněž za základní subjekty. Rozšíření kompetence nad rámec stanovený NIS2 povede k i) neúměrnému vytížení subjektů a rozmělnění povinnosti oproti požadavkům dalších členských států, kde stejnou povinnost mít nebudou a zejména pak k ii) zahlcení NÚKIB reporty, které budou postrádat důležitost a výpovědní hodnotu.	právní úpravy zahrnutí mj. i poskytovatelé služeb cloud computingu. Do režimu vyšších povinností, se kterým je vázána povinnost hlásit všechny kybernetické bezpečnostní incidenty, budou poskytovatelé služeb cloud computingu spadat pouze v případě, že jsou velkým podnikem, nebo poskytovatelem státního cloud computingu podle zákona o informačních systémech veřejné správy. Navrhovaná právní úprava vychází ze základní zásady, na níž je založena směrnice NIS 2, totiž že subjekty spadající do oblasti působnosti právní úpravy by měly být zařazeny do dvou kategorií, s přihlédnutím k míře kritické důležitosti, pokud jde o odvětví nebo druh služby, kterou poskytují, a také k jejich velikosti (viz recitál 15 uvedené směrnice). Jinak řečeno, stane-li se osoba poskytovatelem regulované služby ve vyšším povinnostním režimu, znamená to, že odvětvím, v němž poskytuje službu, respektive kombinací tohoto odvětví a vlastní velikosti dosahuje hranice vysoké míry kritické důležitosti pro Českou republiku. Kritérium poskytování státního cloud computingu vychází z požadavku na zabezpečení digitální infrastruktury státu. Podle ustanovení § 6m odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy je pro zajištění provozu informačního systému veřejné správy zařazeného do kritické bezpečnostní úrovně pomocí služeb cloud computingu nutné využít služeb státního poskytovatele cloud computingu. Poskytovatel státního cloud computingu bude tedy zřejmě zajišťovat provoz určité části pro stát kritických systémů, z toho důvodu by na něj měly být kladeny minimálně obdobné požadavky na zajištění kybernetické bezpečnosti, jaké jsou kladeny na systémy, k zajištění jejichž provozu jsou jeho služby

			využívány. Z důvodu kumulace zajišťování provozu více kritických systémů orgánů veřejné správy nestačí spoléhat na přenesení povinností v rámci řízení dodavatelů. Z výše uvedeného vyplývá nutnost zařadit tyto poskytovatele do režimu vyšších povinností. Požadavek na hlášení všech kybernetických bezpečnostních incidentů bez ohledu na to, zda mají významný dopad, reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob.
216. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 17 Náležitosti hlášení kybernetických bezpečnostních incidentů, odst. 3 písm. b) a c), odst. 5, Vyhláška o Portálu NÚKIB a požadavcích na vybrané úkony, § 3 Hlášení kybernetického bezpečnostního incidentu Doplnit náležitosti závěrečné zprávy buď přímo do odstavce 3 nebo do § 3 Vyhlášky o Portálu NÚKIB Paragraf 17 odst. 3 písm. b) a c) ZKB ukládá poskytovatelům regulované služby povinnost do 30 dní od oznámení incidentu nebo předložení zprávy o aktuálním stavu zvládnutí kybernetického bezpečnostního incidentu předložit závěrečnou zprávu, jejíž náležitosti mají být dle odst. 5 stanoveny prováděcím předpisem.	Akceptováno Ustanovení § 17 odst. 5 návrhu zákona obsahuje zmocňovací ustanovení pro vydání prováděcího předpisu, který stanoví mj. obsahové náležitosti hlášení incidentu. Tímto předpisem je vyhláška o Portálu NÚKIB a požadavcích na vybrané úkony, která v § 3 odst. 1 stanovuje obsahové náležitosti formuláře pro hlášení incidentů, přičemž z odst. 2 písm. d) tohoto ustanovení vyplývá, že jde přes daný formulář vytvořit i závěrečnou zprávu, jejíž náležitosti byly doplněny do odst. 3.

		Vyhláška o Portálu NÚKIB ale v § 3, který popisuje obsahové náležitosti úkonů spojených s hlášením kybernetických bezpečnostních incidentů se ale nevěnuje konkrétním náležitostem závěrečné zprávy, nýbrž pouze popisu obsahu formuláře pro hlášení incidentů, z něhož vyplývá, že slouží primárně k oznamování incidentů dle § 17 odst. 1 písm. a) nebo c) podávání průběžné zprávy o podstatných změnách stavu zvládání kybernetického bezpečnostního incidentu podle § 17 odst. 3 písm. b) zákona. Navrhujeme proto doplnit obsahové náležitosti závěrečné zprávy, aby se předešlo nejistotě regulovaných osob ohledně způsobu plnění povinností podle § 17 odst. 1 písm. b) a c), obzvláště vzhledem k tomu, že za jejich porušení hrozí dle § 58 odst. 1 písm. h) ve spojení s odst. 15 písm. a) pokuta ve výši až 250 000 000 Kč nebo do výše 2 % čistého celosvětového ročního obratu.	Připomínkové místo s vypořádáním souhlasí.
217. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 19 Informační povinnost poskytovatele regulované služby, odst. 1 V odst. 1 po slovech „je dotčen kybernetickým bezpečnostním incidentem s významným dopadem“ doplnit slova „, po konzultaci s poskytovatelem regulované služby,“ V případě, že NÚKIB uloží takovou povinnost bez předchozí konzultace, může dojít k poskytnutí informací, které takový incident mohou prohloubit, případně i vyvolat další incidenty případným zveřejněním zranitelností, kterých útočník využil.	Akceptováno - nyní § 20 Připomínkové místo s vypořádáním souhlasí.
218. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 19 Informační povinnost poskytovatele regulované služby, odst. 2 Na začátku odstavce 2 nahradit slova „Poskytovatel regulované služby“ za slova „Dozví-li se poskytovatel regulované služby o významné kybernetické hrozbě ohrožující poskytování jím poskytované regulované služby“. Ze současného znění zákona není patrné, o jakých hrozbách by měl poskytovatel regulované služby uživatele informovat a zároveň je	ROZPOR Neakceptováno - nyní § 20 O hrozbách, o kterých se poskytovatel regulované služby nedozví a nemohl dozvědět, není z podstaty věci možné kohokoliv informovat a toto jednání sankcionovat. Vztahovat informační povinnost na uživatele kterékoliv regulované služby se zároveň jeví jako výrazně extenzivní výklad, který úmyslem

		povinnost stanovena nezávisle na vědomosti poskytovatele o existenci hrozby. Povinnost je přitom spojena s nejvyšší možnou pokutou dle § 58 odst. 1 písm. k) ve spojení s odst. 15 písm. a). Navrhujeme proto jasně definovat, že poskytovatel je povinen informovat pouze o hrozbách, o kterých se dozví, a které ohrožují jím poskytovanou regulovanou službu. Dle současného znění by totiž bylo možné sankcionovat jakéhokoli poskytovatele za jakoukoli významnou hrozbu nezávisle na tom, jestli se hrozba dotýká jím poskytované regulované služby a jestli o hrozbě poskytovatel věděl nebo vědět měl.	zákonodárce není a nevyplývá z textu zákona ani důvodové zprávy. Vzhledem k provázanosti poskytovatele regulované služby, regulované služby a uživatele regulované služby, by nemělo dojít k pomýlení, že bude poskytovatel regulované služby muset informovat o hrozbách, jež se službou, kterou poskytuje, vůbec nesouvisí, případně pak informovat uživatele jiných regulovaných služeb.
219. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 19 Informační povinnost poskytovatele regulované služby, odst. 2 Ve větě první po slovech „bez zbytečného odkladu“ doplnit slova „informovat Úřad, který“ a upravit slovo „informovat“ na „informuje“ v části věty „způsobem informovat uživatele“. Informace o významné kybernetické hrozbě by měl poskytovatel regulované služby poskytnout NÚKIB, který agregovaně předá informaci širokému spektru subjektů, aby tak nedocházelo k přílišnému zahlcení pracovních kapacit poskytovatele regulované služby při nutnosti podávání individualizované informace o možnosti čelit takové hrozbě jednotlivým subjektům. Tyto kapacity pak může poskytovatel využít pro řešení případné hrozby a k dalším úkonům potřebným k udržení nejvyšší úrovně kybernetické ochrany. Variantně bychom požadovali alespoň ujištění o tom, že informace předávané poskytovatelem jsou shodné s generickými informacemi podávanými subjektům čelícím významné kybernetické hrozbě.	Neakceptováno - nyní § 20 Informování příjemců služeb o hrozbách přímo ze strany poskytovatelů regulovaných služeb je požadavkem směrnice NIS 2. Přehledem o uživatelích regulované služby (např. seznamem zákazníků) disponuje pouze daný poskytovatel regulované služby. Předání informací o hrozbě společně se seznamem zákazníků Úřadu, aby je tento mohl o hrozbě informovat, se nejeví jako vhodné a efektivní řešení. Pouze poskytovatel regulované služby bude nadto disponovat dostatečně podrobnými a aktuálními informacemi jak o samotné hrozbě, tak o krocích, které mohou uživatelé učinit v reakci na tuto hrozbu. Připomínkové místo s vypořádáním souhlasí.
220. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 23 odst. 5 a 6 Vypustit Navrhujeme, aby byla zrušena všechna uvedená ustanovení:	Neakceptováno - nyní § 24 Zákon o kybernetické bezpečnosti ani v současné podobě neobsahuje jiný, než v současnosti navrhovaný proces vydávání reaktivního protipatření (dříve reaktivního opatření). Účelem reaktivního

		§ 23 odst. 5 a 6 – návrh připouští podání jen připomínek ve lhůtě 30 dnů proti vydanému opatření obecné povahy, připomínky jsou poněkud slabší nástroj ochrany ve vztahu k námitkám, o nichž je orgán vydávající opatření obecné povahy povinen samostatně rozhodnout, zrušením ustanovení se použije postup podle § 172 a násl. správního řádu, kde je možno uplatnit připomínky i námitky. Ve srovnání s připomínkami představují námitky procesně silnější nástroj ochrany práv. Dále je potřeba uvést, že jen postup podle § 172 a násl. správního řádu je zárukou uplatnění práv, povinností nebo zájmu těch, kteří jsou opatřením obecné povahy přímo dotčeni, jelikož ustanovení § 173 odst. 2 správního řádu určuje, že proti opatření obecné povahy nelze podat opravný prostředek, kterým by mohli dosáhnout nápravy. Proti opatření obecné povahy nelze podat odvolání ani rozklad (na rozdíl od správního rozhodnutí).	protiopatření je co nejrychleji a v případech, které nesnesou odkladu reagovat na vyvstálé riziko. Z tohoto důvodu byl jediný přiléhavý nástroj obsažený v rámci správního řádu příslušně upraven a navrhovaná část celého procesu opatření obecné povahy nebyla zavedena jako součást procesu vydávání reaktivního protiopatření, stejně jako nebyla součástí procesu původního reaktivního opatření. Zavedení navrhovaného by tedy bylo v přímém rozporu s účelem tohoto ustanovení, které je již ověřeným institutem, který byl ze strany Úřadu již několikrát úspěšně použit. Připomínkové místo s vypořádáním souhlasí.
221. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - Díl 3 Vztah poskytovatele regulované služby a jeho dodavatelů Navrhujeme doplnit ustanovení zavazující určeného dodavatele k součinnosti při plnění zákonných požadavků poté, co byl prokazatelně informován, že se stává osobou zajišťující bezpečnostně významnou dodávku strategické služby. Dodavatel by měl mít v zákoně výslovně stanovenou povinnost spolupracovat. V praxi totiž bez součinnosti dodavatele nemusí být poskytovatel regulované služby schopen splnit zákonné požadavky.	Neakceptováno Uložení zákonné povinnosti dodavatelům bezpečnostně významné dodávky poskytovat součinnost poskytovateli strategicky významné služby Úřad považuje za neproporcionální řešení. Navrhované řešení by neúměrně zatížilo Úřad, potažmo stát, přičemž vymáhání plnění takto stanovené povinnosti by bylo velmi problematické. V potaz je také nutno vzít skutečnost, že aplikací navrhovaného řešení by si Úřad vytvořil příliš extenzivní pravomoci. Úřad si je vědom, že pro poskytovatele strategicky významné služby může být za určitých okolností složité získat informace zejména o svých nepřímých dodavatelích. Z tohoto důvodu návrh zákona nestanoví poskytovateli strategické služby povinnost zjistit informace o dodavatelích bezpečnostně významných dodávek, ale stanoví povinnost poskytovatele strategicky významné služby

			tyto informace o dodavatelích bezpečnostně významných dodávek aktivně zjišťovat, a to s vynaložením přiměřeného úsilí. Posouzení, zda poskytovatel strategicky významné služby vynaložil přiměřené úsilí, či nikoliv bude vždy záviset na konkrétních skutkových okolnostech. Vzhledem k výše uvedenému je Úřad přesvědčen, že získávání informací o dodavatelích bezpečnostně významných dodávek má být v gesci poskytovatelů strategicky významné služby. Povinnosti dodavatelů je nutné smluvně ošetřit v rámci řízení dodavatelů. Připomínkové místo s vypořádáním souhlasí.
222. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 24 Řízení dodavatelů a vztah k zadávání veřejných zakázek, odst. 2 Navrhujeme upřesnit v důvodové zprávě kritéria pro posouzení možnosti/nemožnosti zanesení bezpečnostních požadavků. Jedná se o nový institut, proto by bylo vhodné koncipovat důvodovou zprávu podrobněji. Zejména jde o to, zda je poskytovatel regulované služby povinen splnit povinnosti i v případě značných nákladů.	Neakceptováno – nyní § 25 Ustanovení § 25, resp. jeho odst. 2, není v regulaci kybernetické bezpečnosti ničím novým, naopak jde o ustanovení přejaté z aktuálně účinného § 4 odst. 4 zákona č. 181/2014 Sb., které doznalo pouze mírných formulačních změn tak, aby nedocházelo k výkladovým nejasnostem. Stejně jako za současného zákona č. 181/2014 Sb. tedy bude platit, že poskytovatel regulované služby bude povinen zohlednit požadavky vyplývající z bezpečnostních opatření podle § 14 a § 15 návrhu zákona při výběru svých dodavatelů, stejně jako bude i do budoucna platit současná povinnost povinných osob zohledňovat požadavky vyplývající z bezpečnostních opatření ve smlouvách se svými dodavateli. Oproti současné úpravě bylo doplněno „<i>tam, kde je to možné</i>“. Toto doplnění míří zejména na situace, kde nové požadavky vyplývající z bezpečnostních opatření vstupují do již existujících smluvních vztahů. V takovém případě je poskytovatel regulované služby povinen učinit vše pro to, aby již uzavřené smlouvy

			vedl do souladu s požadavky návrhu zákona (požadavky vyvěrajícími z bezpečnostních opatření podle § 14 a § 15 návrhu zákona). V odůvodněných případech, kdy není možné smlouvu změnit či ukončit (z toho důvodu odstavec 2 používá formulaci „<i>tam, kde je to možné</i>“), je možné ve smluvním vztahu po nezbytně nutnou dobu pokračovat a požadovanou úroveň kybernetické bezpečnosti zajistit jiným způsobem (zejm. zavedením kompenzačních bezpečnostních opatření). Výše nákladů na promítnutí bezpečnostních požadavků do smluv obecně nemůže být důvodem pro neplnění požadavků zákona, v závislosti na konkrétních skutkových okolnostech však může být např. relevantním důvodem pro rozložení plnění jednotlivých povinností do delšího časového úseku, případně pro zavedení jiných kompenzačních opatření, která budou zajišťovat potřebnou úroveň kybernetické bezpečnosti. Od požadavků stanovených v § 25 je pak potřeba odlišovat mechanismus podle § 29 a násl. návrhu zákona, resp. opatření obecné povahy podle § 31 návrhu zákona, které může být (v závislosti na jeho obsahu) přímo aplikovatelné a jeho plnění v tu chvíli nebude probíhat v režimu § 25. Připomínkové místo s vypořádáním souhlasí.
223. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 25 Speciální úprava předání informací a dat od významného dodavatele, odst. 1 Doporučujeme navrhnout bližší specifikaci „<i>informace a data související s provozem aktiv soužících k poskytování regulované služby, kterými významný dodavatel disponuje a které nejsou předmětem ochrany podle autorského práva</i>“.	Akceptováno jinak - nyní § 26 Pokud by informace a data související s provozem aktiv sloužících k poskytování regulované služby, která jsou zároveň předmětem ochrany podle autorského práva, byla nepostradatelná pro zajištění kybernetické bezpečnosti regulované služby, nelze je z povinnosti předání vyjmout. Výsledná množina předaných dat a informací by mohla být nepoužitelná

	Doporučujeme doplnění explicitní úpravy pro situaci, kdy významný dodavatel požadovanými informacemi a daty nedisponuje, ale bude požadováno jejich opatření a následné vydání: <i>„Pokud významný dodavatel informacemi nebo daty souvisejícími s provozem aktiv sloužících k poskytování regulované služby nedisponuje, přesto bude účelné uložit jejich opatření a vydání, je poskytovatel regulované služby povinen uhradit významnému dodavateli v této souvislosti účelně vynaložené náklady.“</i> Již v současné době působí aplikační problémy nedostatečné vymezení okruhu dat a informací spadajících pod povinnost vydání podle § 6a odst. 2 a 3 ZoKB. Navržená úprava představuje minimální zpřesnění na informace a data, kterými významný dodavatel disponuje. Pro případ požadavku takových informací a dat, kterými naopak nedisponuje, by mu měla náležet odměna v podobě účelně vynaložených nákladů. Návrh ZoKB to implicitně řeší v odstavci 4 dotčeného ustanovení. V rámci vyváženosti je však nutné dle odst. 4, která chrání poskytovatele významné služby, zakotvit rovněž ochranu významných dodavatelů, a to v podobě explicitního závazku na nárok na odměnu za poskytnuté plnění. Významný dodavatel by rovněž neměl být nucen předávat informace a data, která představují dílo ve smyslu autorského zákona. Je za poskytovateli regulované služby, aby si vhodně ošetřil licenční problematiku v soukromoprávní smlouvě. NÚKIB by neměl suplovat zanedbání těchto otázek ve smlouvě. Ve svém důsledku může takto široká povinnost významného dodavatele předat data a informace vést k rezignaci poskytovatele regulované služby, jako zadavatelů veřejných zakázek, na ošetření problematiky licenčních ujednání, exitového plánu apod.	a institut předání dat by postrádal smysl. Dotčené strany by z tohoto důvodu měly mít náležitě upravena smluvní ujednání týkající se finanční kompenzace práv duševního vlastnictví. Odstavec 4 předmětného ustanovení byl upraven následovně: <i>„Významný dodavatel nebo jiný orgán nebo osoba, která požadovanými informacemi a daty disponuje, má nárok na úhradu účelně vynaložených nákladů spojených s předáním informací a dat ze strany poskytovatele regulované služby v režimu vyšších povinností. [...]“.</i> Co se týče vymezení okruhu dat a informací spadajících pod povinnost předání, ten se bude odvíjet od okolností konkrétního případu a není možné jej stanovit paušálně. Povinnost zanést do smlouvy specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání povinnou osobou je součástí bezpečnostních opatření, která bude poskytovatel regulované služby v režimu vyšších povinností povinen zavádět. Vzhledem k tomu, že příslušná ujednání by měla být součástí smluvního vztahu mezi poskytovatelem regulované služby a významným dodavatelem, měl by institut předání dat podle § 26 sloužit jako <i>ultima ratio</i> až poté, co selžou jednání mezi dotčenými stranami. Zároveň musí být pro vydání rozhodnutí splněna podmínka hrozícího či probíhajícího kybernetického bezpečnostního incidentu, který by mohl mít závažný vliv na poskytování regulované služby s dopadem na zachování základních funkcí státu, hospodářských činností, bezpečnosti, veřejného zdraví, majetku nebo životního prostředí, která vymezuje kritičnost nastalé situace. Podmínka hrozícího incidentu je dostatečně

			určitým vyjádřením akutnosti situace a zároveň dostatečně obecnou podmínkou tak, aby bylo možné zahrnout pod toto ustanovení širokou paletu typů incidentů, které hrozí. Nadužívání tohoto institutu je z výše uvedených důvodů vysoce nepravděpodobné, o čemž svědčí i dosavadní praxe Úřadu, kdy rozhodně nedochází k vysoké frekvenci aplikace tohoto ustanovení. Připomínkové místo s vypořádáním souhlasí.
224. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 58 přestupky, odst. 15 Navrhujeme v písm. a) a v písm. b) za slovo „nebo“ vložit slova „tam, kde je to vzhledem k okolnostem přiměřené“ Znění návrhu zákona věrně implementuje znění směrnice, která v souladu s judikaturou k soutěžním článkům 101 a 102 SFEU konstatuje <u>možnost</u> uložení pokuty za přestupek vypočítané na základě obratu podniku ve smyslu soutěžního práva, tj. ekonomické jednotky/skupiny, ke které pachatel patří. V souladu s judikaturou SDEU zdůrazňujeme „pouhou“ možnost takového postupu, tedy zabránění automatickému používání obratu skupiny jako stropu pro výpočet pokuty u pachatele, který náleží do (nějaké) skupiny/konsolidačního celku.	Akceptováno jinak Dojde k úpravě ustanovení o přestupcích (§ 60 odst. 15 návrhu zákona) a doplnění podmínky pro uplatnění kritéria obratu konsolidačního celku (obviněný skutek spáchal ve spojení s konsolidačním celkem nebo v jeho prospěch). Tím dojde k zesouladění s koncepcí podniku ve smyslu čl. 101 a 102 SFEU, jak požaduje směrnice NIS 2. Připomínkové místo s vypořádáním souhlasí.
225. Svaz průmyslu a dopravy ČR	Z	Zákon o kybernetické bezpečnosti - § 54 Vzájemná součinnost s členskými státy EU, § 63 Součinnost, § 67 Zástupce pro Českou republiku Působnost zákona – implementace one-stop-shop mechanismu ve smyslu článku 26 odst. 1 a 2 směrnice NIS 2 Předložený zákona o kybernetické bezpečnosti nedostatečným způsobem implementuje požadavky čl. 26 odst. 1 a 2 směrnice NIS 2. V souladu s uvedeným odůvodněním navrhujeme do § 1 návrhu zákona doplnit nové odstavce 4) a 5) s následujícím zněním:	Akceptováno jinak - nyní § 57, 65 a 68 Připomínka vychází z premisy, že regulovány mají být pouze subjekty, které mají v České republice sídlo (se speciálním režimem pro poskytovatele veřejných sítí a služeb elektronických komunikací a vybrané poskytovatele služeb v odvětví digitální infrastruktury, k tomu viz dále), přičemž se odkazuje na znění směrnice NIS 2 a jejího čl. 26 odst. 1. Směrnice NIS 2 ale nehovoří o „sídle“, nýbrž o

		„4) Aniž je dotčen mechanismus součinnosti podle § 60 a povinnosti k jmenování zástupce podle § 67, tento zákon se nevztahuje na osoby, které mají sídlo v jiném členském státě, s výjimkou těchto případů: a) poskytovatel veřejně dostupné služby elektronických komunikací [poznámka pod čarou: Zákon č. 127/2005 Sb., o elektronických komunikacích]; b) osoba zajišťující veřejnou komunikační síť [poznámka pod čarou: Zákon č. 127/2005 Sb., o elektronických komunikacích]; c) následující subjekty, jejichž hlavní provozovna ve smyslu odstavce 5 se nachází v České republice: 1. subjekt poskytující služby registrace jmen domén a poskytovatel regulované služby, který je poskytovatelem služby systému překladu jmen domén (DNS), 2. poskytovatel správy a provozu registru internetových domén nejvyšší úrovně, 3. poskytovatel služby cloud computingu, 4. poskytovatel služby datového centra, 5. poskytovatel služby sítě pro doručování obsahu (CDN), 6. poskytovatel služby on-line tržiště, 7. poskytovatel služby internetového vyhledávače, 8. poskytovatel služby platformy sociální sítě, 9. poskytovatel řízené služby (MSP), nebo 10. poskytovatele řízené bezpečnostní služby (MSSP).	„usazení“ (angl. <i>establishment</i>), a tyto pojmy je třeba odlišovat. Pojem usazení byl zaveden již směrnicí NIS 1, kde byl vykládán funkčně a předpokládal účinný výkon činnosti regulovaného subjektu prostřednictvím stálých struktur, nezávisle na právní formě takové struktury nebo její závislosti na jiných strukturách umístěných mimo území daného státu. Vycházel přitom z práva na usazení definovaného Smlouvou o fungování EU a zahrnoval jak primární usazení, tedy zřízení nebo přesunutí hlavního centra činnosti na území daného státu, tak i sekundární usazení, tedy zřízení zastoupení, pobočky nebo dceřiné společnosti v jiném členském státě EU za současného zachování původního sídla v jiném členském státě. Směrnice NIS 2 zavedený pojem usazení bez dalšího přejímá. I pro potřeby směrnice NIS 2 (srov. bod 114 preambule) a návrhu zákona tak pojem usazení má být vykládán tak, že jde o místo, kde jsou fakticky vykonávány činnosti regulovaného subjektu prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, odštěpný závod nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem. Kritérium usazení může být v určitých případech splněno i v případě, že se v daném státě fyzicky nacházejí sítě a informační systémy používané pro výkon regulované služby. Otázka stálého zařízení totiž není ani judikaturou Soudního dvora EU k výkladu svobody usazování přesně definována, může se tak jednat o kancelář, provozovnu, pobočku apod. Stěžejním je požadavek na fyzickou přítomnost dané osoby na území předmětného státu. V praxi pak bude běžné, že jedna osoba bude usazena ve více státech EU současně.

	5) <i>Pro účely tohoto zákona se má za to, že hlavní provozovna subjektu podle odst. 4 písm. b) v Evropské unii je umístěna v členském státě, v němž jsou převážně přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. Nelze-li takový členský stát určit, nebo nejsou-li tato rozhodnutí přijímána v Evropské unii, má se za to, že hlavní provozovna je v členském státě, v němž daný subjekt provádí činnosti k zajištění kybernetické bezpečnosti. Nelze-li takový členský stát určit, má se za to, že dotčený subjekt má hlavní provozovnu v členském státě, v němž má provozovnu s nejvyšším počtem zaměstnanců v Evropské unii.</i> Ačkoliv NÚKIB připomínky k nedostatečné implementaci těchto ustanovení čl. 26 odst. 1 a 2 směrnice NIS 2 v rámci veřejné konzultace odmítl, vzhledem k potenciálním negativním dopadům nesprávné implementace na této připomínce trváme. Navrhujeme proto důslednou implementaci tohoto mechanismu ve smyslu čl. 26 odst. 1 a 2 směrnice NIS 2. V rámci vypořádání připomínek NÚKIB k tomuto uvedl, že „<i>ustanovení § Zástupce poskytovatele regulované služby</i>“ [resp. nyní § 67 návrhu zákona – Zástupce pro Českou republiku], resp. vymezení působnosti návrhu zákona, je třeba vnímat v kontextu § <i>Vzájemná součinnost s členskými státy Evropské unie</i> [resp. nyní tedy § 63 návrhu zákona – Součinnost], které ve svém odst. 3 omezuje pravomoci Úřadu vůči subjektům poskytujícím služby vyjmenované v navrhovaném odst. 4 písm. c) s hlavní provozovnou mimo ČR. Úřad je vůči těmto subjektům oprávněn provést kontrolu nebo jiný úkon pouze na základě a v rozsahu žádosti o součinnost ze strany jiného členského státu, v němž má poskytovatel regulované služby umístěnou svou hlavní provozovnu.“ Citovaná ustanovení §§ 63 a 67 však implementují jen odstavce 3, 4 a 5 článku 26 směrnice NIS 2 a nijak nereflektují požadavky odst. 1 a 2, které představují tzv. one-stop-shop mechanismus, resp. tedy stanovují že některé subjekty (z povahy poskytovaných služeb) vždy budou podléhat jen jedné národní úpravě v rámci EU (nikoliv tedy jednotlivým národními úpravám v každém členském státě, kde je	Pro vyjasnění situace a větší zesouladění s čl. 26 odst. 1 směrnice NIS 2 bude do návrhu zákona (§ 1) doplněno ustanovení o osobní působnosti zákona. Co se týče odkazu na úpravu v současném zákoně reflektující požadavky směrnice NIS 1, je potřeba jej posuzovat ve světle zbylých ustanovení směrnice. Směrnice NIS 1 nepožadovala po členských státech poskytování vzájemné součinnosti, jediná kooperace, která byla vyžadována, byla konzultace dotčených států při určování provozovatelů základní služby. Nebylo tedy potřeba si tedy nad dotčenými subjekty ponechávat dozorovou pravomoc. To se s příchodem směrnice NIS 2 změnilo a Úřad je nucen zvolit takové řešení, které zajistí, aby vzájemná součinnost byla v praxi realizovatelná. Připomínka navrhuje text „<i>aniž je dotčen mechanismus součinnosti podle § 60...</i>“ (pravděpodobně myšlen § 54 – nyní § 57), taková úprava je však podle názoru Úřadu nedostatečná a neopravňuje Úřad vůči dotčeným subjektům na vyžádání orgánu jiného členského státu aktivovat dozorové pravomoci (vzájemná součinnost není v zásadě o ničem jiném). Aby byl Úřad schopen vzájemnou součinnost poskytnout (např. dožádat po subjektu informaci, provést u něj kontrolu), musí existovat povinnost, která bude předmětem dozorové činnosti Úřadu. Návrh obsažený v připomínce takovou povinnost, a tedy i možnost Úřadu uplatnit na dožádání dozorové pravomoci, nepřináší. Aby však bylo dosaženo záměru směrnice NIS 2, kterým je jednak <i>one-stop-shop</i> pravidlo, jednak harmonizace povinností, které přeshraničně operující subjekty v digitálním odvětví plní, bude vůči těmto subjektům upraven okruh povinností v oblasti zavádění bezpečnostních opatření a hlášení incidentů

	taková služba poskytována). Ačkoliv by bylo možné vykládat teritoriální aplikovatelnost zákona prostřednictvím přímé aplikace článku 26 směrnice NIS2, nepovažujeme takový postup za vhodnou legislativní techniku, jelikož může vyvolávat značnou právní nejistotu u adresátů tohoto zákona. Domníváme se, že vyjasnění aplikovatelnosti zákona žádným způsobem neomezuje princip součinnosti a zástupce ve smyslu §§ 63 a 67, které jsou ostatně přímo předvídány v čl. 26 odst. 3 – 5 směrnice NIS 2, a tudíž evropský zákonodárce předpokládal, že tato ustanovení budou existovat vedle sebe. Pro vyloučení pochybností o tom, že mechanismus součinnosti bude i nadále možné uplatňovat navrhuje doplnit výslovný odkaz. Zároveň platí, že cílem návrhu zákona je implementovat směrnici NIS 2 (k tomu rovněž srov. § 1 odst. 2 návrhu zákona). Předložený návrh zákona nad rámec prosté implementace však obsahuje další povinnosti, které nemusí mít ve směrnici jednoznačnou oporu – např. prověřování dodavatelského řetězce ve smyslu § 28 a násl. návrhu zákona nebo požadavky na zjištění dostupnosti strategicky významných služeb ve smyslu § 34 návrhu zákona. Ačkoliv směrnice NIS 2 vychází z principu minimální harmonizace (srov. čl. 5) a veškeré povinnosti v tomto zákoně by tak měly být vykládány eurokonformně a v mezích směrnice NIS 2, při aplikaci těchto specifických povinností nemusí být zjevné, že na poskytovatele usazené v jiných členských státech EU, se tyto specifické povinnosti neuplatní, a tedy že nepodléhají působnosti českého zákona o kybernetické bezpečnosti. Jinými slovy nemusí být zjevné, že v souladu s čl. 26 odst. 1 a 2 směrnice NIS 2 podléhají jen právní úpravě členského státu, ve kterém mají hlavní provozovnu. V souladu s čl. 26 odstavce 1 a 2 směrnice NIS2 proto považujeme za klíčové vyjasnit na úrovni zákona, že český zákon o kybernetické bezpečnosti se neuplatní na vybrané subjekty, které jsou usazený či mají hlavní provozovnu v jiném členském státě či v něm poskytují své služby, a proto podléhají právnímu řádu tohoto členského státu. Navrhujeme stanovit, že zákon se nevztahuje na poskytovatele usazené v jiném členském státě, ledaže naplňují některou z výjimek	tak, že bude odkázáno na prováděcí předpis Komise podle čl. 21 odst. 5 a čl. 23 odst. 11 směrnice NIS 2. Tím bude zajištěno, že ačkoli subjekty mající hlavní provozovnu v jiném členském státě budou formálně vzato vázání českými národními povinnostmi (za účelem toho, aby nad nimi mohl Úřad na vyžádání vykonat dozorovou činnost), budou jimi vázání jen v rozsahu harmonizujících předpisů, kterými bude vázán i ve státě, do jehož jurisdikce v souladu s čl. 26 odst. 1 písm. b) směrnice NIS 2 spadá. Zároveň však tato úprava nevylučuje, aby Úřad tam, kde je to otázkou národní bezpečnosti (tedy výlučné pravomoci členských států, do které unijní právo nemůže zasahovat), mohl dotčené subjekty zavázat svým rozhodnutím nebo opatřením obecné povahy i nad rámec povinností vyplývajících z prováděcích aktů Komise. Reakce připomínkového místa. Připomínkové místo s vypořádáním nesouhlasilo. Reakce NÚKIB Zaslán návrh na úpravu § 19 a § 57. Připomínkové místo s vypořádáním souhlasí.

	stanovených v čl. 26 odst. 1 směrnice NIS2, jak jsou navržené implementovat do nového odstavce 4. V souladu s čl. 26 směrnice NIS 2 se český zákon o kybernetické bezpečnosti tak uplatní pouze na: - osoby sídlící v České republice, které naplní definici poskytovatele regulované služby (<i>standardní teritoriální princip již implementovaný v návrhu zákona</i>). - poskytovatele veřejně dostupné služby elektronických komunikací, který v souladu se zákonem o elektronických komunikacích poskytuje služby na území České republiky (<i>čl. 26 odst. 1 písm. a) směrnice NIS2</i>); - osoby zajišťující veřejnou komunikační síť v souladu se zákonem o elektronických komunikacích na území České republiky (<i>čl. 26 odst. 1 písm. a) směrnice NIS2</i>); a - ty poskytovatele specifikovaných služeb, kteří mají hlavní provozovnu na území České republiky, navrhuje implementovat v odst. 4 písm. c) bodech 1 – 10 tohoto návrhu (<i>čl. 26 odst. 1 písm. b) směrnice NIS2</i>). Pro úplnost uvádíme, že obdobným způsobem byla z působnosti dosavadní směrnice „NIS1“ (směrnice (EU) 2016/1148) vyňata aplikovatelnost na poskytovatele digitálních služeb. Pro srovnání: Článek 26 odst. 1 směrnice NIS 2 Má se za to, že subjekty spadající do oblasti působnosti této směrnice podléhají pravomoci členského státu, v němž jsou usazeny, s výjimkou těchto případů: [...] Článek 18 odst. 1 směrnice NIS 1 Pro účely této směrnice se má za to, že poskytovatel digitálních služeb podléhá pravomoci členského státu, v němž je primárně usazen. Má-li poskytovatel digitálních služeb v některém členském	

		státě své sídlo, má se za to, že je v tomto členském státě rovněž primárně usazen. Článek 18 odst. 1 směrnice NIS 1 byl přitom implementován ve stávajícím znění zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, následovně: „<i>Tento zákon se nevztahuje na poskytovatele digitální služby, který má sídlo v jiném členském státě.</i>“ (srov. § 33 odst. 4 zákona č. 181/2014 Sb.).	
226. Svaz průmyslu a dopravy ČR	Z	Vyhláška o kritériích rizikovosti dodavatele - Příloha bod 11 Vypustit bod 11 přílohy vyhlášky <i>„Je důvodná obava, že schopnost dodavatele poskytovat plnění může být významným způsobem omezena či jinak narušena“.</i> Bod 11 přílohy vyhlášky nesměruje k ochraně vůči dodavatelům, kteří představují bezpečnostní hrozbu pro Českou republiku nebo vnitřní či veřejný pořádek, ale proti dodavatelům, kteří by potenciálně nemuseli být schopni dostát svým smluvním závazkům. Čistě ekonomické schopnosti dodavatelů jsou záležitostí podnikatelského rizika poskytovatelů strategicky významných služeb, kteří pravděpodobně disponují podrobnějšími informacemi o sektoru, v němž podnikají než orgány státní správy. Jedná se tudíž o nadbytečné ustanovení, které má zbytečný potenciál omezovat svobodu podnikání poskytovatelů strategicky významných služeb. Z tohoto důvodu navrhujeme ustanovení vypustit.	ROZPOR Neakceptováno Nutno zmínit, že teze prováděcích právních předpisů jsou sice součástí předkládaného materiálu, ale budou následně předmětem samostatného připomínkového řízení při procesu jejich vydávání. Vaši připomínku bereme na vědomí a doporučujeme ji případně uplatnit v rámci připomínkového řízení k předmětné vyhlášce, aby mohla být řádným způsobem vypořádána. Dále je pravdou, že toto kritérium spadá do kompetencí podnikatelských subjektů, avšak vzhledem ke kritičnosti plnění bezpečnostně významných dodávek bylo toto kritérium zařazeno do seznamu kritérií, přičemž je nutno zmínit, že případné omezení či zákaz nebudou vydávány na základě jednoho kritéria. V těchto případech se kritéria vyhodnocují jako celek. Na základě tohoto vyhodnocení celku pak mohou být podniknuty další kroky, včetně případného omezení, či krajně zákazu, dodavatele. Úřad každopádně považuje otázku schopnosti poskytnout či nikoliv daná plnění za velmi důležitou pro bezpečnostně významné dodávky, směřující do kritické části stanoveného rozsahu.

			Nutno však dodat, že toto se může do samostatného připomínkového řízení změnit.
227. Svaz průmyslu a dopravy ČR	Z	Vyhláška o regulovaných službách - Příloha k vyhlášce č. [bude doplněno] Sb., Kritéria pro identifikaci regulované služby, 7. Výrobní průmysl, Výroba motorových vozidel (kromě motocyklů), přívěsů a návěsů <i>Vypustit „I. poskytovatel regulované služby v režimu vyšších povinností v případě, že sériově vyrábí osobní motorová vozidla,“</i> Aktuální návrh vyhlášky stanovuje pro výrobce motorových vozidel, který vyrábí sériově osobní motorová vozidla režim vyšších povinností dle ZKB. Tím navyšuje požadavky, které vyplývají pro takového výrobce ze směrnice NIS 2. Směrnice NIS 2 totiž výrobce motorových vozidel zařazuje do kategorie důležitých subjektů, tj. ekvivalentu subjektů v režimu nižších povinností. Máme za to, že důležitým aspektem při transpozici směrnic do českého práva je významně se neodlišovat od ostatních členských států EU a nenarušovat tak hospodářskou soutěž v EU. Již nyní je zřejmé, že většina členských států ponechá i ve svých národních právních úpravách výrobu motorových vozidel v nižší kategorii regulovaných subjektů. S ohledem na majetkové i funkční propojení českého automobilového sektoru se zahraničím, zvláště pak Německem, je vysoce žádoucí, aby se ČR v tomto neodchylovala. V případě, že by na výrobce motorových vozidel bylo v České republice kladeno více povinností než v jiných členských státech EU, existuje nezanedbatelné riziko snížení konkurenceschopnosti českých podniků a tím narušení hospodářské soutěže. Jako nejzásadnější rozdíl mezi právní úpravou povinností subjektu ve vyšší a nižší úrovni povinností spatřujeme v povinnosti subjektu ve vyšší úrovni povinností řídit z hlediska bezpečnosti své dodavatele. Taková povinnost bude pro české výrobce motorových vozidel podstatnou zátěží. Vznikla by tak nežádoucí situace, kdy zahraniční dodavatelé nemusí být ochotni plnit zvýšené požadavky, které na ně	Neakceptováno Jak je uvedeno mj. v důvodové zprávě k návrhu vyhlášky o regulovaných službách, sérioví výrobci motorových vozidel jsou stěžejní součástí ekonomiky České republiky, z toho důvodu je logickým zájmem státu, aby jejich činnost nebyla ohrožena kybernetickými incidenty v systémech, které pro své fungování používají. Tento přístup, kdy se stát zaměřuje na ochranu kritických a stěžejních subjektů operujících v jednotlivých odvětvích, je společný pro všechna odvětví, nejde tedy o žádné znevýhodňování velkých a „úspěšných“, ale o podporu toho, aby tyto subjekty poskytovaly své služby i nadále. Zajištění kybernetické bezpečnosti systémů, které organizace používá pro své fungování, by mělo být jedním ze stěžejních zájmů samotné organizace, neboť bez toho může být ohrožena její existence. Zajištění kybernetické bezpečnosti není něco, co by organizace dělala pro stát, dělá to primárně sama pro sebe. Úřadu pisatel neobjasnil, z čeho dovozuje, že „již nyní je zřejmé, že většina členských států ponechá i ve svých národních právních úpravách výrobu motorových vozidel v nižší kategorii regulovaných subjektů“. Naopak dle našich informací většina členských států teprve připravuje návrhy svých transpozičních předpisů. Zesouladění regulace kybernetické bezpečnosti napříč EU je sice základním cílem směrnice NIS 2, nicméně pořád jde o směrnici, nikoli nařízení, pořád je zde tedy prostor pro státy, aby si ty části, kde to směrnice umožňuje, přizpůsobily svým národním potřebám. Z povahy věci je potřeba

		český výrobce motorových vozidel bude muset klást. Finální výrobci by, v případě zařazení do režimu vyšších povinností, velmi pravděpodobně byli nuceni promítnout zvýšené náklady do finální ceny produktu nebo přenést náklady na své dodavatele. NÚKIB uvádí jako odůvodnění pro zařazení výrobců motorových vozidel do režimu vyšších povinností zásadní ekonomický význam společností provozujících sériovou výrobu osobních motorových vozidel pro Českou republiku. Tento argument nerozporujeme, nicméně s odkazem na výše uvedené by implementace vyhlášky v navržené podobě vedla k ohrožení ekonomické činnosti těchto subjektů a přeneseně k ohrožení této podstatné části české ekonomiky. Naopak by měl český zákonodárce velmi pozorně přistupovat k tomu, aby nestanovoval nepřiměřeně přísné požadavky, a bral v potaz nastavení pravidel v dalších členských státech.	počítat s tím, že transpozice směrnice se bude stát od státu lišit a požadavky na regulované subjekty budou v různých státech odlišné. Ačkoli rozumíme volání po harmonizaci české a německé úpravy, primárním zájmem České republiky a cílem činnosti Úřadu je ochrana národních zájmů. Z praxe je nám navíc známo, že německé společnosti (ať již v postavení mateřských společností, nebo zákazníků českých firem) vyžadují poměrně velké množství opatření zajišťujících kvalitu výroby a zavedení systému řízení bezpečnosti informací je poměrně běžnou součástí plnění těchto opatření. Co se týče komentáře ke zvýšené zátěži související s řízením dodavatelů, praxe posledních let ukázala jednoznačnou závislost automobilového odvětví na dodavatelských komponentech. Nelze tedy akceptovat argument, že řízení dodavatelského řetězce je pro podniky působící v sériové výrobě automobilů zatěžující, naopak je to stěžejní část jejich fungování, na kterou musí z podstaty věci klást velký důraz. Kybernetická bezpečnost dodavatelů je přitom součástí řízení celého dodavatelského řetězce, bez spolehlivých dodavatelů a dostatečného smluvního ukotvení dodavatelských vztahů prakticky nelze v odvětví podnikat. Konkrétní podoba řízení bezpečnosti dodavatelů a obecně dodavatelského řetězce pak samozřejmě bude uzpůsobena potřebám odvětví a subjektů samotných, neboť návrh zákona i jeho prováděcí vyhláška o bezpečnostních opatřeních pro vyšší režim jsou založeny na řízení rizik (obdobně i vyhláška o bezpečnostních opatřeních pro nižší režim umožňuje nezavádění těch opatření, která nejsou pro danou společnost relevantní nebo přiměřená). Reakce připomínkového místa:

			Vysvětleno na jednání k vypořádání dne 22. září. S další diskuzí počítáme v rámci samostatného MPŘ k vyhláškám. Připomínkové místo s vypořádáním souhlasí.
228. Svaz průmyslu a dopravy ČR	D	Zákon o kybernetické bezpečnosti - § 45 Evidence vedené Úřadem, odst. 1 Navrhujeme rozšířit výčet o „dodavatele s vysokou mírou bezpečnostního rizika“ Pro zvýšení přehlednosti by bylo dobré mít k dispozici přehlednou evidenci dodavatelů s vysokou mírou rizika.	Vysvětleno – nyní § 48 Dle § 48 odst. 1 písm. c) je jednou z evidencí vedených Úřadem také „<i>evidence dodavatelů bezpečnostně významných dodávek</i>“. Bezpečnostní riziko spojené s konkrétním dodavatelem bude pouze jedním z parametrů v dané evidenci. Upozorňujeme, že tato evidence bude striktně neveřejná a vztahuje se na ni mlčenlivost zaměstnanců dle § 48 odst. 4 návrhu zákona. Přehled dodavatelů u nichž bude uplatněn mechanismus dle § 31 (Omezení rizik spojených s dodavatelem) návrhu zákona, bude samozřejmě dostupný na webu Úřadu. Připomínkové místo s vypořádáním souhlasí.

229. Svaz průmyslu a dopravy ČR	a D	Zákon o kybernetické bezpečnosti - § 4 Režim poskytovatele regulované služby v případě poskytování více regulovaných služeb jedním poskytovatelem Stanovit povinnosti poskytovatele v případě poskytování více regulovaných služeb jedním poskytovatelem odlišně vůči každé jednotlivé regulované službě určené dle kritérií pro identifikaci regulované služby ve vymezených odvětvích nebo kritérii pro určení regulované služby, která vymezují významnost dopadu služby na zabezpečení důležitých společenských nebo ekonomických činností. Na poskytovatele regulovaných služeb mohou být kladeny pouze takové povinnosti, které jsou nezbytné pro zajištění oprávněného veřejného zájmu a jsou tedy proporční k významnosti dopadu dané služby na zabezpečení důležitých společenských nebo ekonomických činností. Považujeme proto za exesivní, aby subjekt provozující více na sobě nezávislých služeb, kdy je dopad pouze jedné ze služeb, např. interpersonální komunikační služby nezávislé na číslech, významný pro zabezpečení důležitých společenských nebo ekonomických činností natolik, že odpovídá vyšší míře povinností, musel plnit vyšší míru povinností vůči všem službám, bez ohledu na jejich vzájemné propojení a nesl tak značné ekonomické náklady s tím spojené. Směrnice (EU) 2022/2555 neukládá členským státům stanovit jediný režim pro poskytovatele více služeb a rozsah řízení kybernetické bezpečnosti poskytovatelem regulované služby dle § 9 je zpravidla logicky navázán na provoz dané služby. Česká implementace v navrhovaném znění by v současné podobě měla zásadní a neodůvodnitelný ekonomický dopad na české subjekty, který by mohl vést k omezení poskytování některých regulovaných služeb, které často nepředstavují hlavní podnikatelskou činnost subjektu (např. interpersonálních komunikační služby nezávislé na číslech, diskuze na obsahových webech resp. sociální sítě apod.).	Neakceptováno V případě této připomínky je nutné vysvětlit způsob fungování režimu vůči fungování zavádění bezpečnostních opatření v rámci daného režimu. Pokud se připomínkové místo obává neúčelného plnění přísnějších povinností nadbytečně i tam, kde to není nutné, je možné v rámci bezpečnostních opatření tento problém řešit plánem zvládání rizik a prohlášením o aplikovatelnosti, což vyhláška o bezpečnostních opatřeních pro vyšší režim požaduje a je to ústřední nástroj pro práci s vyhláškou. Tak jako tak to adresát bude muset udělat, protože v dané situaci alespoň jednu regulovanou službu ve vyšším režimu bude mít. Právě tam může se všemi systémy napříč organizací pracovat účelně. U jiných povinností, např. hlášení incidentů, ustanovení o jednotnosti režimu vynikne ještě více - pokud by v organizaci existovaly různé režimy pro různé regulované služby, bude organizace nákladně udržívat v chodu dva přístupy k bezpečnosti, což je nejen neekonomické, ale také uživatelsky nepřívětivé - právě tento aspekt pak v důsledku snižuje celkovou bezpečnost. Je také potřeba poznamenat, že dle zkušeností z kontrol vykonávaných Úřadem je snaha rozdělovat systémy na jednotlivé služby stejně spíše jen optická - i kdyby pravidlo o jednotnosti režimu nebylo zavedeno, tak pokud se na nějakém aktivu sejde režim vyšších a nižších povinností, bylo by k tomuto aktivu potřeba přistupovat tak, aby splnilo pravidla jak pro vyšší, tak pro nižší režim. To pak ale v praxi znamená, že stejně je podstatná část architektury pod vyšším režimem, protože bývá téměř vždy využívána pro všechny regulované služby společně.

			Připomínkové místo s vypořádáním souhlasí.
230. Svaz průmyslu a dopravy ČR	D	Zákon o kybernetické bezpečnosti § 27 odst. 4) Vyhláška o regulovaných službách § 6 odst. 2) Kritéria pro určení poskytovatele regulované služby, kterému plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce Upravit řízení pro určení poskytovatele regulované služby, kterému plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, v ZKB. Specifikovat o jaký typ řízení se jedná a stanovit přiměřenou lhůtu pro splnění povinností vyplývajících z rozhodnutí, jako nezbytnou součást rozhodnutí. Specifikovat kritéria posuzování „Závažného dopadu na bezpečnost České republiky nebo vnitřní či veřejný pořádek“, a/nebo definovat tyto pojmy v § 2 ZKB. Rozhodnutí NÚKIB ukládající poskytovateli regulované služby plnit povinnosti mechanismu prověřování bezpečnosti dodavatelského řetězce sebou nese pro dotčený subjekt značné náklady. Musí tak být bez pochybností, že se jedná o správní rozhodnutí a dotčenému subjektu jsou dostupné náležité prostředky ochrany svých práv dle správního práva. Vzhledem k tomu, že se jedná o novou pravomoc NÚKIB, bez ustálené rozhodovací praxe, která má zásadní ekonomický dopad na subjekty rozhodnutí, je s ohledem na právní jistotu nezbytné, aby mandatorní součástí rozhodnutí dle zákona byla rovněž přiměřená lhůta pro splnění povinností plynoucích z mechanismu prověřování bezpečnosti dodavatelského řetězce. S ohledem na právní jistotu subjektů je pak také nezbytné specifikovat kritéria pro posuzování závažnosti dopadu na bezpečnost České republiky, resp. její vnitřní či veřejný pořádek, případně tyto pojmy definovat pro účely tohoto zákona v § 2 ZKB.	Akceptováno jinak – nyní § 28 Došlo k rámcové úpravě registrace a určení strategicky významné služby a jejímu vložení do pův. § 28 Kritéria pro identifikaci a určení strategicky významné služby. Poté, co dojde k registraci regulované služby nebo k vydání rozhodnutí o určení strategicky významné služby, NÚKIB označí tuto službu v evidenci a vyrozumí o tom poskytovatele strategicky významné služby. Ten pak bude mít ode dne doručení vyrozumění roční přechodnou lhůtu (došlo ke změně, přechodná lhůta v § 33 odst. 2 byla původně navázána na účinnost zákona). Až na výjimky stanovené v návrhu zákona postupuje NÚKIB podle zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů. Nemohli jsme však vyhovět požadavku na specifikaci kritérií posuzování závažného dopadu na bezpečnost České republiky nebo vnitřní či veřejný pořádek. Jedná se neurčité právní pojmy, které nelze konkrétně definovat a s obdobnými pracuje i řada jiných předpisů (např. zákon č. 365/2000 Sb., o informačních systémech veřejné správy nebo zákon č. 325/1999 Sb., o azylu). Závažnost dopadu bude řádně odůvodněna v konkrétních rozhodnutích NÚKIB. Připomínkové místo s vypořádáním souhlasí.

231. Svaz průmyslu a dopravy ČR	a D	Zákon o kybernetické bezpečnosti § 34 Zajištění dostupnosti strategicky významné služby Návrhy dalších možných řešení nad rámec již uplatněných ve stanovisku s čj. 57/2023 Navrhujeme: a. „Za odstavec 2 vložit nový odstavec 3, a ostatní odstavce přečíslovat. Nový odstavec 3 zní: <i>(3) Odstavce 1 a 2 se neuplatní na kritickou část stanoveného rozsahu strategicky významné služby, kterou je služba cloud computingu, jež byla certifikována v rámci evropského systému certifikace kybernetické bezpečnosti, nestanoví-li zvláštní právní předpis jinak.“</i> b. „Za odstavec 2 vložit nový odstavec 3, a ostatní odstavce přečíslovat. Nový odstavec 3 zní: <i>(3) Odstavce 1 a 2 se neuplatní na kritickou část stanoveného rozsahu strategicky významné služby, kterou je služba cloud computingu, jež byla certifikována v rámci evropského systému certifikace kybernetické bezpečnosti, a jejíž dostupnost je zajištěna z území alespoň dvou členských států, nestanoví-li zvláštní právní předpis jinak.“</i> c. „Za odstavec 2 vložit nový odstavec 3, a ostatní odstavce přečíslovat. Nový odstavec 3 zní: <i>(3) Odstavce 1 a 2 se neuplatní na kritickou část stanoveného rozsahu strategicky významné služby, kterou je služba cloud computingu, jejíž dostupnost je zajištěna z území alespoň dvou členských států, nestanoví-li zvláštní právní předpis jinak.“</i> 3 návrhy úpravy ustanovení § 34 ZKB, které jsou obecné a vztahují se na veškeré služby cloud computingu, bez ohledu na to, jaké strategicky významné služby jsou součástí:	Neakceptováno Připomínkovým místem předložený návrh nesměruje k cíli, s kterým byla úprava reprezentovaná § 35 a souvisejícími navržena. Cílem navrhované úpravy je zajištění dostupnosti strategicky významné služby z území České republiky, tak aby v případě mimořádných událostí (ať již naturogenních nebo antropogenních) bylo možné zajistit dostupnost strategicky významné služby z České republiky, byť v omezeném rozsahu, kvalitě a čase. K variantě a. lze uvést, že není jasné, jak by certifikace měla výše uvedeného cíle dosáhnout, neboť cílem připravované certifikace je něco jiného. Nadto zatím nejsou certifikační schémata schváleny, natož aplikovány. K variantě b. lze uvést to stejné jako k variantě a. Přídavek dostupnosti ze dvou členských států neřeší dostupnost z České republiky. Stejně tak varianta c., která vynechává certifikaci, nicméně neřeší dostupnost z České republiky. Nad rámec toho je nutné uvést, že § 35 směřuje k zajištění strategicky významné služby jako takové (tedy například distribuce elektrické energie), nikoli cloudové služby, která může nějakým způsobem poskytování strategicky významné služby podporovat. Připomínkové místo s vypořádáním souhlasí.

		a. první návrh je navázán na systém evropské certifikace kybernetické bezpečnosti bez návaznosti na konkrétní úroveň záruky b. druhý návrh je nad rámec prvního doplněn tak, že vedle požadavků certifikace musí být zajištěna dostupnost služby cloud computingu alespoň ze dvou členských států, c. třetí návrh je pak omezen tak, že musí být zajištěna dostupnost služby cloud computingu alespoň ze dvou členských států, ale již není vyžadována certifikace. Poslední část ustanovení se vztahuje na zvláštní úpravu vyplývající ze zákona o informačních systémech veřejné správy – ta by se měla vztahovat zejména na poskytování státního cloud computingu.	
232. Notářská komora ČR	Z	Obecně k návrh zákona a k návrhu vyhlášky o regulovaných službách Podle čl. 4 odst. 1 Listiny základních práv a svobod lze povinnosti ukládat toliko na základě zákona. Povinnosti jsou sice návrhem zákonem stanoveny, ale to, jakým subjektům jsou určeny (poskytovatelé regulované služby) a v jakém rozsahu (režim vyšších a nižších povinností), je stanoveno až návrhem prováděcího právního předpisu. Tedy text zákona v § 6 odkazuje při působnosti normy na vyhlášku, která má být podle zákona vydána; obdobně je tomu v § 5 písm. a). Zmocnění v § 6 odst. 3 přitom směřuje toliko ke stanovení režimu poskytovatele regulované služby Domníváme se, že je třeba materiály komplexně upravit tak, aby nedocházelo k ukládání povinností konkrétním subjektům na základě podzákonného právního předpisu.	Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem, jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech [§ 3 a § 2 písm. d)], tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby [§ 3, ve spojení s § 2 písm. i) a k) a § 22a]. Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon [§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)], a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá [§ 3 a § 2 písm. b)]. Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání, a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto

			mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Reakce připomínkového místa: K připomínce č. 232 – stále považujeme režim, stanovený návrhem, za protiústavní (porušení principu „povinnosti lze ukládat toliko na základě zákona“), neboť dochází k ukládání povinností konkrétním subjektům na základě podzákonného právního předpisu. Obstát bez dalšího nemůže argumentace, že v minulosti byl již obdobný přístup zvolen. Reakce NÚKIB Připomínkovému místu byly zaslány upravené části materiálů a bylo doplněno vyjádření k předmětné připomínce. Reakce připomínkového místa Připomínku lze považovat za vypořádanou
233. Notářská komora ČR	Z	K § 29 odst. 4 Domníváme se, že obdobné privilegované postavení jako advokáti (neprolomení povinnosti mlčenlivosti) by mělo být přiznáno také notářům, kteří při výkonu notářské činnosti podle § 2 notářského řádu a další činnosti podle § 3 odst. 1 a 2 notářského řádu provádí odborné právní služby, obdobné výkonu advokacie, a které jsou rovněž kryty povinností mlčenlivosti podle § 56 notářského řádu. K rozdílnému postavení mezi advokáty a notáři není z hlediska neprolomení povinnosti mlčenlivosti žádný věcný důvod.	Akceptováno jinak – nyní § 30 Dotčené ustanovení bylo na základě jiných připomínek přepracováno, obdobně jako u sankčního zákona je prolomení mlčenlivosti v současné době koncipováno tak, že v § 30 odst. 5 jsou vyjmenovány orgány, ve vztahu k nimž se mlčenlivost výslovně prolamuje (orgány činné v trestním řízení, Finanční analytický úřad, správce daně, orgány Celní správy České republiky). V případě potřeby získání jiných informací krytých povinností mlčenlivosti bude přistoupeno k podání žádosti o zproštění povinnosti

			mlčenlivosti. Dále byl doplněn § 30 odst. 6, který od prolomení povinnosti mlčenlivosti odlišuje prolomení bankovního tajemství. Změny týkající se § 30 odst. 5 a 6 byly zrcadlově promítnuty do doprovodného zákona v podobě změn zákonů upravujících činnost orgánů označených v § 30 odst. 5 a 6. Připomínkové místo s vypořádáním souhlasí.
234. Notářská komora ČR	Z	K návrhu vyhlášky o regulovaných službách, k příloze (Kritéria pro identifikaci regulované služby), bodu 1. Veřejná správa Výkon veřejné správy je natolik rozmanitou a komplexní různorodou činností, kdy podle nás nelze obecně ve vyhlášce určit, že „každý“ orgán nebo osoba, který veřejnou moc vykonává (resp. subjekt, který je uveden ve taxativním výčtu v příloze vyhlášky, jenž však fakticky pokrývá v zásadě celé spektrum orgánů veřejné moci) je poskytovatelem regulované služby, která je navíc vymezena pouze zcela obecně jako jedna obecná služba „výkon svěřených pravomocí“. Jedná se tak o zcela obecné kritérium a naprosto striktně formálně (formalisticky) zvolené hledisko, bez zohlednění materiálního přístupu, který by měl brát v potaz povahu a rozsah výkonu veřejné moci u konkrétního subjektu s přihlédnutím k pravděpodobnosti vzniku kybernetického rizika. Domníváme se proto, že např. to, že „profesní komora“ vykonává svěřené pravomoce, by nemělo být jediným kritériem pro to, aby byla poskytovatelem regulované služby (v režimu nižších pravomocí). Domníváme se, že ne všechny činnosti, které Notářská komora ČR vykonává podle zákona č. 358/1992 Sb. jsou činnosti, na které by měla materiálně dopadat požadavky na kybernetickou bezpečnost, tak jak je předpokládá návrh zákona. Naplnění kritérií pro identifikaci regulované služby (kterou by měl provést poskytovatel regulované služby ve smyslu § 8 odst. 1 a 2 návrhu zákona) je tak ryze formálním úkonem, když jediným	Vysvětleno Kritéria pro identifikaci poskytovatele regulované služby musí mít charakter objektivního kritéria, jelikož jsou zákon a vyhlášky postaveny na principu sebeidentifikace – jakýkoliv materiální korektiv by na jedné straně značně redukoval právní jistotu adresátů a na straně druhé nechával prostor k obcházení zaváděné regulace, což se projevilo i v minulé praxi Úřadu. Tato kombinace faktorů pak vede jen k nedůvodným odlišnostem mezi typově shodnými organizacemi. Veřejná správa je specifická, nicméně zvolená varianta taxativního výčtu subjektů a přiřazení relevantního režimu je za nás nejvhodnější a zároveň nejvíce transparentní. Každý orgán veřejné moci bude zpravidla vykonávat jen jednu regulovanou službu a hlásit údaje jen pro tuto službu (výkon svěřených pravomocí) – tím je to pro něj s ohledem na hlášení vůči Úřadu jednodušší. Návrh zákona a navazující prováděcí předpisy jsou postaveny na principu řízení rizik, což povinným subjektům umožňuje přizpůsobit si zavádění bezpečnostních opatření. Není tedy pravda, že by každý subjekt zaváděl vždy veškerá bezpečnostní opatření obsažená v relevantní vyhlášce. Každý

		kritériem je výkon svěřených pravomocí dotyčného orgánu, který bude naplněn z povahy věci vždy. Stejně tak § 12 odst. 3 návrhu zákona předpokládá, že poskytovatel bude povinen nahlásit údaje pro každou regulovanou službu; v daném případě je však služba vždy jen jedna jediná („výkon svěřených pravomocí“). Z komparativního pohledu lze zmínit platnou <u>maďarskou úpravu</u>, implementující NIS2 – zákon o certifikaci kybernetické bezpečnosti a dohledu nad kybernetickou bezpečností (https://net.jogtar.hu/jogszabaly?docid=a2300023.tv), který (s účinností od 1.1.2014) v čl. 17 zákona a jeho příloze uvádí povinné subjekty. V této úpravě není žádná úprava obdobná českému návrhu (tedy obecně „veřejná správa“), tedy ani výslovně „profesní komory“. Právní úpravy z jiných členských zemí EU, implementující NIS2, dosud nejsou známy. Požadujeme důkladnou revizi a úpravu materiálu ve smyslu této zásadní připomínky.	subjekt má povinnost si stanovit, které jeho konkrétní činnosti lze považovat za regulovanou službu výkon svěřených pravomocí (služba je v důvodové zprávě k předmětné vyhlášce dostatečně vysvětlena). Následně identifikuje primární aktiva v organizaci a vybere ta, která potřebuje k výkonu svěřených pravomocí (resp. související s výkonem této služby), čímž si stanoví rozsah řízení kybernetické bezpečnosti. Bezpečnostní opatření včetně identifikace podpůrných aktiv jsou následně zaváděna pouze v tomto stanoveném rozsahu, navíc dochází k postupnému a kontinuálnímu zavádění těchto bezpečnostních opatření. Regulace veřejné správy, resp. výkonu svěřených pravomocí, kontinuálně navazuje na aktuálně účinný zákon o kybernetické bezpečnosti a jeho úpravu veřejné správy, kromě toho jsou subjekty veřejné správy explicitně zmíněny na mnoha místech směrnice NIS2, která s regulací veřejné správy počítá (mj. v čl. 2 odst. 2 písm. f)). Důkladnou revizi či úpravu materiálu tak z výše uvedených důvodů nepovažujeme za nezbytnou. Reakce připomínkového místa: K připomínce č. 234 - stále nepovažujeme za akceptovatelný režim, kdy poskytovatelem regulované služby stanoví v zásadě každý orgán veřejné moci, navíc s naprosto vágně a obecně definovanou službou „výkon svěřených pravomocí“. Tato zcela obecné pojetí je ostatně v příkrém rozporu s pojetím ostatních regulovaných služeb (§ 5 písm. b) až o) vyhlášky o regulovaných službách a příslušné části přílohy), které přesně a konkrétně definují jak jednotlivé služby, tak jejich poskytovatele.

			V připomínce jsme zmínili maďarskou úpravu, implementující NIS2, kde žádná úprava obdobná českému návrhu není, tedy ani obecně „veřejná správa“, ani výslovně „profesní komory“. V mezidobí jsme získali belgickou a německou pracovní podobu implementačního; belgická notářská komora by neměla být zahrnuta do působnosti, v Německu pak ano, ale z toho titulu, že vydává certifikáty (el. podpis). Lze tak shrnout, že žádný z dosud známých evropských návrhů, implementujících NIS2, nemá tak široce definovanou působnost, jako návrh český. Reakce NÚKIB Připomínkovému místu byly zaslány upravené části materiálů a bylo doplněno vyjádření k předmětné připomínce. Reakce připomínkového místa Připomínku lze považovat za vypořádanou
235. Notářská komora ČR	D	K § 19 odst. 1 Pokud chápeme navrhovanou úpravu správně, poskytovatel regulované služby na základě vlastního správního uvážení v zásadě neformálně (bez vydání rozhodnutí ve smyslu správního řádu) určí, zda kybernetický incident oznámí či nikoli uživatelům služby. Doporučujeme dané upřesnit v důvodové zprávě.	Neakceptováno – nyní § 20 odst. 1 V důvodové zprávě k dotčenému ustanovení je výslovně uvedeno, že „poskytovatel regulované služby sám posoudí potřebu oznámit kybernetický bezpečnostní incident s významným dopadem uživatelům napadené regulované služby“. S ohledem na skutečnost, že poskytovateli regulované služby se stanou také osoby, které nelze považovat za správní orgány, není namístě předpokládat, že by návrh zákona pro provozovatele regulované služby, kteří současně jsou správními orgány, stanovil odlišný postup (tj. případnou aplikaci správního uvážení a případné vydání správního rozhodnutí). Není tedy

			potřeba doplňovat důvodovou zprávu požadovaným způsobem. Připomínkové místo s vypořádáním souhlasí.
236. Notářská komora ČR	D	K § 23 odst. 3 věta druhá Doporučujeme v důvodové zprávě doplnit vztah k doručování prostřednictvím datových schránek, kdy při doručování mezi OVM platí fikce doručení okamžikem přijetí zprávy do datové schránky příjemce.	Akceptováno – nyní § 24 odst. 4 Problematika doručování mezi OVM bude v důvodové zprávě explicitně zmíněna. Připomínkové místo s vypořádáním souhlasí.
237. Notářská komora ČR	D	K § 45 odst. 2 Údaje z evidence vedené Úřadem jsou neveřejné a jsou poskytovány podle § 45 odst. 2 v odůvodněných případech. Je zde stanoveno pravidlo, že se údaje poskytnou orgánu veřejné moci, je-li to nezbytné pro výkon jeho působnosti, není však zřejmé, zda budou Úřadem poskytnuty v zásadě kterémukoli OVM na požádání, nebo bude moci Úřad oprávněn údaje odmítnout poskytnout (vydáním rozhodnutí či v režimu neformálního správního uvážení). Doporučujeme dané upřesnit v důvodové zprávě.	Akceptováno – nyní § 48 odst. 2 Podmínkou pro poskytnutí informace je, že orgán veřejné moci tuto informaci potřebuje pro výkon své působnosti. Důvodová zpráva byla upravena. Připomínkové místo s vypořádáním souhlasí.
238. Notářská komora ČR	D	K návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, k § 4 odst. 1 V § 4 odst. 1 slova „§ 4 až 6“ doporučujeme nahradit slovy „§ 4 odst. 2 až 8, § 5, § 6“ <u>Odůvodnění:</u> Text v § 4 odst. 1 zjevně odkazuje na bezpečnostní opatření, která jsou uvedena až v odstavcích 2 až 8.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
239. Vedoucí Úřadu vlády ČR	Z	V § 30 odst. 2 písm. a) a b) (Omezení rizik spojených s dodavatelem) je navrhováno, aby NÚKIB předložil opatření obecné povahy po projednání s orgány uvedenými v § 29 odst. 1 a 2 a s MF Bezpečnostní radě státu (BRS) „pro informaci“ nebo „k projednání“. § 30 odst. 3 pak řeší následný postup NÚKIB při vydávání opatření obecné povahy po informování o něm členů BRS nebo po jeho projednání v BRS. V Důvodové zprávě je pak uvedeno, že „účelem	Neakceptováno – nyní § 31 Bezpečnostní rada státu byla zvolena jakožto orgán, ve které jsou členové vlády zodpovědní za otázky bezpečnosti zastoupeni, jako taková by tedy měla být způsobilá posoudit i závažné a komplexní otázky týkající se bezpečnosti České republiky. Ostatní

		<i>tohoto postupu je zajistit, že je omezení nebo zákaz navrhovaný opatřením obecné povahy proporcionální, tedy že zjištěné ohrožení bezpečnosti je významné natolik, že méně invazivní řešení není pro zajištění bezpečnosti, vnitřního a veřejného pořádku ČR dostačující“.</i> V souladu s čl. 9 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, v platném znění, BRS tvoří předseda vlády a další členové vlády podle rozhodnutí vlády. Tzn. složení BRS neodpovídá složení vlády a je proměnné. S ohledem na zdůvodnění účelu navrhovaného postupu projednání opatření obecné povahy BRS se jeví jako žádoucí, aby o natolik významném zjištění ohrožení bezpečnosti byli informováni, nebo měli možnost se k němu vyjádřit všichni členové vlády, ne pouze členové BRS (strategicky významná služba může být identifikována i v odvětvích, jejichž gestoři nemusí být zastoupeni v BRS).	členové vlády budou o připravovaném opatření obecné povahy informováni prostřednictvím svých ministerstev v případě, že do jejich působnosti opatření zasáhne a budou do jeho přípravy zapojeni; v případě potřeby může samozřejmě BRS ze svého podnětu eskalovat otázku navrhovaného opatření až na vládní úroveň. S tím také plyne procesní stránky věci, kdy Bezpečnostní rada státu může návrh opatření obecné povahy v případě, že je jí předložen, neprojednat, přerušit jeho projednávání, vrátit jej k přepracování, případně s ním vyjádřit nesouhlas. Jakékoliv rozhodnutí je pro Úřad samozřejmě závazné. Předmětné ustanovení bylo nicméně v návaznosti na připomínky k němu dále rozpracováno a upraveno. Připomínkové místo s vypořádáním souhlasí.
240. Vedoucí Úřadu vlády ČR	Z	V Důvodové zprávě k § 30 odst. 2 písm. a) a b) je dále uvedeno, že „<i>po informování BRS, nebo pro projednání návrhu opatření obecné povahy BRS, Úřad zveřejní návrh opatření obecné povahy obvyklým způsobem</i>“. V návrhu zákona nicméně není uvedeno, jak bude výsledek „projednání BRS“ zohledněn v procesu vydávání opatření obecné povahy. V souladu s Jednacím řádem BRS (viz čl. 3) je součástí materiálu předkládaného BRS k projednání návrh usnesení BRS, kterým BRS může projednávaný materiál schválit, vzít na vědomí, přerušit jeho projednávání, vrátit jej k přepracování, případně s ním vyjádřit nesouhlas. Považujeme za nutné v návrhu zákona objasnit, jak by NÚKIB při vydávání opatření obecné povahy (popř. při jeho rušení podle § 30 odst. 4) postupoval v případě nesouhlasu BRS s jeho návrhem.	Akceptováno Do zákona byl doplněn souhlas Bezpečnostní rady státu a jeho význam pro vydávání opatření obecné povahy. Implicitně lze dovodit, že v případě jiné reakce, než souhlasu či vzetí na vědomí Bezpečnostní radou státu, Úřad nebude moci přistoupit k vydání návrhu opatření obecné povahy. Předmětné ustanovení bylo v návaznosti na připomínky k němu dále rozpracováno a upraveno. Připomínkové místo s vypořádáním souhlasí.
241. Vedoucí Úřadu vlády ČR	Z	Podle § 30 odst. 2 NÚKIB předloží opatření obecné povahy BRS po projednání s ostatními orgány uvedenými v § 29 odst. 1 a 2 (tzn.	Akceptováno

		MPO, MZV, MV, Nejvyšší státní zastupitelství, Policie ČR, Úřad pro ochranu hospodářské soutěže, Finanční analytický úřad a zpravodajské služby ČR) a s MF. V souladu s Jednacím řádem BRS (čl. 2, odst. 2) musí být materiál určený k projednání BRS předložen v rámci připomínkového řízení k připomínkám všem členům BRS a vedoucím dotčených ústředních správních úřadů. Návrh opatření obecné povahy, které již bylo projednáno podle § 29 odst. 1 a 2, by tak měl být připomínkován některými ministerstvy dvakrát. Považujeme za nutné tuto skutečnost pro informaci doplnit do Důvodové zprávy k návrhu zákona.	Důvodová zpráva byla doplněna. Připomínkové místo s vypořádáním souhlasí.
242. Vedoucí Úřadu vlády ČR	D	V § 30 odst. 2 je navrženo, že NÚKIB předloží opatření obecné povahy BRS po projednání s ostatními orgány uvedenými v § 29 odst. 1 a 2 a s MF. Doporučujeme zvážit možnost doplnění MF mezi subjekty uvedené v § 29. Dále v této souvislosti upozorňujeme, že ministr financí je členem BRS, a tudíž i připomínkovým místem před předložením materiálu na schůzi BRS.	Vysvětleno MF má v procesu vydávání opatření specifickou roli, jelikož na rozdíl od ostatních orgánů uvedených v § 30 nebude typicky v pozici orgánu posuzujícího bezpečnostní otázky opatření, avšak bude posuzovat soulad opatření se závazky České republiky v oblasti mezinárodní ochrany investic. Pakliže však bude MF disponovat informacemi, které budou pro posouzení předmětné hrozby nezbytné, bude zapojeno také do procesu přípravy opatření postupem dle § 31. Co se týče možné duplikace role MF v procesu, tak tato nebyla shledána jako problematická právě s ohledem na specifické postavení MF v procesu přípravy opatření, kdežto z titulu člena BRS bude ministr financí seznámen až s finálním znění návrhu opatření. Připomínkové místo s vypořádáním souhlasí.
243. Místopředseda vlády pro digitalizaci Úřad vlády České republiky	Z	Obecně k zákonu Chápeme důležitost tohoto návrhu nového zákona a podporujeme značné množství změn. Mimo jiné také z důvodu snah o dobrou a kvalitní koordinaci digitalizace veřejné správy bychom rádi byli přítomni při vypořádávání připomínek k tomuto zákonu.	Akceptováno jinak S připomínkovým místem dohodnut bližší postup. Připomínkové místo s vypořádáním souhlasí.

244. Místopředseda vlády pro digitalizaci Úřad vlády České republiky	Z	Požadavek reflektovat aktuální záležitosti spojené s navyšováním kybernetické bezpečnosti státu K § 54 odst. 6 a k § 67 odst. 1: Požadujeme v návrhu nového zákona o kybernetické bezpečnosti reflektovat aktuální schválené projekty, které mimo jiné sám NÚKIB doporučoval při vedení vládou schváleného záměru BIVOJ. Jednotná státní doména .gov.cz je schválena usnesením vlády ze dne 11. ledna 2023 č. 23. Jednotná státní doména .gov.cz již jako povinnost vyjádřena i v návrhu vyhlášky o dlouhodobém řízení informačních systémů veřejné správy, u které již skončilo MPŘ a připomínková místa již souhlasila se zněním vyhlášky, která zakotvuje mimo jiné i tuto povinnost zavést vybraným orgánům státní správy do 1. 1. 2025 jednotnou státní doménu .gov.cz na webové stránky daných orgánů státní správy. Dále během tohoto léta bude aktualizována Informační koncepce ČR, v jejíž aktualizované podobě je uvedena jednotná státní doména .gov.cz jako princip a jako jeden z cílů. Zároveň bude během tohoto léta schválena povinnost ÚOSS migrovat dle harmonogramu na úrovni usnesení vlády během tohoto léta. Důvodů, proč mají orgány státní správy postupně migrovat na jednotnou státní doménu .gov.cz, je značné množství a byly již uváděny i během pracovních schůzí ÚV ČR MDG – NÚKIB a během mnoha jiných jednání, mimo jiné i na již vytvořené pracovní skupině pro jednotnou doménu .gov.cz pod RVIS. Odůvodnění nutnosti postupné migrace na jednotnou státní doménu .gov.cz jsou přehledně popsány mimo jiné také v příloze <i>Harmonogramu migrace ÚOSS na jednotnou doménu .gov.cz</i> (ve sjednocených pravidel pro státní domény), které můžeme v případě potřeby zaslat. Na okraj si dovolíme upozornit také, že výše uvedené záležitosti, z nichž se nyní dokončují v MPŘ a jsou ve fázi předložení vládě, mohou být oficiálně schváleny vládou během vypořádání připomínek k tomuto zákonu.	Vysvětleno – nyní § 57 a 68 Došlo k vysvětlení v rámci vypořádací schůzky. S připomínkovým místem ale bude dohodnut bližší postup v této věci do budoucna. Současně již nyní došlo k přijetí právní úpravy, která se např. jednotné státní doméně gov.cz věnuje, a posunu projektů do další fáze. Připomínkové místo s vypořádáním souhlasí.

		V textu navrhovaného zákona proto požadujeme přiměřeně na vhodné místa doplnit jednotnou státní doménu .gov.cz. Navrhujeme konkrétně tyto: 1) § 54 odst. 6 na konci za slova „České republiky“ vložit text: „, a to včetně jednotné státní domény .gov.cz“. 2) § 67 odst. 1 za slova „provozu registru internetových domén nejvyšší úrovně“ vložit text: „, včetně jednotné státní domény .gov.cz“. Jsme nicméně otevření případně jednotnou doménu .gov.cz zmínit v zákoně i na jiném vhodně zvoleném místě, pokud předkladatel návrhu zákona takové místo uvede. Jelikož samotný zákon by neukládal žádnou povinnost pracovat na jednotné státní doméně .gov.cz, pouze by ji v našem požadovaném znění zmínil, v důvodové zprávě mohou být reflektovány stručně důvody její existence, jak již bylo z naší strany dříve navrhováno během komunikace před MPŘ (kdy jsme zástupcům NÚKIB již konkrétní podklady pro inspiraci zasílali), v důvodové zprávě na zákonné úrovni nemusí být nijak podrobně rozebírány ostatní souvislosti. S textací důvodové zprávy jsme připraveni případně pomoci v případě potřeby.	
245. Místopředseda vlády pro digitalizaci Úřad vlády České republiky	Z	K § 28 odst. 3 písm. c) ve spojení s § 28 odst. 3 písm. a) NÚKIB uvádí, že „dodavatelem bezpečnostně významné dodávky ten, kdo poskytovateli strategicky významné služby poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku.“ V současné podobě návrhu bude subjektem mechanismu prakticky každý lokální a regionální subjekt, který poskytuje provozovateli „kritické součásti stanoveného rozsahu“ velkoobchodně jakoukoli bezpečnostně významnou dodávku podle § 28 odst. 3 písm. b), což je ale fakticky jakákoli služba, protože NÚKIB definuje aktiva natolik široce, že „kritickou částí stanoveného rozsahu“ je podle návrhu fakticky celá síť poskytovatele sítě či služby elektronických komunikací. Důsledkem toho je, že mechanismus nedopadne jen na subjekty, u kterých to NÚKIB dle důvodové zprávy předpokládá, ale	Neakceptováno – nyní § 29 Ve vztahu k poskytovatelům sítí či službám elektronických komunikací NÚKIB považuje za nutné chránit veškeré funkce veřejné komunikační sítě, které jsou považovány za kritické. Tyto kritické funkce nemusí být nutně vztaženy pouze na jádro sítě, jelikož mnohdy zabezpečují a udržují chod poskytování služeb koncovým uživatelům, a to zejména v rámci rádiové přístupové sítě. Například řízení či monitorovací funkce rádiových stanic představují prostředek, pomocí kterého se koncoví uživatelé připojují právě ke službám poskytovaným jádrem sítě. V případě jejich kompromitace tak může být narušeno či zcela porušeno poskytování služeb koncovým

	na stovky dalších subjektů. Úřad nebere v úvahu fakt, že sektor elektronických komunikací je extrémně propojen řadou dodavatelsko-odběratelských vztahů. Protože mechanismus úřad definuje extrémně široce fakticky jako celou síť, budou regulovanými subjekty i stovky malých a středních regionálních a lokálních operátorů, kteří poskytují velkoobchodní služby velkým národním operátorům. Zjevně jim neposkytují „kritickou“ službu (typicky pronájem vlákna či propoj základnové stanice s nějakým koncentračním bodem), ale přesto budou předmětem tlaku na změnu dodavatele od svých větších obchodních partnerů, protože budou součástí „kritické části stanoveného rozsahu“. To bude mít zásadní vliv na podnikání malých a středních regionálních firem, který není zohledněný v RIA (která má dle obecných zásad pro hodnocení dopadů regulace hodnotit dopad na podnikatelské prostředí „zejména s ohledem na osoby samostatně výdělečně činné a malé a střední podniky“). I z tohoto důvodu požadujeme změnit § 28 odst. 3 písm. a) skutečně jen na kritické části sítě.	uživatelům. Je pravdou, že jádro sítě je nejvýznamnější z hlediska bezpečnosti a integrity sítě a dostupnosti poskytovaných služeb, ale bez zabezpečené rádiové přístupové sítě pozbývá funkční jádro smysl, jelikož nemůže dojít k propojení koncových zařízení s jádrem, což souvisí s nemožností zajistit dostupnost. Obdobný přístup ke kritičnosti sítí, nehledě na jejich umístění v rámci architektury sítě, zvolilo také Dánsko, dále pak v rámci EU Belgie či Finsko. Kritické části sítě jsou omezeny rozsahem zahrnutých aktiv a rozsahem bezpečnostně významných dodávek. Byť by se striktně jazykovým výkladem dalo dovodit, že je možné do kritického rozsahu sítě zahrnout pouze aktiva s dopadem "kritická", nelze tak učinit. Co se týče ochrany aktiv stanoveného rozsahu, u kterých poskytovatel tyto ohodnotil úrovní vysoká (v rámci připomínky se jedná o část "vysoká nebo"), tak zde, na základě předešlých zkušeností a poznání (vyplývajících zejména z kontrolní činnosti NÚKIB), NÚKIB konstatuje, že tato aktiva jsou velmi důležitá až kritická pro fungování strategicky významných služeb. Aktiva ohodnocena jako vysoká mají podstatné dopady na primární aktiva, a tím pádem na chod celé strategicky významné služby. Ochrana pouze kritických aktiv by nebyla v plném rozsahu schopna pokrýt bezpečnost strategicky významné služby v doménách dostupnost, důvěrnost i integrity. Dopady jsou limitovány také rozsahem bezpečnostně významné dodávky, která je omezena jen na takové dodávky, které poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu

			1.technického prostředku nebo vybavení s výpočetní kapacitou, 2.programového prostředku nebo vybavení, nebo 3.informační či komunikační služby. Z toho lze dovodit, že například v připomínce zmíněný pronájem vlákna (bez výpočetní kapacity) do rozsahu nespadne. Co se týče dopadů na regionální a lokální operátory, lze konstatovat, že v případě, že dodávají bezpečnostně významné dodávky do kritické části sítě (tak jak bylo vysvětleno v předchozích odstavcích), je potenciálně možné za naplnění zákonem stanovených podmínek, že jejich odběratelé (tedy poskytovatelé strategicky významných služeb) od nich budou požadovat plnění od takových subdodavatelů, u kterých není riziko, že by jejich dodávky mohli negativně působit na strategicky významnou službu, a tedy i na bezpečnost České republiky. Mechanismus jako takový ovšem na tyto malé a střední podnikatele přímý dopad mít nebude. Po schůzce: V rámci vypořádací schůzky došlo k dovysvětlení dané problematiky a k odsouhlasení návrhu vypořádání ze strany připomínkového místa. Připomínkové místo s vypořádáním souhlasí.
246. Ministerstvo vnitra	Z	K § 2 odst. 2, § 27, § 34 a k Hlavě V, dílu 1: Ministerstvo vnitra společně s Národní agenturou pro komunikační a informační technologie, s. p. (dále jen „NAKIT“) začalo již v roce 2016 budovat Dohledové centrum eGovernmentu, a to jako pracoviště zajišťující bezpečnostní dohled, monitoring,	Neakceptováno – nyní § 2, 28 a 35 V prvé řadě je nutno podotknout, že téma Vládního dohledového centra je mezi MV, NAKIT a NÚKIB diskutováno již poměrně dlouho (nejméně od začátku roku 2023). NÚKIB opakovaně dával předkladateli

	vyhodnocování a reakci na incidenty pro informační systémy eGovernmentu, které v té době byly v gesci Ministerstva vnitra. V průběhu času se podařilo nastavit všechny procesy bezpečnostní části pracoviště i procesy navazující na část provozních dohledů, která v kritických komunikačních systémech Ministerstva vnitra zajišťuje tuto službu v režimu 24/7. Aktuálně tato dvě pracoviště úzce spolupracují a sdílejí i některé společné nástroje. V průběhu let se rovněž pracoviště podařilo stabilizovat personálně a ukotvit ho jako stabilního a perspektivního partnera pro organizace, se kterými má formálně podepsanou a realizovanou spolupráci. Jedná se zejména o bezpečnostní složky státu, ale i akademické a komerční organizace. Tato spolupráce je možná i díky tomu, že všichni zaměstnanci Vládního dohledového centra (dále jen „VDC“) musí mít bezpečnostní prověrku podle zákona č. 412/2005 Sb. (operátoři minimálně stupeň „Vyhrazené“, ostatní pracovníci minimálně stupeň „Důvěrné“). V Akčním plánu k Národní strategii kybernetické bezpečnosti České republiky na období 2021 až 2025 byl Ministerstvu vnitra uložen úkol č. 82: „Zajistit rozvoj dohledového centra e-Governmentu s cílem vytvořit jednotné Vládní dohledové centrum poskytující jednotný monitoring a dohled pro systémy e-Governmentu a další relevantní systémy.“. Tímto úkolem byly rovněž jako spolupracující subjekty pověřeny Ministerstvo obrany, Ministerstvo zahraničních věcí, Národní úřad pro kybernetickou a informační bezpečnost, Úřad vlády a zpravodajské služby. VDC je unikátní pracoviště typu SOC (Security Operations Center) v rámci státní správy, které zajišťuje v režimu 24/7 bezpečnostní monitoring a dohled nad přímo připojenými informačními systémy (dále jen „IS“) a okamžitou eskalaci v případě podezření na bezpečnostní událost nebo incident. U informačních systémů připojených v pasivním módu zajišťuje toto pracoviště pomoc s analýzou dodaných logů a poskytuje zpětnou informaci ke zjištění. V obou případech poskytuje službu řízení bezpečnostního incidentu s vypracováním závěrečné zprávy z řešení incidentu a návrhu dalších opatření. Pokud je informační systém připojen pouze pasivně, dochází rovněž ke vzájemné výměně důležitých	zpětnou vazbu a připomínky k tomu, co v návrhu a celé oblasti týkající se Vládního dohledového centra absentuje. Nutno podotknout, že tyto připomínky a zpětná vazba dosud nebyly uspokojivě vyřešeny a zohledněny. Z nejvýznamnějších nedostatků lze zmínit například to, že dosud nebyly uspokojivě osvětleny služby, které by Vládní dohledové centrum mělo poskytovat, nebyl předložen ani rámcový plán financování takové služby, nebyly definovány kapacity Vládního dohledového centra, nebyly uspokojivě definováni odběratelé služeb, nebyla přeložena analýza toho, kdo a jaké služby by využíval a zda jsou zamýšlení adresáti služeb na toto připraveni. Úroveň přípravy tohoto ustanovení stejně jako procesů navazujících na zavedení takové povinnosti do zákona se nejeví v současné chvíli jako dostatečná. NÚKIB nebyly ani na doprovodných jednáních dodány potřebné podklady, které by dokládaly, že je Vládní dohledové centrum připravené na zavedení do praxe, a není tak možné tyto změny akceptovat a zavést do návrhu zákona v podobě, v jaké byly NÚKIB představeny. Nad rámec výše uvedeného zůstává vůbec otázkou, zda je zákon o kybernetické bezpečnosti tím pravým místem pro toto ustanovení. K úpravě § 27: Neakceptováno. Návrh zákona zná dva způsoby, určení strategicky významné služby. První z nich je samoidentifikační proces, ve kterém poskytovatel regulované služby ve vyšším režimu ověří, jestli naplňuje kritéria i pro to, aby byl strategicky významnou službou. Druhý způsob je pak určení Úřadem v případě, že sezná, že konkrétní poskytovatel regulované služby ve vyšším režimu naplňuje příslušná kritéria. Určení subjektem

	bezpečnostních informací, které mohou přispět k posílení bezpečnosti služeb poskytovaných VDC i bezpečnosti externího informačního systému, který dostává informace od VDC. Tato forma spolupráce, byť nedochází k reálnému monitoringu informačního systému, je velmi důležitá pro preventivní činnost a zabránění případné kompromitaci nebo útoku na informační systém, který není v přímé ochraně VDC, ale informace již je známá a je třeba ji v co nejkratší době z VDC doručit na koncové pracoviště řešící bezpečnostní dohled informačního systému. Stejně důležitý je i opačný proces, kdy informace vznikne mimo VDC a je na VDC doručena ve velmi krátké době kteroukoliv denní i noční hodinu. V tomto jsou pracoviště typu SOC velmi důležitá, protože mají přístup přímo k datům z logování IS, data z logů mohou investigovat přímo nebo i zpětně, a to kdykoliv potřebují, s daty pracují v reálném čase a jsou tak nejbližší k připojené organizaci a jejím datům, mohou přímo ochránit připojenou organizaci a případně i zastavit začínající nebo probíhající útok. Kromě výše uvedených základních služeb poskytuje toto pracoviště i další (doplňkové) služby, které vhodně doplňují mozaiku toho, co je pro organizaci nebo IS důležité a VDC je schopné tuto potřebu díky svým schopnostem a znalostem za určitých podmínek uspokojit. Díky splnění tohoto úkolu tak ve státní správě vzniklo unikátní, robustní bezpečnostní pracoviště, které má silné schopnosti v monitoringu bezpečnosti a detekci událostí a incidentů v reálném čase a je schopno nastartovat řešení incidentu v minimálním čase. Protože se jedná o pracoviště, které už díky své podstatě je připraveno sdílet své kapacity pro více IS a zákazníků, dochází zde k nezbytnému synergickému efektu a okamžité ochraně všech na základě jediné informace jednomu subjektu. Tím, že dochází ke sdílení kapacit mezi všechny připojené organizace, dochází zároveň k obrovským úsporám z rozsahu, protože není nezbytné budovat tyto sdílené schopnosti v každé organizaci, pořizovat HW a SW nezbytný pro vybudování takového specifického pracoviště, shánět odborníky pro toto pracoviště (na pracovním trhu je dlouhodobě nedostatek několika desítek tisíc odborníků na bezpečnost a nedaří se tento problém řešit.	stojícím mimo tyto procesy a mimo režim zákona o kybernetické bezpečnosti je zcela nesystémovým a nevyhovujícím nástrojem. Subjekty, na které by toto „určení“ dopadlo, by byly zbaveny jakékoliv právní ochrany proti takovému kroku (usnesení Bezpečnostní rady státu nelze napadnout opravnými prostředky, které jinak správní řád účastníkům podobných řízení přiznává). Nad to je nutné konstatovat, že požadovaného výsledku (tj. vstupu Bezpečnostní rady státu do procesu určování strategicky významných služeb) lze dosáhnout již v navrhované podobě zákona. Bezpečnostní rada státu může Úřadu usnesením nařídit (a může tak učinit na návrh Výboru kybernetické bezpečnosti) určení konkrétního poskytovatele jako poskytovatele strategicky významné služby, pokud budou naplněny příslušné podmínky. Tím bude dosaženo jako požadovaného vstupu ze strany Bezpečnostní rady státu, tak zachování práv dotčeného poskytovatele. K úpravě § 34: Neakceptováno. Úroveň přípravy tohoto ustanovení stejně jako procesů navazujících na zavedení takové povinnosti do zákona se nejví v současné chvíli jako dostatečné. Úřadu nebyly ani na doprovodných jednáních dostatečně dodány potřebné podklady, které by dokládaly, že je Vládní dohledové centrum připravené na zavedení do praxe, a není tak možné tyto změny akceptovat a zavést do zákona v podobě, v jaké byly Úřadu představeny. K úpravě Hlavy V dílu 1: Neakceptováno. Úroveň přípravy tohoto ustanovení, stejně jako procesů navazujících na zavedení takové povinnosti do zákona, se nejví v současné chvíli jako dostatečné.

	Naopak se jejich nedostatek každým rokem zvyšuje) a řešit otázku finančního ohodnocení těchto drahých odborníků ve státní správě (Ministerstvu vnitra se společně s NAKIT, s. p. podařilo nalézt a odzkoušet fungující model, jak tento problém dlouhodobě a udržitelně vyřešit). Díky všem výše uvedeným bodům lze tak na úrovni státu ročně ušetřit desítky milionů korun za budování a provozování podobných pracovišť, pro jejichž provoz ale nebudou mít dostatek kvalifikovaných odborníků a finančních prostředků, a hrozí zde stav, kdy dojde ke zdání a pocitu bezpečnosti v organizaci, ale díky špatnému fungování a nastavení drahých nástrojů nebude bezpečnost dostatečně a dobře zajištěna a dojde ke kompromitaci s potenciálně až fatálními důsledky. Z výše uvedených důvodů a na základě historie budování dohledového centra na Ministerstvu vnitra a NAKIT, s. p. až do úrovně VDC Ministerstvo vnitra připravilo návrh na legislativní ukotvení tohoto pracoviště jako dalšího prvku zajištění kybernetické bezpečnosti České republiky. Toto pracoviště tak vhodně doplňuje stávající strukturu a organizace, aniž by zasahovalo do jejich rolí a kompetencí. Naopak doplňuje tuto mozaiku o další, doposud nepokrytou schopnost státu, která zde dlouhodobě chyběla a vznikla jako výsledek vládního úkolu v Akčním plánu. Jelikož pro správné a efektivní fungování pracoviště tohoto typu je kritický čas a doba poskytnutí informace a její využití v nástrojích „v první linii“, Ministerstvo vnitra požaduje začlenění Vládního dohledového centra do všech nezbytných evropských struktur, aby došlo k co nejrychlejšímu poskytování bezpečnostně relevantních informací mezi podobnými pracovišti v rámci Evropské unie. Již v současné době, díky využívání nástrojů pro rychlé sdílení informací (např. MISP), je Dohledové centrum eGovernmentu schopno tuto výměnu informací po pracovní úrovni uskutečňovat národně nebo i mezinárodně. O spolupráci s VDC již zároveň, díky zapojení odborníků tohoto pracoviště do různých projektů, programů a pracovních skupin (například TAIEX nebo technologická pracovní skupina pod VKZBP MZV ČR), je velký zájem i z jiných států, se	Úřadu nebyly ani na doprovodných jednáních dostatečně dodány potřebné podklady, které by dokládaly, že je Vládní dohledové centrum připravené na zavedení do praxe a není tak možné tyto změny akceptovat a zavést do zákona v podobě, v jaké byly Úřadu představeny. Připomínkové místo s vypořádáním souhlasí.

		kterými Česká republika navazuje nebo chce navázat úzkou spoluprací. Na základě uvedeného požadujeme: 1. V § 2 na konci odstavce 2 doplnit písmeno l), které zní: <i>„l) Vládním dohledovým centrem bezpečnostní dohledové centrum státu.“.</i> 2. V § 27 doplnit odstavec 3, který zní: <i>„(3) Strategicky významnou službou je dále regulovaná služba stanovená u poskytovatele regulované služby v režimu vyšších povinností rozhodnutím Bezpečnostní rady státu na návrh Výboru kybernetické bezpečnosti v případě, že by narušení bezpečnosti informací regulované služby mohlo způsobit mimořádně závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek.“.</i> 3. V § 34 za odstavec 2 vložit nový odstavec 3, který zní: <i>„(3) Poskytovatel strategicky významné služby podle § 27 odst. 3 je povinen připojit strategicky významné služby v rozsahu kritické části stanoveného rozsahu na Vládní dohledové centrum.“.</i> U stávajících odstavců 3 až 5 pak navrhujeme upravit číslování na 4 a 6. Dále pak ve stávajícím odstavci 3 požadujeme za slova <i>„podle § 27 odst. 2“</i> doplnit slova <i>„a 3.“</i>. 4. V Hlavě V, dílu 1 požadujeme doplnit § 44, který zní: <i>„§ 44</i> <i>Provozovatel Vládního dohledového centra</i> <i>(1) Provozovatelem Vládního dohledového centra je Ministerstvo vnitra.</i> <i>(2) Provozovatel Vládního dohledového centra poskytuje služby Vládního dohledového centra a provádí následující činnosti:</i> <i>a) provozuje komunikační a kontaktní centrum pro zajištění svých služeb,</i>	

		b) provádí bezpečnostní monitoring, detekci, analýzu a klasifikaci kybernetických bezpečnostních událostí a incidentů, c) zajišťuje a koordinuje okamžitou reakci na kybernetické bezpečnostní incidenty, d) provádí hledání hrozeb v kybernetickém prostoru, e) připravuje návrhy preventivních i následných opatření v reakci na hrozby nebo řešení kybernetických bezpečnostních incidentů, f) poskytuje bezpečnostní zpravodajství, g) poskytuje podporu pro manažera kybernetické bezpečnosti, h) podílí se na výzkumu a vývoji kybernetických bezpečnostních nástrojů a řešení, i) spolupracuje s orgány a osobami působícími v oblasti kybernetické bezpečnosti, j) plní roli CSIRT týmu podle příslušného předpisu Evropské unie a podílí se na fungování mezinárodních uskupení v oblasti kybernetické bezpečnosti, včetně Sítě CSIRT, k) prioritizuje poskytování svých služeb a výkon svých činností podle přístupu založeného na rizicích, dostupných kapacitách a parametrech poskytovaných služeb. (3) Provozovatel Vládního dohledového centra může poskytovat i další služby související se zajištěním kybernetické bezpečnosti.“.	
247. Ministerstvo vnitra	Z	K § 16 odst. 4: Lhůtu 1 roku považujeme za nepřiměřeně dlouhou s ohledem na možnou rychlost napadení a rozsah dopadů, a proto ji navrhuje zkrátit.	Vysvětleno Lhůta koresponduje se lhůtou podle dosavadní právní úpravy a je nastavena takovým způsobem, aby měl poskytovatel regulované služby dostatečný časový prostor pro stanovení rozsahu (§ 13), na který se povinnost hlášení incidentů vztahuje. Lhůta je stanovena jako maximální možné časové období, ve kterém musí poskytovatel regulované služby začít povinnost plnit, nic tak nebrání v hlášení incidentů

			okamžitě po zápisu do evidence. Vedle toho je v § 16 odst. 5 zakotvena možnost hlásit incidenty ze strany jakéhokoliv subjektu na dobrovolné bázi bez omezení. Připomínkové místo s vypořádáním souhlasí.
248. Ministerstvo vnitra	Z	K § 17 odst. 3: Ustanovení § 16 návrhu stanoví povinnost hlášení kybernetických bezpečnostních incidentů v režimu vyšších povinností Národnímu úřadu pro kybernetickou a informační bezpečnost (dále také jen „Úřad“). V návrhu zákona však zcela chybí povinnost Úřadu informovat orgány činné v trestním řízení, které mohou predikovat, že kybernetický bezpečnostní incident je z 95 % trestným činem (na rozdíl od kybernetické bezpečnostní události). S ohledem na zkušenosti v této oblasti považujeme za vhodné, aby Úřad měl v zákoně taktéž zakotvenou povinnost vyplývající z § 8 trestního řádu. Tuto povinnost považujeme za zásadní, neboť jen tak bude možné zahajovat včas úkony trestního řízení a zároveň provádět zajišťovací úkony tak, aby bylo možné procesovat další úklony (například evropský vyšetřovací příkaz). V minulosti se staly případy, kdy Úřad byl informován, ale orgány činné v trestním řízení se o kybernetickém útoku dozvěděly z médií či jiných zdrojů, tedy dodatečně a s časovým odstupem. Dle našeho názoru se touto úpravou odstraní stálá diskuze, jak dalece chránit práva oznamovatelů trestné činnosti v rámci kybernetického prostoru. Jelikož jsou v návrhu zákona široce upravovány povinnosti subjektů provozující regulované služby, a to včetně stanovených sankcí, je vhodné zajistit i další přenos informací tak, aby v rámci naplnění účelu předmětného zákona byl reálně zahájen proces zajištění vnitřní bezpečnosti (tedy zahájení prověřování či vyšetřování trestného činu). Zde se lze odkázat na § 5 návrhu, ve kterém jsou uvedeny dopady, které jednoznačně představují předmět zájmu orgánů činných v trestním řízení, tedy dopad na veřejnou bezpečnost nebo veřejné zdraví, přeshraniční dopady kybernetického bezpečnostního incidentu a zejména ohrožení	Neakceptováno V § 8 odst. 1 větě druhé zákona č. 141/1961 Sb., trestního řádu, v účinném znění, je stanoveno, že státní orgány jsou povinny neprodleně oznamovat státnímu zástupci nebo policejním orgánům skutečnosti nasvědčující tomu, že byl spáchán trestný čin. Uvedená povinnost je dostatečně srozumitelná, není tedy nutné ani účelné doplňovat ji zvláštním ustanovením v návrhu zákona. Připomínkové místo s vypořádáním souhlasí.

		života a zdraví, majetkových hodnot nebo životního prostředí. Jedině orgán činný v trestním řízení má oprávnění konat dle trestního řádu či zákona o mezinárodní justiční spolupráci ve věcech trestních a Úřad je v této souvislosti pouze v postavení správního orgánu. Urychlené informování orgánu činného v trestním řízení je jedním ze základních principů rychlé reakce v rámci řešení kybernetického bezpečnostního incidentu a při zajišťování stop a důkazních prostředků. Návrh zákona dále uvádí, že úřad předává bez zbytečného odkladu informace o kybernetickém bezpečnostním incidentu s významným dopadem, které se týkají dvou nebo více členských států, dotčeným členským státům a Agentuře Evropské unie pro kybernetickou bezpečnost [§ 41 odst. 5 písm. k)], čímž se paradoxně může stát, že část Evropy bude mít informace ke kybernetickému útoku na citlivý systém v České republice (a na systémy dotčených států), ale orgány činné v trestním řízení České republiky tuto informaci neobdrží včas, aby mohly koordinovat úkony trestního řízení (např. v oblasti urychleného uchování dat na zahraničních útočících serverech). Zároveň je Úřad povinen předávat informace o oznámených kybernetických incidentech Agentuře Evropské unie pro kybernetickou bezpečnost (byť v anonymizované formě), tudíž považujeme za logické, že o incidentech by měly být informovány i orgány činné v trestním řízení na národní úrovni. Na základě uvedeného požadujeme na konci textu § 17 odst. 3 písm. a) doplnit slova „, přičemž Úřad nebo Národní CERT bez zbytečného odkladu oznámení postoupí orgánům činným v trestním řízení k prověření podezření ze spáchání trestného činu“.	
249. Ministerstvo vnitra	Z	K § 28 odst. 1: 1. Máme za to, že na základě § 28 odst. 1 návrhu zákona se Úřad de facto staví do pozice zpravodajské služby, neboť může shromažďovat informace a data ke kterékoliv osobě či společnosti, které by se týkala možná hrozba pro bezpečnost České republiky, vnitřní či veřejný pořádek. Úřad je primárně správním orgánem a má vyhodnocovat konkrétní rizika, která	Ad 1: Neakceptováno – nyní § 29 odst. 1 NÚKIB shromažďuje a vyhodnocuje informace primárně za účelem zajištění fungování mechanismu bezpečnosti dodavatelského řetězce. Z povahy činnosti správních orgánů však nelze vyloučit, že získané informace budou využity i při dalších činnostech NÚKIB nebo jiných orgánů veřejné moci. Bylo by v rozporu se základními zásadami činnosti

		mohou nastat v rámci dodávky technologie, jež by mohla poškodit zájmy České republiky. Na základě uvedeného navrhuje text § 28 odst. 1 upravit takto: „<i>Úřad shromažďuje a vyhodnocuje informace a data spojené s orgánem či osobou, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo v rámci prověřování kritérií rizikovosti dodavatele.</i>“. 2. Slovní spojení „<i>orgánem nebo osobou</i>“ navrhuje upřesnit. Doporučujeme například zavedení legislativní zkratky, neboť se toto slovní spojení objevuje též na dalších místech návrhu (např. § 56 odstavec 1, § 63 odstavec 2 atd.) a působí jako legislativní zkratka, která však v návrhu zavedena není, a není tak zřejmé, o jaké orgány se jedná.	správních orgánů, pokud by NÚKIB tyto informace nepředal, respektive nevyužil při výkonu ostatních pravomocí. NÚKIB však garantuje, že v žádostech o součinnost podle § 29 odst. 1 až 3 bude postupovat v souladu s principem proporcionality. Tento soulad bude kontrolován i dotazovanými orgány a osobami, které řádně neodůvodněné žádosti nemusí vyhovět. Je vhodné doplnit, že žádosti o součinnost podle § 29 odst. 1 až 3 se nijak neliší od obdobných institutů zákona. Konečně podle našeho názoru úprava § 29 odst. 1 navrhovaná Ministerstvem vnitra nijak nezužuje rozsah informací nebo pravomoci NÚKIB. Jedná se pouze o přeformulování návrhu NÚKIB. Reakce připomínkového místa Připomínkové místo s vypořádáním nesouhlasí. Reakce NÚKIB Připomínkovému místo bylo zasláno doplnění vyjádření a upravený návrh § 29. Reakce připomínkového místa Připomínkové místo považuje provedené úpravy za dostatečné a s návrhem vypořádání souhlasí. Připomínkové místo s vypořádáním souhlasí. Ad 2: Akceptováno jinak. Do § 2 odst. 2 bylo doplněno vymezení pojmu "orgán". Pojem "osoba" již právní řád zná a jedná se samozřejmě o právnickou nebo fyzickou osobu. Připomínkové místo s vypořádáním souhlasí.
250. Ministerstvo vnitra	Z	K § 29 odst. 2:	Akceptováno – nyní § 30 odst. 2

	Podle § 29 odst. 2 návrhu má mj. policie povinnost poskytnout Úřadu na jeho žádost za účelem výkonu činnosti podle § 28 odst. 1 informace nebo jinou součinnost, a to bez zbytečného odkladu, nejpozději však do 30 dnů. Z důvodové zprávy k návrhu zákona vyplývá, že se bude jednat především o poskytnutí informací, kterými policie již disponuje, nicméně není vyloučena ani možnost aktivního zjišťování potřebných informací. Stejná povinnost je uvedeným ustanovením stanovena mimo jiné i zpravodajským službám České republiky, avšak podle § 69 odst. 3 návrhu zákona pouze za předpokladu, že tomu nebrání zvláštní předpis (např. zákon o zpravodajských službách) nebo zákonná či státem uznaná povinnost mlčenlivosti. Při poskytování informací nebo součinnosti podle § 29 odst. 2 rovněž není dotčena povinnost mlčenlivosti advokáta podle právního předpisu upravujícího výkon advokacie (viz odstavec 4). Dle našeho názoru, vyhovění žádosti podle § 29 odst. 2 návrhu by v rámci činnosti policie, v určitých případech, mohlo ohrozit či zmařit účel trestního řízení. Zajišťování kybernetické bezpečnosti České republiky je nepochybně ve společenském zájmu, ale stejně tak je tomu i u trestního řízení, potažmo stíhání trestních činů. Nehledě na skutečnost, že u řady vedených trestních řízení si výhradní právo na poskytování informací vyhrazuje sám dozorující státní zástupce podle § 8a odst. 3 trestního řádu, a tedy policejní orgán je oprávněn poskytovat informace jen po jeho předchozím souhlasu. Dle našeho názoru je zde patrný nesoulad v možnosti odmítnutí součinnosti dle jiných právních předpisů u policie, tak jak je to umožněno zpravodajským službám. Navrhujeme, aby byla do návrhu včleněna možnost, aby policie mohla posoudit, zda vyhovění požadavku Úřadu nemůže ohrozit či zmařit účel trestního řízení, a v takových případech mu nevyhovět, vyhovět pouze v omezeném rozsahu nebo požadavku Úřadu vyhovět v jiné lhůtě, než se kterou kalkuluje návrh zákona. V úvahu připadá například situace, kdy policie, ačkoli byla požádána o součinnost Úřadem, nejprve zajistí věci důležité pro trestní řízení a eventuálně provede další nezbytné úkony a poté vyhoví požadavku	Došlo k úpravě znění § 30, úprava požadovaná vznesenou připomínkou byla zohledněna v §30 odst. 5 písm. a). (1) Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí a Ministerstvo vnitra za účelem výkonu činnosti podle § 29 odst. 1 poskytnou Úřadu na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů ode dne obdržení žádosti, stanovisko o naplnění kritéria rizikovosti dodavatele konkrétním orgánem či osobou nebo požadované informace. (2) Nejvyšší státní zastupitelství, Policie České republiky, Úřad pro ochranu hospodářské soutěže a zpravodajské služby České republiky za účelem výkonu činnosti podle § 29 odst. 1 poskytnou Úřadu na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů ode dne obdržení žádosti, požadované informace. (3) Finanční analytický úřad za účelem výkonu činnosti podle § 29 odst. 1 poskytne Úřadu na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů ode dne obdržení žádosti, požadované informace, které získal při své činnosti podle zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. (4) Nezíská-li Úřad z vlastní činnosti nebo postupem podle odstavce 1 a 2 informace potřebné pro výkon činnosti podle § 29 odst. 1, poskytnou na základě žádosti Úřadu tyto informace orgány a osoby neuvedené v odstavci 1 a 2 a to do 30 dnů ode dne obdržení žádosti.

		úřadu, a to v případě, že by opačný postup mohl ohrozit či zmařit účel trestního řízení. Vzhledem k tomu, že § 29 odst. 2 návrhu se týká i Nejvyššího státního zastupitelství, navrhujeme zvážit rozšíření této možnosti i na uvedené státní zastupitelství. Na základě uvedeného navrhujeme v § 29 doplnit odstavec 5, který zní: <i>„(5) Pokud by vyhověním žádosti Úřadu podle odstavce 2 došlo k ohrožení či zmaření účelu trestního řízení, Policie České republiky ji nevyhoví, vyhoví pouze částečně, nebo poskytnutí informace nebo jiné součinnosti na nezbytně nutnou dobu odloží.“.</i>	(5) Při poskytování informací podle tohoto ustanovení není porušením povinnosti mlčenlivosti poskytnutí informace a) orgánem činným v trestním řízení, ledaže by poskytnutí informace, na kterou se mlčenlivost vztahuje, zmařilo účel trestního řízení, b) Finančně analytickým úřadem, c) správcem daně podle daňového řádu, d) orgánem Celní správy České republiky. (6) Při poskytování informací podle tohoto ustanovení není porušením bankovního tajemství poskytnutí informace bankou. Zároveň s úpravou § 30 budou také upraveny související zvláštní zákony v doprovodném zákoně. Připomínkové místo s vypořádáním souhlasí.
251. Ministerstvo vnitra	Z	K § 30 odst. 1: Navrhujeme slova „významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku“ nahradit slovy „významné ohrožení bezpečnosti České republiky, vnitřního či veřejného pořádku nebo kritické infrastruktury“. Pojem kritická infrastruktura, jak je definován v zákoně o krizovém řízení („prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení, jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu“) vhodně rozšiřuje hodnoty, které by měly být na základě § 30 a následujících ustanovení chráněny.	Neakceptováno – nyní § 31 odst. 1 Návrh mechanismu bezpečnosti dodavatelského řetězce zcela záměrně nepracuje s pojmem „kritická infrastruktura“ (stejně tak bylo upuštěno od pojmu „kritická informační infrastruktura“ v celém návrhu zákona), který je širší, než zamýšlený dopad mechanismu. NÚKIB se však domnívá, že mechanismus ve svém návrhu pojímá všechny strategicky významné služby, u kterých je to žádoucí. Nelze také vyloučit, že poskytovatelé strategicky významné služby budou zároveň provozovateli prvků kritické infrastruktury. Připomínkové místo s vypořádáním souhlasí.

252. Ministerstvo vnitra	Z	K § 30 odst. 2 a 3: Požadujeme upravit mechanismus projednání opatření obecné povahy tak, že návrh opatření obecné povahy bude předkládám v navrhovaném režimu (pro informaci/k projednání dle současného rozdělení) vládě České republiky, a nikoliv Bezpečnostní radě státu. Nepovažujeme za vhodné zavádět mechanismus projednání návrhu opatření patření obecné povahy ze strany Bezpečnostní rady státu. Bezpečnostní rada státu se návrhy opatření obecné povahy zpravidla nezabývá a pravidelně se schází pouze s frekvencí přibližně 6x ročně. Oproti tomu se vláda schází každý týden a návrhy opatření obecné povahy projednává (viz např. § 11 odst. 1 zákona o ochraně státních hranic České republiky). Pokud by projednání opatření obecné povahy mělo čekat na běžné jednání Bezpečnostní rady státu, může dojít k jeho významnému zpoždění. Pokud by kvůli projednání opatření obecné povahy mělo být svoláno mimořádné jednání Bezpečnostní rady státu, je tento postup zbytečně administrativně náročný pro všechny zapojené subjekty. Zároveň považujeme vládu České republiky za vhodnější fórum pro posouzení takto závažného rozhodnutí.	Neakceptováno – nyní § 31 odst. 2 a 3 Bezpečnostní rada státu byla vyhodnocena jako orgán, který je pro potřeby mechanismu projednání návrhu opatření obecné povahy nejvhodnější, jelikož jeho členové jsou relevantní pro posuzování národních bezpečnostních otázek, a to včetně těch, které se týkají kyberbezpečnosti. V Bezpečnostní radě státu jsou zastoupeni členové vlády a v případě potřeby může být záležitost přenesena až na úroveň vlády. Bezpečnostní rada státu může také s ohledem na její jednací řád návrh opatření obecné povahy, pokud jí bude předložen k projednání, například vrátit k přepracování, vyjádřit s ním nesouhlas nebo jeho projednávání přerušit. Výsledek projednání Bezpečnostní radou státu je pak pro Úřad závazný. Reakce připomínkového místa Ministerstvo vnitra na připomínce v tuto chvíli trvá, a to do sdělení výsledku jednání k vypořádání připomínky č. 252 mezi NÚKIB a ÚV. Reakce NÚKIB Připomínkovému místu bylo zasláno doplnění vyjádření a upravený návrh § 31. Reakce připomínkového místa Připomínkové místo považuje provedené úpravy za nedostatečné a s návrhem vypořádání nesouhlasí. Závěr vypořádání Ačkoliv stále preferujeme, aby takto klíčové rozhodnutí činila vláda ČR, akceptujeme zasláný návrh a naši zásadní připomínku č. 252 považujeme za vypořádanou.

			Připomínka vypořádána.
253. Ministerstvo vnitra	Z	K § 30 odst. 4: Navrhujeme lhůtu pro přezkum prodloužit ze 3 na 4 roky. Lze předpokládat zvýšenou zátěž všech zainteresovaných subjektů, zejména na začátku a konci daného období.	Akceptováno – nyní § 31 odst. 4 Navrhovaná změna byla zapracována do návrhu zákona. Současně uvádíme, že Úřad v okamžiku, kdy zjistí rozhodné skutečnosti pro zrušení opatření obecné povahy, uplatní instituty, které mu umožní opatření obecné povahy zrušit, a to bez ohledu na běh lhůty pro pravidelné přezkoumání. Připomínkové místo s vypořádáním souhlasí.
254. Ministerstvo vnitra	Z	K § 31: Požadujeme doplnit odstavce 5, který zní: <i>„(5) Žádost podle odstavce 2 lze znovu podat nejdříve po uplynutí 2 let od právní moci rozhodnutí o zamítnutí žádosti o poskytnutí výjimky.“.</i> Návrhem se minimalizuje riziko zahlcení úřadu a součinnostních subjektů.	Akceptováno jinak – nyní § 32 Uvedený návrh byl přidán do zákona se změnou na "pokud nastane podstatná změna okolností". Připomínkové místo s vypořádáním souhlasí.
255. Ministerstvo vnitra	Z	K § 38: Domníváme se, že je nezbytné jasně vymezit vztah mezi stavem kybernetického nebezpečí a krizovými stavy tak, aby nedocházelo k nejasnostem v kompetencích při samotném řešení události či incidentu. Je tedy třeba zohlednit skutečnost, že stav kybernetického nebezpečí se bude využívat pro řešení událostí, jejichž rozsah nemá takovou intenzitu, aby bylo třeba vyhlášovat krizový stav (k vyhlášení nouzového stavu se přistupuje až v případě, kdy není možné vzniklé ohrožení odvrátit v rámci stavu kybernetického nebezpečí). Současné znění však stav kybernetického nebezpečí užitými slovními spojeními (zachování ústavnosti, svrchovanosti a územní celistvosti) staví téměř na roveň stavu ohrožení státu. Navrhujeme text § 38 upravit následovně:	Akceptováno jinak – nyní § 39 Souhlasíme s připomínkou gestora problematiky krizových stavů na tom, že smyslem stavu kybernetického nebezpečí je nestavět jej na roveň krizových stavů, ale jako nástroj k řešení ohrožení nebo narušení bezpečnosti informací v kyberprostoru. Z toho důvodu akceptujeme navrženou změnu, jen s ohledem na pojmy zavedené již výše v návrhu a další drobné jazykové úpravy navrhujeme mírně odlišné znění původně navrhovaného ustanovení. Připomínkové místo s vypořádáním souhlasí.

		„§ 38 Stav kybernetického nebezpečí <i>Stav kybernetického nebezpečí lze vyhlásit v případě, kdy je značně ohrožena nebo narušena bezpečnost, dostupnost nebo integrity informací v kybernetickém prostoru, což může mít za následek negativní dopady na poskytování regulovaných služeb nebo zachování hospodářských činností, bezpečnosti, veřejného zdraví nebo životního prostředí, a nebyl pro řešení této situace vyhlášen nouzový stav, nebo stav ohrožení státu.“.</i>	
256. Ministerstvo vnitra	Z	K § 39 odst. 1: Návrh zásadně prodlužuje časového období, na které je možné vyhlásit stav kybernetického nebezpečí. Dle současné úpravy (§ 21 odst. 3) lze vyhlásit stav kybernetického nebezpečí nejvýše na 7 dnů. Uvedenou dobu může ředitel Úřadu prodloužit, ale souhrnná doba trvání vyhlášeného stavu kybernetického nebezpečí nesmí být delší než 30 dnů. Aktuálně je navrhováno toto časové období prodloužit až na 30 dnů s možností prodloužení se souhlasem vlády na v podstatě neomezenou dobu. Fakticky se tak jedná o přiblížení úpravy krizovým stavům v krizovém zákoně, s čímž je v zásadě možné souhlasit. Požadujeme však v důvodové zprávě dostatečně zdůvodnit, čím je tato změna opodstatněna, zejména s ohledem na nově definovaná opatření ředitele Úřadu uvedená v § 40.	Akceptováno – nyní § 40 odst. 1 Toto ustanovení bylo na základě našich společných jednání upraveno tak, že samostatně může stav kybernetického nebezpečí trvat pouze po dobu maximálně 60 dní. Připomínkové místo s vypořádáním souhlasí.
257. Ministerstvo vnitra	Z	K § 39 odst. 4: Krizovými opatřeními mohou být pouze taková opatření, která jsou přímo uvedena v zákoně č. 240/2000 Sb., o krizovém řízení, ve znění pozdějších předpisů, konkrétně v § 6, § 7 a § 14. Nelze za ně tak považovat opatření, která byla vyhlášována za stavu kybernetického nebezpečí podle zákona o kybernetické bezpečnosti. Zároveň nepovažujeme za žádoucí „mechanicky ukončovat“ platnost opatření (vyhlášených ředitelem Úřadu za stavu kybernetického	Akceptováno jinak – nyní § 40 odst. 4 Dle společné dohody bylo dotčené ustanovení komplexně přepracováno. Nově je možné, aby stav kybernetického nebezpečí fungoval i vedle vládou nařízeného krizového stavu. V rámci stále platného stavu kybernetického nebezpečí tak mohou zůstat v

		nebezpečí) vyhlášením nouzového stavu. Jedná se o „specifická“ opatření, která mohou být v platnosti i za krizových stavů, případně i po jejich skončení – viz opatření u jiných specifických stavů (opatření povodňových komisí, mimořádná veterinární opatření apod.). Navrhujeme z § 39 odstavec 4 poslední větu vypustit.	účinnosti i opatření v něm navržená, tedy se z nich nestávají opatření krizová. Připomínkové místo s vypořádáním souhlasí.
258. Ministerstvo vnitra	Z	K § 40 odst. 1: V § 40 je třeba rozlišovat intenzitu zásahu do práv soukromých subjektů a rozlišovat tak mezi opatřeními, která je oprávněn vyhlášovat ředitel Úřadu, a těmi, která vyhláší vláda jako krizová opatření. Intenzita navržených opatření překračuje účel stavu kybernetického nebezpečí a svým rozsahem se dostává do roviny krizových opatření. 1. V odstavci 1 písm. a) je stanoveno, že „<i>Ředitel Úřadu je v době stavu kybernetického nebezpečí za účelem jeho řešení oprávněn poskytnout věcné prostředky v majetku České republiky, které má v užívání Úřad, a které jsou nezbytné k řešení kybernetického bezpečnostního incidentu, nebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem.</i>“. Požadujeme upravit ustanovení tak, aby jednoznačně směřovalo k poskytnutí věcných prostředků pouze osobám, které se podílejí na řešení kybernetického bezpečnostního incidentu či zabezpečení aktiv apod. Zákon nedefinuje, komu může ředitel Úřadu prostředky poskytnout, což nepovažujeme za vhodné. Lze doporučit alespoň obecné vymezení okruhu osob, např. poskytovatel regulované služby, jeho dodavatel, osoba postižená bezpečnostním incidentem, osoby, které se podílejí na řešení kybernetického bezpečnostního incidentu nebo zabezpečení aktiv. Na navrženém vymezení osob doslovně netrváme, lze zvolit i jinou množinu oprávněných osob. 2. V odstavci 1 písm. a) je rovněž nezbytné blíže specifikovat nakládání s těmito prostředky (zda se vrací, zda jde o užití za náhradu apod.). Příkladem může být nakládání s	Ad 1: Akceptováno – nyní § 41 odst. 1 Ustanovení bylo komplexně přepracováno po společných jednáních. Konkrétní namítané ustanovení bylo rovněž upraveno tak, aby bylo zřejmé, komu se věcné prostředky poskytují. Ad 2: Akceptováno Ustanovení bylo komplexně přepracováno po společných jednáních, došlo k doplnění postupu k navrácení nespotřebovaných věcných prostředků po skončení stavu kybernetického nebezpečí. Ad 3: Akceptováno Ustanovení bylo odstraněno. Ad 4: Akceptováno Ad 5: Akceptováno Ad 6: Vysvětleno Zpřístupněním neveřejné sítě v tomto případě není mířeno na její primární užívání Úřadem, nicméně jen jako užívání podpůrné, které bude zpravidla zahrnovat pouze posílání informací, a to v případě, že takové informace nebude možné doručit dostatečně rychlým způsobem jinak. Prakticky se tak nemusí stát, aby Úřad měl do takové sítě přístup, nicméně postačí aby mu byla zpřístupněna zprostředkovaně, případně pokud bude zpřístupněna pouze ta část sítě, která je nezbytná k řešení značného ohrožení nebo narušení

		pohotovostními zásobami podle zákona č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy. 3. Opatření uvedené v odstavci 1 písm. b) je příliš široké, neboť umožňuje Úřadu vyžadovat téměř jakékoliv informace od kohokoliv, a je tak žádoucí jeho konkretizace ve vztahu k řešení kybernetického incidentu, případně ve vztahu k ostatním opatřením, která lze za stavu kybernetického nebezpečí vyhlásit. 4. U opatření v odstavci 1 písm. c) je nutné doplnit normativní text o možnost odmítnutí poskytnutí personálních kapacit nebo věcných prostředků z objektivních příčin (například zdravotní indispozice). 5. V případě opatření podle odstavce 1 písm. d) chybí upřesnění, co se rozumí prací v pohotovostním režimu a komu je ředitel Úřadu práci v tomto režimu oprávněn nařídít. Požadujeme tedy tento termín upravit tak, aby odpovídal již existujícím institutům a vhodně na jejich úpravu v jiném zákoně odkazoval, případně zavést v zákoně jeho jednoznačnou definici, pokud se má jednat o nový institut. Zákoník práce upravuje v § 95 pracovní pohotovost. Dále zákon o krizovém řízení zná pracovní povinnost a pracovní výpomoc [§ 2 písm. d) a e)], které nařizuje vláda, respektive hejtman [§ 6 odst. 1 písm. c), § 14 odst. 4 písm. a)]. Žádný z těchto zákonů však nezná pojem „<i>pohotovostní režim</i>“, tento pojem není upřesněn ani v důvodové zprávě. Domníváme se, že se jedná o nepřesné pojmenování jednoho z výše uvedených režimů. 6. U opatření v odstavci 1 písm. h) chybí upřesnění, o jaké neveřejné komunikační síť se jedná. Pokud by mělo jít i o komunikační síť provozované Ministerstvem vnitra pro potřeby integrovaného záchranného systému, za účelem zamezení ohrožení činnosti složek integrovaného záchranného systému by měla pro tento případ být v zákoně uvedena výjimka. Navrhujeme ustanovení upravit v souladu s uvedeným.	bezpečnosti informací v kybernetickém prostoru za stavu kybernetického nebezpečí. Bezpečnostní politiky by tuto variantu měly zohledňovat. Tato formulace je převzata ze zákon o IZS a vysvětlena v důvodové zprávě. Připomínkové místo s vypořádáním souhlasí.

259. Ministerstvo vnitra	Z	K § 41 odst. 4: V ustanovení se objevuje sousloví „<i>sít' CSIRT</i>“, aniž by však zkratka „<i>CSIRT</i>“ byla legislativně definována. Navrhujeme proto v návrhu definovat zkratku „<i>CSIRT</i>“.	Akceptováno – nyní § 44 Připomínkové místo s vypořádáním souhlasí.
260. Ministerstvo vnitra	Z	K § 42 odst. 2 a § 48 odst. 2: Podle uvedených ustanovení má zájemce/žadatel předložit potvrzení příslušných orgánů, např. Finanční správy ČR, příslušného finančního úřadu, výpis z Rejstříku trestů atd. V této souvislosti navrhujeme, aby si Úřad některé informace dohledal v rámci své úřední činnosti, a to poté, co zájemce udělí Úřadu souhlas s tímto dohledáním, a to z důvodu snížení byrokratické zátěže.	Akceptováno jinak – nyní § 45 a 51 Podle §53 odst. 1 písm. l) daňového řádu není nutný souhlas zájemce s dohledáním, což vede k dalšímu snížení byrokratické zátěže. Vyžádání si výpisu z rejstříku trestu by vyžadovalo speciální prolomení mlčenlivosti v rámci nZKB, neboť zákon č. 269/1994 Sb., o rejstříku trestů, upravuje vydávání výpisu správnímu orgánu pro účely správního řízení, jež v tomto případě zahájeno není. Nadto bylo naznáno, že se nejedná o administrativní zátěž, jež by byla neúnosná či zjevně nepřiměřená, i s ohledem k historickému vývoji institutu Národního CERT. Připomínkové místo s vypořádáním souhlasí.
261. Ministerstvo vnitra	Z	K § 56 a § 57: Upozorňujeme, že bude-li se v daném případě aplikovat kontrolní řád, je třeba zohlednit možné riziko případného vzniku duplicitní právní úpravy spočívající v oprávnění ukládat opatření k odstranění nebo prevenci nedostatků zjištěných kontrolou, které upravuje § 19 kontrolního řádu. Požadujeme se s touto otázkou vypořádat v důvodové zprávě.	Akceptováno – nyní § 59 a 60 Bude dovysvětleno v důvodové zprávě. Úřad bude moci ukládat nápravné opatření i bez kontroly. Připomínkové místo s vypořádáním souhlasí.
262. Ministerstvo vnitra	Z	K § 58 odst. 1 písm. p) a § 58 odst. 2 písm. p): Podle uvedené skutkové podstaty se poskytovatel regulované služby v režimu vyšších povinností dopustí přestupku tím, že neplní některou z povinností uloženou rozhodnutím o uložení nápravného opatření podle § 57. Za totéž chování lze sankcionovat jakoukoliv	Akceptováno – nyní § 61 Připomínkové ustanovení o přestupcích (§ 60) bylo v odst. 6 a 7 návrhu zákona upraveno tak, že se

		osobu, tj. také poskytovatele regulované služby, podle odst. 6 písm. d). Požadujeme uvedené ustanovení vypustit tak, aby došlo k odstranění duplicitní skutkové podstaty přestupku. Alternativně navrhuje skutkovou podstatu vypustit z odstavce 6 a vložit ji do odstavce 7. Obdobnou připomínku uplatňujeme rovněž k § 58 odst. 2 písm. p).	skutková podstata podle odst. 6 písm. d) přesunula do odst. 7, nově jako písm. b). Připomínkové místo s vypořádáním souhlasí.
263. Ministerstvo vnitra	Z	K § 62: Upozorňujeme, že bude-li se aplikovat kontrolní řád, může vyvstat riziko vzniku duplicitní právní úpravy spočívající v úpravě přestupků, sankcí a správního trestání, které upravuje § 15 a § 17 kontrolního řádu. Požadujeme se s touto otázkou vypořádat v důvodové zprávě.	Akceptováno – nyní § 64 Důvodová zpráva byla doplněna. Připomínkové místo s vypořádáním souhlasí.
264. Ministerstvo vnitra	Z	K § 63: Podle § 63 odst. 1 (věty první) návrhu jsou orgány veřejné moci povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty poskytnout Úřadu podněty, informace a jiné formy součinnosti potřebné k výkonu pravomocí a za účelem splnění povinností Úřadu, které jsou stanoveny tímto zákonem. Zmíněný § 63 odkazuje na problematiku součinnosti, kdy nastává otázka legálnosti poskytnutí informací, které jsou součástí trestního řízení či jiné policejní činnosti (spisového materiálu). Samotné znění ustanovení je direktivní a nekoresponduje se současnou legislativní úpravou, a to právě vůči orgánům veřejné moci. V návaznosti na argumentaci k § 29 návrhu zákona navrhuje § 63 odst. 1 doplnit o výjimku (resp. možnost potupovat v nezbytně nutné míře odlišně) pro orgány činné v trestním řízení. Na konci textu § 63 odst. 3 tedy navrhuje doplnit slova „; <i>plnění těchto povinností mohou orgány činné v trestním řízení v nezbytně nutném rozsahu omezit nebo na nezbytně nutnou dobu odložit, pokud by poskytnutím součinnosti došlo k ohrožení či zmaření účelu trestního řízení</i>“.	Akceptováno – nyní 65 Děkujeme za doplnění. Zmíněné ustanovení nemělo nikdy za cíl narušovat procesy upravené jinými právními předpisy, natož narušovat úkony orgánů činných v trestním řízení při jejich činnosti. Měli jsme za to, že tomuto cíli dostatečně odpovídá "a nestanoví-li zvláštní předpis jinak,..." v odstavci 1 dotčeného ustanovení tohoto návrhu. Přesto byla připomínka akceptována a navrhovaná věta doplněna. Připomínkové místo s vypořádáním souhlasí.

265. Ministerstvo vnitra	Z	K § 66: Navrhujeme do § 66 návrhu k výčtu informací, které jsou uchovávány odděleně mimo spis, přidat i ty, jež by mohly ohrozit či zmařit účel trestního řízení. Navrhujeme toto znění § 66: „§ 66 <i>Části písemností a záznamy, které obsahují utajované informace nebo informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, účinnost protipatření podle § 20, opatření obecné povahy podle § 30 nebo ohrozit či zmařit účel trestního řízení, uchovává Úřad v řízeních podle § 20, § 30 a § 31 odděleně mimo spis.“.</i>	Akceptováno jinak – nyní § 67 Dotčené ustanovení bylo změněno v tom smyslu, že pokrývá i zmaření účelu trestního řízení. Ohrožení účelu trestního řízení nebylo v dotčeném ustanovením uvedeno s ohledem na skutečnost, že zákon č. 141/1961, trestní řád, v účinném znění, v souvislosti s trestním řízením zmiňuje výhradně zmaření jeho účelu, viz § 51 odst. 2, § 88 odst. 9 a § 88a odst. 3. S ohledem na skutečnost, že Úřad není orgánem, který by se v rámci své agendy pravidelně zabýval trestněprávní problematikou, a zároveň nemusí ve všech případech vědět, zpřístupnění které informace může vést ke zmaření účelu trestního řízení, máme za vhodné nastavit spolupráci s orgány předávajícími informace tím způsobem, aby tyto orgány samy označily informace, u nichž je podle jejich názoru uvedené riziko dáno. Připomínkové místo s vypořádáním souhlasí.
266. Ministerstvo vnitra	Z	K Závěrečné zprávě z hodnocení dopadů regulace: 1. V části 3.1 shrnutí závěrečné zprávy RIA jsou vyhodnocovány dopady na státní rozpočet a ostatní veřejné rozpočty, avšak podle našeho názoru jde pouze o obecné konstatování a o velmi hrubé odhady předpokládaných dopadů. Ve shrnutí závěrečné zprávy RIA se mimo jiné na str. 4 uvádí, že k „zavedení mechanismu bezpečnosti dodavatelského řetězce je namístě podrobněji doplnit, že na poměry nových oblastí působnosti ústředního orgánu státní správy se očekává nízký dopad na státní rozpočet. Ve vztahu k návrhu zákona lze předpokládat především nutnost vyhrazení jednotek až nízkých desítek tabulkových míst u zapojených státních orgánů a rozšíření stávajících či připravovaných informačních systémů k technické obsluze procesů	Ad 1: Vysvětleno Požadavek na větší konkretizaci vyjádření dopadů na systemizovaná místa orgánů státní správy nemůže být splněn, závěrečná zpráva RIA byla pečlivě vypracována v souladu s metodikami pro zpracování RIA, které vydává Vláda. Možné dopady nové právní úpravy byly vyhodnocovány na základě veškerých, v danou chvíli dostupných, informací a vstupů, které NÚKIB obdržel od ministerstev a všech dalších zapojených orgánů, žádné další informace k daným problematikám nebyly v době zpracování RIA dostupné, a proto není možné konkrétněji predikovat některé dopady.

		<i>prověřování. V souladu s principem efektivity a cílem minimalizace ekonomických nákladů se bude maximálně využívat fungující synergie s již existujícími agendami a procesy, jakými jsou kupříkladu prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům veřejné správy či prověřování zahraničních investorů podle zákona o prověřování zahraničních investic, a to včetně účelného využívání informačních systémů, které tyto agendy podporují. Dopady na státní rozpočet pak může mít také zvýšení nákladů poskytovatelů strategicky významné služby z řad veřejné správy.“</i> Vzhledem k obecnosti vyhodnocení zvýšených nároků na systemizovaná místa u povinných subjektů a s ohledem na skutečnost, že vstup zákona v účinnost i podle předkladatele bude znamenat potřebu navýšení tabulkových míst, žádáme o větší konkretizaci vyjádření dopadů na systemizovaná místa orgánů státní správy. 2. Návrh zákona mj. zavádí mechanismus prověřování bezpečnosti dodavatelských řetězců. Národní úřadu pro kybernetickou a informační bezpečnost pak může vydat opatření obecné povahy, kterým zakáže nebo omezí plnění bezpečnostně relevantních dodávek poskytovatelům strategicky významných služeb. Takový zákaz představuje možný zásah do práva podnikat a provozovat jinou hospodářskou činnost a do vlastnického práva. Tato otázka byla předmětem rozsáhlých diskusí s komerčním sektorem, když Ministerstvo vnitra s ohledem na záměr budovat tzv. virtuálního operátora veřejné správy bude touto regulací dotčeno obdobně jako komerční provozovatelé 5G sítí. NÚKIB přitom odhaduje, že až 75 poskytovatelů strategicky významné služby budou soukromé subjekty. Vzhledem k takto vysokému počtu regulovaných subjektů s možnou zahraniční majetkovou účastí a s povahou zásahu do jejich práv navrhujeme doplnit závěrečnou zprávu hodnocení dopadů regulace o část, která vyhodnotí rizika spočívající s	Ad. 2: Neakceptováno Téma souladu mechanismu bezpečnosti dodavatelského řetězce s mezinárodními bilaterálními či multilaterálními dohodami bylo jednak zkoumáno ze strany NÚKIB, jednak bylo předmětem konzultací s relevantními orgány státu. U problémů souvisejících s posuzováním dopadů rizik spočívajících s uplatněním nároků dotčených subjektů podle mezinárodních dohod o ochraně investic NÚKIB nepředpokládá, že by takové nároky byly akceptovány/připuštěny. Dále, v případě potenciálních sporů, a to na základě dostupných informací, nelze takové dopady vyčíslit, jelikož obdobné spory, snad vyjma arbitrážního sporu mezi Švédskem a společností Huawei, jsou v rámci mezinárodních sporů doposud nedohledatelné. Zmíněná arbitráž navíc nedoznala rozhodnutí. Připomínkové místo s vypořádáním souhlasí.

		uplatněním nároků dotčených subjektů podle mezinárodních dohod o ochraně investic.	
267. Ministerstvo vnitra	D	Obecně k návrhu: Dáváme ke zvážení, zda by s ohledem na skutečnost, že § 40 obsahuje omezení práv osob, nebylo vhodné do návrhu doplnit úpravu poskytování případných náhrad (za poskytování osobní či věcné pomoci, škod apod.).	Akceptováno Doplněna ustanovení, podle kterých se budou náhrady škod a náhrady za omezení vlastnického práva nebo uložení povinnosti řídit nastavením podle zákona o krizovém řízení. Případná novelizace zákona o krizovém řízení tak může buď sama o sobě změnit náležitosti náhrad, případně je také počítáno s variantou, že novela krizového zákona s sebou přinese i novelu tohoto návrhu zákona, v rámci které budou náhrady upraveny dle potřeby. Připomínkové místo s vypořádáním souhlasí.
268. Ministerstvo vnitra	D	K § 5 písm. a) bodu 2: Doporučujeme zvážit, zda pojem „<i>veřejná bezpečnost</i>“, byť je v právu běžně užívaný, odpovídá smyslu „<i>regulované služby</i>“, pro který byl zaveden. Smyslu předkládaného návrhu by podle našeho soudu odpovídal více pojem „<i>vnitřní bezpečnost</i>“.	Vysvětleno Máme za to, že je možné ji vypořádat vysvětlením, nicméně pokud nebude Ministerstvo vnitra s uvedeným vysvětlením souhlasit, můžeme vypořádání změnit a připomínku akceptovat. Úprava podle navrženého znění vychází z výslovného překladu směrnice NIS2, která uvádí: „(...) narušení služby poskytované tímto subjektem by mohlo mít významný dopad na veřejný pořádek, veřejnou bezpečnost nebo ochranu zdraví“. Tento překlad odpovídá také anglické verzi směrnice, kde se uvádí: „<i>disruption of the service provided by the entity could have a significant impact on public safety, public security or public health</i>“. Obě definice tedy jasně pracují s veřejností tohoto kritéria. Náš dosavadní výklad tohoto pojmu (protože se objevoval také v předchozí směrnici NIS1) odpovídal v zásadě širokému výčtu „ochrana jednotlivce i společnosti

			proti útokům, jež ohrožují např. bezpečnost státu či jednotlivých státních orgánů, institucí a funkcí, bezpečnost jednotlivce, zejména jeho čest, důstojnost, svobodu a fyzickou integritu nebo majetek státu či jednotlivce". Tato definice se v některých dílčích aspektech liší od definice vnitřní bezpečnosti „Vnitřní bezpečnost státu pak v širším významu znamená zachování a zajištění vnitřních funkcí státu, ochranu jeho demokratických základů, ochranu vnitřního pořádku, bezpečnosti a zákonnosti, ochranu životů a zdraví, majetkových hodnot a životního prostředí před hrozbami majícími původ na území státu." (tato definice se objevuje v jedné z metodik MV, pokud je již neplatná, tak se rádi necháme poučit o novější verzi). Právě tyto dílčí odlišnosti u nás vzbuzují obavu ze dvou směrů - pokud namísto pojmu ze směrnice použijeme pojem vnitřní bezpečnost, bude transpozice směrnice provedena správně? A ještě důležitější otázka, pokud definice vnitřní bezpečnosti pracuje s „před hrozbami majícími původ na území státu." není tato definice vůbec aplikovatelná, protože v kybernetickém prostoru mají hrozby původ kdekoli a nelze je omezovat na původ výhradně v České republice. Z těchto dvou důvodů jsme se rozhodli pojem zachovat, nicméně jak uvádíme výše, nebráníme se další diskuzi a budeme rádi za případné upřesnění. Připomínkové místo s vypořádáním souhlasí.
269. Ministerstvo vnitra	D	K § 29 odst. 1 a 2: Doporučujeme upřesnit, od jakého okamžiku se navržené lhůty počítají.	Akceptováno - nyní § 30 V § 30 odst. 1 a 2 bylo upřesněno, že rozhodnou právní skutečností určující počátek běhu předmětné lhůty je obdržení žádosti Úřadu.

			Připomínkové místo s vypořádáním souhlasí.
270. Ministerstvo vnitra	D	K § 39 odst. 2: Navrhujeme povinnosti, které jsou uloženy provozovateli celoplošného televizního nebo rozhlasového vysílání při vyhlášení stavu kybernetického nebezpečí, zahrnout do samostatného ustanovení, popřípadě do povinností právnických osob, neboť se domníváme, že by tento přesun zajistil lepší přehlednost v systematice předkládaného návrhu.	Akceptováno - nyní § 40 Připomínkové místo s vypořádáním souhlasí.
271. Ministerstvo vnitra	D	K § 40 odst. 2 písm. a): Ustanovení § 40 odst. 2 doporučujeme upravit takto: <i>„a) provést opatření uvedené v odstavci 1,</i> <i>b) strpět omezení vyplývající z opatření v odstavci 1,“</i> a stávající písmena b) až d) označit jako c) až e). Původní návrh totiž ukládá orgánům a osobám povinnost plnit opatření za stavu kybernetického nebezpečí bez přímé vazby na konkrétní opatření uvedená v odstavci 1. Dále je doplněno nové písmeno b), které ukládá povinnost strpět omezení vyplývající z vyhlášených opatření.	Akceptováno jinak - nyní § 41 Na základě společných jednání došlo ke komplexnímu přepracování ustanovení týkajících se stavu kybernetického nebezpečí. V souvislosti s tím došlo i k úpravě odstavce dva. Připomínkové místo s vypořádáním souhlasí.
272. Ministerstvo vnitra	D	K § 41 odst. 3 písm. v) a x), § 43, § 45 odst. 1 písm. f), § 53 odst. 3, § 54 odst. 1 písm. b) a c) a odst. 3 a 4, § 60 odst. 1 a 5 a § 61 odst. 1 a 5: Navrhujeme v odůvodnění důvodové zprávy blíže rozvést, zda se pro účely jmenovaných ustanovení upravujících kontrolní činnosti Národního úřadu pro kybernetickou a informační bezpečnost a Stálé komise pro kontrolu činnosti Úřadu podle návrhu užije kontrolní řád, jakožto obecný procesní předpis pro oblast kontrol, nebo se uplatní jiná, zvláštní (speciální) úprava.	Neakceptováno Jestliže není stanoveno jinak, uplatní se právní úprava podle obecných právních předpisů (v tomto případě mj. správního řádu a zákona o kontrole). Návrh speciální úpravu v uvedených případech neobsahuje, proto v nich bude Úřad postupovat podle obecných právních předpisů. Jelikož se jedná o obecné právní pravidlo, nepovažujeme za nezbytné důvodovou zprávu upravit požadovaným způsobem. Připomínkové místo s vypořádáním souhlasí.

273. Ministerstvo vnitra	D	K § 42 odst. 5: Navrhujeme větu poslední u návrhu odstranit, a to pro její normativně diskutabilní obsah. Z návrhu není jasné, jaký bude následek stavu, kdy provozovatel Národního CERT nezbytné náklady nevynaloží.	Neakceptováno - nyní § 45 odst. 5 Jedná se o imperfektní normu, jež v zákoně sankci nemá. Připomínkové místo s vypořádáním souhlasí.
274. Ministerstvo vnitra	D	K tezí prováděcích právních předpisů: 1. V příloze dokumentu „Vyhláška o kritériích rizikivosti dodavatele“ navrhujeme v bodě 1. za slova „<i>demokratický politický systém</i>“ doplnit slova „<i>nebo nejsou dodržována lidská práva a svobody</i>“. 2. U přílohy dokumentu „<i>Vyhláška o kritériích rizikivosti dodavatele</i>“, kde jsou stanovena kritéria 1. až 3., upozorňujeme, že určení uvedených kritérií může být poměrně složité, v zájmu vyšší míry transparentnosti doporučujeme alespoň příkladem v odůvodnění uvést, o co se hodnocení bude opírat (např. zprávy a hodnocení vybraných mezinárodních organizací apod.). 3. V příloze dokumentu „<i>Vyhláška o kritériích rizikivosti dodavatele</i>“, navrhujeme v bod 8. zohlednit i vznik českého sankčního mechanismu podle zákona č. 1/2023 Sb. Dále lze doporučit zpřesnění, zda má jít o mezinárodní sankce v rámci organizací (např. OSN, EU) nebo i jiných států (např. USA). Dále upozorňujeme, že kritérium spočívající ve slovním spojení „<i>či existuje vysoká pravděpodobnost, že na danou zemi budou tyto mezinárodní sankce uvaleny</i>“ je velmi neurčité, proto jej navrhujeme vypustit. 4. V návrhu „<i>Vyhlášky o kritériích rizikivosti dodavatele</i>“, která byla Ministerstvu vnitra poskytnuta na jaře 2023 ke konzultacím, bylo uvedeno též kritérium dodavatele spočívající v „<i>pravomocném odsouzení dodavatele pro trestný čin spáchaný ve spojitosti s předmětem podnikání nebo významně ohrožující bezpečnost nebo vnitřní či veřejný pořádek České republiky nebo jiných členských států</i>“.	Ad 1: Neakceptováno Byť jsou teze prováděcích právních předpisů součástí předkládaného materiálu, tyto budou předmětem samostatného připomínkového řízení při procesu jejich vydávání. Vaši připomínku bereme na vědomí a určitě doporučujeme veškeré připomínky směřující k prováděcím předpisům uplatnit v rámci připomínkového řízení k vyhláškám k navrhovanému zákonu, aby tyto mohly být řádným způsobem vypořádány. Nutno ovšem dodat, že konkrétně zmíněný prováděcí předpis, tedy vyhláška o kritériích rizikivosti dodavatele, se ruší. Zmíněná kritéria posuzování rizikivosti dodavatele v rámci vyhlášky sloužila primárně jako vodítko/metodika k určení hrozby, přičemž vyhláška o kritériích rizikivosti dodavatele byla, mimo jiné důvodů uvedených v této a obdobných připomínkách, vyřazena. Kritériem tudíž zůstává bezpečnost ČR a její vnitřní či veřejný pořádek. Ad 2: Vysvětleno Byť jsou teze prováděcích právních předpisů součástí předkládaného materiálu, tyto budou předmětem samostatného připomínkového řízení při procesu jejich vydávání. Vaši připomínku bereme na vědomí a určitě doporučujeme veškeré připomínky směřující k prováděcím předpisům uplatnit v rámci připomínkového řízení k vyhláškám k navrhovanému

		<i>Evropské unie, Evropského hospodářského prostoru, Severoatlantické aliance či Organizace pro hospodářskou spolupráci a rozvoj</i>“. Ministerstvo vnitra navrhovalo, aby kritériem bylo již samotné zahájení trestního řízení, a doporučoval zvážit také zahrnutí pravomocných rozhodnutí o správních deliktech v oblasti ochrany utajovaných informací, ochrany osobních údajů, ochrany duševního a průmyslového vlastnictví apod. To vše v rozsahu, kterým může dané řízení/odsouzení mít vliv nebo ohrozit bezpečnost státu či účel chráněný tímto zákonem. Z předkládaného návrhu není jasné, proč bylo dané kritérium v aktuálně překládaném návrhu vypuštěno. Navrhujeme zvážit jeho doplnění.	zákonu, aby tyto mohly být řádným způsobem vypořádány. Nutno však dodat, že zmíněná kritéria posuzování rizikivosti dodavatele v rámci vyhlášky sloužila primárně jako vodítko/metodika k určení hrozby, přičemž samotná vyhláška o kritériích rizikivosti dodavatele byla, mimo jiné důvodů uvedených v připomínce, vyřazena. Kritériem tudíž zůstává bezpečnost ČR a její vnitřní či veřejný pořádek. Ad 3: Vysvětleno Byť jsou teze prováděcích právních předpisů součástí předkládaného materiálu, tyto budou předmětem samostatného připomínkového řízení při procesu jejich vydávání. Vaši připomínku bereme na vědomí a určitě doporučujeme veškeré připomínky směřující k prováděcím předpisům uplatnit v rámci připomínkového řízení k vyhláškám k navrhovanému zákonu, aby tyto mohly být řádným způsobem vypořádány. Nutno však dodat, že zmíněná kritéria posuzování rizikivosti dodavatele v rámci vyhlášky sloužila primárně jako vodítko/metodika k určení hrozby, přičemž samotná vyhláška o kritériích rizikivosti dodavatele byla, mimo jiné důvodů uvedených v připomínce, vyřazena. Kritériem tudíž zůstává bezpečnost ČR a její vnitřní či veřejný pořádek. Ad 4: Vysvětleno Byť jsou teze prováděcích právních předpisů součástí předkládaného materiálu, tyto budou předmětem samostatného připomínkového řízení při procesu jejich vydávání. Vaši připomínku bereme na vědomí a určitě doporučujeme veškeré připomínky směřující k

			prováděcím předpisům uplatnit v rámci připomínkového řízení k vyhláškám k navrhovanému zákonu, aby tyto mohly být řádným způsobem vypořádány. Je nasnadě ovšem znít, že uvedený prováděcí právní předpis se ruší. Zmíněná kritéria posuzování rizikovosti dodavatele v rámci vyhlášky sloužila primárně jako vodítko/metodika k určení hrozby, přičemž vyhláška o kritériích rizikovosti dodavatele byla, mimo jiné z důvodu připomínek směřujících k smyslu kritérií, vyřazena. Kritériem tudíž zůstává bezpečnost ČR a její vnitřní či veřejný pořádek. Připomínkové místo s vypořádáním souhlasí.
275. Ministerstvo vnitra	D	K nadpisu návrhu: Podle čl. 31 odst. 1 písm. b) Legislativních pravidel vlády doporučujeme za datem odstranit čárku.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
276. Ministerstvo vnitra	D	K označení částí: 1. V souladu s čl. 25 odst. 2 písm. a) Legislativních pravidel vlády navrhujeme části neoznačovat tučně. 2. V případě části třetí pak dáváme na zvážení, zda by její nadpis neměl znít pouze „ZÁVĚREČNÉ USTANOVENÍ“.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
277. Ministerstvo vnitra	D	K označení hlav: Podle čl. 25 odst. 2 písm. b) Legislativních pravidel vlády doporučujeme označení hlav uvést malým písmem s velkým počátečním písmenem a zároveň označení hlav neuvádět tučně.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
278. Ministerstvo vnitra	D	K označení Hlavy II a nadpisu § 71: Upozorňujeme na duplicitní nadpis.	Akceptováno Připomínkové místo s vypořádáním souhlasí.

279. Ministerstvo vnitra	D	K označení paragrafů: Počínaje § 2 navrhujeme v souladu s čl. 26 Legislativních pravidel vlády neoznačovat paragrafy tučně.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
280. Ministerstvo vnitra	D	K § 12 odst. 2 písm. b), § 17 odst. 3 písm. b), 32 odst. 1 písm. a), § 41 odst. 3 písm. y) a § 52 odst. 2 písm. h): Doporučujeme na koncích ustanoveních odebrat čárky umístěné před spojkami „a“.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
281. Ministerstvo vnitra	D	K § 13 odst. 1 písm. b) a c): Ve větě první doporučujeme text „ <i>písm.</i> “ nahradit slovy „ <i>písmene</i> “.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
282. Ministerstvo vnitra	D	K § 18 odst. 4: Upozorňujeme, že podle čl. 44 odst. 2 Legislativních pravidel vlády by legislativní zkratka neměla být složena z velkých písmen. Navrhujeme tedy rozepsání výrazu „ <i>NUKIB</i> “, případně úpravu, která bude korespondovat s požadavky Legislativních pravidel vlády.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
283. Ministerstvo vnitra	D	K § 25 odst. 2: Před slovem „ <i>zejména</i> “ navrhujeme vložit čárku.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
284. Ministerstvo vnitra	D	K § 30 odst. 3: Navrhujeme slovo „ <i>písmene</i> “ nahradit textem „ <i>písm.</i> “.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
285. Ministerstvo vnitra	D	K § 32 odst. 1 písm. b): Doporučujeme slovo „ <i>písmena</i> “ nahradit tvarem „ <i>písmene</i> “, který je užíván v návrhu.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
286. Ministerstvo vnitra	D	K § 34 odst. 3: V ustanovení navrhujeme text „ <i>odst.</i> “, který je uveden jako první, nahradit slovem „ <i>odstavcích</i> “.	Akceptováno Připomínkové místo s vypořádáním souhlasí.

287. Ministerstvo vnitra	D	K § 35 odst. 1 písm. c) a § 36 odst. 2 písm. d) a f): Upozorňujeme, že v legislativní praxi se neužívá pojem „ <i>e-mailová adresa</i> “, ale pojem „ <i>adresa elektronické pošty</i> “.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
288. Ministerstvo vnitra	D	K § 41 odst. 4 písm. e): Upozorňujeme na sníženou srozumitelnost první věty ustanovení.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
289. Ministerstvo vnitra	D	K § 55 odst. 1 písm. j): Doporučujeme zvážit užití dvojnásobného odkazu, kdy nejprve je odkazováno na § 44 odst. 2 a následně i na § 44 odst. 3. Z odkazů není zřejmý úmysl předkladatele.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
290. Ministerstvo vnitra	D	K § 58 odst. 4 písm. b): Doporučujeme za slovo „ <i>požadavky</i> “ vložit slova „ <i>uvedenými v</i> “.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
291. Ministerstvo vnitra	D	K § 58 odst. 13: Opětovně upozorňujeme na čl. 44 odst. 2 Legislativních pravidel vlády, podle nějž by legislativní zkratka neměla být složena z velkých písmen. Navrhujeme proto rozepsání výrazu „ <i>ENISA</i> “, případně jeho úpravu, která bude korespondovat s požadavky Legislativních pravidel vlády.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
292. Ministerstvo vnitra	D	K § 58 odst. 15 písm. b): Navrhujeme umístit čárku za slovo „ <i>osobou</i> “ a odebrat čárku za slovem „ <i>nebo</i> “.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
293. Ministerstvo vnitra	D	K § 62: Máme pochybnost o systematickém zařazení daného ustanovení, neboť vztah ke kontrolnímu řádu je vymezen již v § 56 a ke správnímu řádu také v § 65.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
294. Ministerstvo vnitra	D	K § 69 odst. 1 písm. a):	Akceptováno

		Slova „ <i>údajů podle odst. 2</i> “ navrhujeme s odkazem na čl. 71 Legislativních pravidel vlády nahradit slovy „ <i>údajů podle odstavce 2</i> “.	Připomínkové místo s vypořádáním souhlasí.
295. Ministerstvo vnitra	D	K § 71: 1. Jednotlivé odstavce přechodného ustanovení navrhujeme uvést do souladu s čl. 26 odst. 3 Legislativních pravidel vlády. 2. Současně doporučujeme ve všech odstavcích revidovat užívání interpunkce.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
296. Ministerstvo vnitra	D	K § 72: 1. Za slovy „ <i>Zrušují se</i> “ navrhujeme vložit dvojtečku. 2. Dále upozorňujeme, že je třeba samostatně zrušit i jednotlivé novely rušených právních předpisů (srov. čl. 52 odst 2 Legislativních pravidel vlády). 3. Doporučujeme rušené právní předpisy řadit podle data jejich publikace ve Sbírce zákonů.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
297. Ministerstvo vnitra	D	K § 73: Navrhujeme ustanovení věnované účinnosti označit jako část čtvrtou a adekvátně tomu upravit i nadpis.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
298. Ministerstvo vnitra	D	K poznámkám pod čarou č. 5, 7, 8 a 10: Navrhujeme uvést celý název citovaného předpisu. Dále upozorňujeme, že slovo „ <i>Nářízení</i> “ není třeba psát s velkým počátečním písmenem.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
299. Asociace malých a středních podniků a živnostníků ČR	Z	RIA <u>Cíl:</u> Požadujeme doplnit RIA o dopad na malé a střední podniky. <u>Odůvodnění:</u> Zpracovatel dopad na malé a střední podniky nevyhodnotil. Přitom střední podniky jsou subjekty, na které směrnice - a tedy i zákon - dopadne, v případě malých a mikropodniků pak na ně dopadne zákon pokud jsou vybranými poskytovateli regulovaných služeb (například poskytovateli služeb elektronických komunikací). NÚKIB má přitom množství metodik dostupných na webu Úřadu	Vysvětleno Problematika jakéhokoliv výpočtu nákladů nebo odhadů je v oblasti kybernetické bezpečnosti dlouhodobě problematická. Se směrnicí NIS2 přibývá do tohoto procesu celá řada neznámých. NÚKIB učinil v rámci zprávy hodnocení dopadů prozatím největší realizovaný výpočet v rámci právních předpisů v jeho gesci, přičemž s vědomím nemožnosti výpočtu

		vlády, například mohl měřit administrativní zátěž podnikatelů dle platné metodiky Ministerstva průmyslu a obchodu z července 2017. Tato metodika je přitom závaznou pro zpracování RIA tak, jak to uvádí na svých stránkách Úřad vlády. Metodika obsahuje vzorovou tabulku pro výpočet administrativní zátěže v právním předpise, kterou NÚKIB zjevně nepoužil, aniž by zdůvodnil, proč. Stejně tak neodůvodnil, proč nepoužil výše zmíněnou metodiku.	konkrétní částky (ve smyslu metodiky MPO) zpracoval hodnocení dopadů alespoň porovnáním různých metodik a výpočtů, což vedlo ve výsledku alespoň k orientačnímu stanovení daných nákladů. Vedle toho je i nadále problematická další neznámá - ještě v tuto chvíli, několik měsíců po přijetí směrnice, probíhají na úrovni Evropské unie diskuze o tom, jak některé definice povinných osob chápat a pojímat, případně jak aplikovat velikostní kritérium. NÚKIB se dlouhodobě snaží vyjednávat racionální přístup a tím omezovat počet regulovaných osob na účelné minimum. Obdobný podnět byl také připomínkou gestora této metodiky, MPO, na základě kterého byly některé dílčí informace do hodnocení dopadů doplněny. V zásadě k této připomínce je nutno uvést, že výpočet podle metodiky měření a přeměňování administrativní zátěže podnikatelů MPO byl obdobným způsobem prováděn již v rámci zdrojových průzkumů, které jsou podkladem výpočtu uvedeného v hodnocení dopadů. S ohledem na výše uvedené se NÚKIB ve spolupráci s Ministerstvem vnitra také zaměřil na přípravu metodické pomůcky ke zjištění výše nákladů v každé konkrétní organizaci, aby tím alespoň podpořil organizace v krátkodobém a střednědobém plánování (viz zde: https://osveta.nukib.cz/mod/page/view.php?id=3149) Připomínkové místo s vypořádáním souhlasí.
300. Asociace malých a středních podniků a živnostníků ČR	Z	K § 6 odst. 3 <u>Cíl:</u> Požadujeme režim poskytovatele regulované služby stanovit přímo v zákoně (v příloze zákona) z důvodu regulační a právní jistoty. <u>Odůvodnění:</u> Odstavec požadujeme změnit takto: Režim poskytovatele regulované služby je stanoven ~~prováděcím právním předpisem v příloze tohoto zákona~~ zákonem. Je-li orgán nebo osoba poskytující regulovanou službu určen rozhodnutím Úřadu podle § 5,	Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných

		je vždy poskytovatelem regulované služby v režimu vyšších povinností.	informačních systémech [§ 3 a § 2 písm. d)], tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby [§ 3, ve spojení s § 2 písm. i) a k) a § 22a]. Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon [§ 4 odst. 1 písm. d) se spojení s § 2 písm. i), k), l) a m)], a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá [§ 3 a § 2 písm. b)]. Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Reakce připomínkového místa: Argumentace, že nyní je způsob provádění prováděcím předpisem aktuální je argumentací zcela nedostatečnou, jenž v podstatě popírá snahu nové legislativy zlepšovat právní prostředí v ČR. Reakce NÚKIB: Vyjádření obsahuje srovnání s předchozí právní úpravou, protože se jedná o právní otázku, která už je vyřešena a byla vyřešena už v minulosti v případě přijímání krizového zákona i současného zákona o kybernetické bezpečnosti. Oba návrhy prošly mezirezortním připomínkovým řízením, stejně tak

			jako přezkumem Legislativní rady vlády, i Parlamentem. Tento způsob identifikace povinných osob (tedy stanovení detailních kritérií v prováděcím právním předpise na základě obecného kritéria v zákoně) nebyl nikdy doposud ústavně ani jinak napadán, a to ani v případě novelizací zmíněných zákonů. Protože se jedná o čistě právní problém, nikoliv problém věcný, je potřeba také uvést, že místa k tomu nejpovolanější - tedy zejm. kabinet ministra pro legislativu a odbor kompatibility Úřadu vlády s navrženým vypořádáním této otázky souhlasí, resp. nemají proti němu námitek. Tento právní názor považujeme spolu s výše uvedeným za směrodatný. Reakce připomínkového místa: Vzhledem ke skutečnostem Vámi uvedeným akceptuji vypořádání našich připomínek k danému materiálu. Připomínkové místo s vypořádáním souhlasí.
301. Asociace malých a středních podniků a živnostníků ČR	Z	K § 10 odst. 2 Cíl: Požadujeme změnit text návrhu takto: Poskytovatel regulované služby zapsaný v evidenci poskytovatelů regulovaných služeb je povinen plnit všechny povinnosti plynoucí mu ze zákona vůči zapsaným regulovaným službám nejpozději od uplynutí šesti měsíců od okamžiku doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb až do okamžiku doručení vyrozumění o výmazu z evidence poskytovatelů regulovaných služeb podle § 11. Odůvodnění: Je třeba přijmout dostatečnou lhůtu k tomu, aby byl subjekt vůbec schopen plnit požadované povinnosti vyplývající ze zákona tak, aby obstál při případné kontrole. Z tezi vyhlášek vyplývá, že některé povinnosti budou poskytovatelé regulované služby v režimu vyšších povinností muset realizovat pomocí zaměstnanců či kontraktorů s konkrétními znalostmi a dovednostmi, které nemusí být v dané organizaci dosud vůbec přítomni. Navíc musí dojít k revizi	Vysvětleno Den doručení písemného vyrozumění o zápisu do evidence regulovaných služeb je rozhodným datem, se kterým celý zákon pracuje i na jiných místech a počítá se od něj běh některých lhůt. Například jedna z hlavních povinností zavádět bezpečnostní opatření má na zavedení podle § 14 odst. 3 návrhu zákona lhůtu v délce jednoho roku a začíná běžet od tohoto rozhodného data. Neplatí tedy, že by tato povinnost začala platit ihned po doručení vyrozumění o zápisu do evidence. Toto ustanovení pouze říká, že od vyrozumění zápisu do evidence platí, že daná služba je regulovanou službou a poskytovatel regulované služby vůči ní musí plnit své povinnosti. Jednotlivé

		smluv s dodavateli a k další řadě plnění, které zajistí compliance. U menších poskytovatelů služeb elektronických komunikací může být velká komplikace vůbec nalézt vhodné lidi – pokud předpokládáme že po datu účinnosti zákona bude podobné subjekty poptávat velká část nově regulovaných subjektů, nemusí se na ně vůbec dostat. Je potřeba si uvědomit, že úřad bude regulovat nově až 2000 subjektů v odvětví elektronických komunikací, z nichž řada jsou mikropodniky v odlehlých venkovských oblastech.	povinnosti pak vyplývají z dalších ustanovení a mají své samostatné lhůty. Připomínkové místo s vypořádáním souhlasí.
302. Asociace malých a středních podniků a živnostníků ČR	Z	K § 28 odst. 3a) Cíl: Odst. 3a) tak požadujeme změnit takto: Pro potřeby mechanismu prověřování bezpečnosti dodavatelského řetězce se rozumí a) kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úroveň kritická, a jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby, Odůvodnění: Dle našeho přesvědčení postačí, když budou předmětem prověřování pouze aktiva, u nichž poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotí dopad narušení bezpečnosti informací na stanovených rozsah strategicky významné služby na úroveň kritická. Tím bude zachována působnost mechanismu pouze na skutečně “kritickou část stanoveného rozsahu” a nikoli na de facto celou síť, jak je nastaven dnes. To by znamenalo, že regulovanými subjekty budou stovky malých a středních podniků, které dodávají v regionech velkým národním operátorům dílčí lokální služby konektivity, které nejsou kritické z hlediska kybernetické bezpečnosti, ale které by se dle návrhu vyhlášky pravděpodobně dostaly do významně široce definované “kritické části stanoveného rozsahu”. Zároveň jsme přesvědčeni, že identifikace podle prováděcího právního předpisu postačuje k tomu, aby NÚKIB dosáhl zamýšleného cíle, tedy že	Neakceptováno - nyní § 29 odst. 3 písm. a) Navrhovaný zákon, včetně ustanovení § 29 odst. 3 písm. a), má za cíl chránit vše, co je z hlediska kybernetické bezpečnosti považováno za kritické pro fungování strategicky významných služeb. Konkrétně v oblasti telekomunikací je nasnadě chránit její kritické části jak v jádru sítě, tak rovněž například v rádiové přístupové síti, jež je z hlediska propojení koncového zařízení s jádrem kritická. Ochrana kritické části stanoveného rozsahu, tak jak je definována dotčeným ustanovením, je kritická z pohledu kybernetické bezpečnosti a, v rámci logiky navrhovaného zákona, žádoucí. Vaše obavy chápeme, avšak dodáváme, že vyhláška o nepominutelných funkcích je významná z hlediska komplexity a kaskádovitosti veřejných komunikačních sítí. To znamená, že na těchto sítích je závislá řada dalších strategicky významných služeb, přičemž u těchto sítí je díky jejich dobré mezinárodní standardizaci snazší určit části, které jsou pro fungování takové sítě kritické. Z toho důvodu vyhláška o nepominutelných funkcích upravuje veškeré kritické funkce, nehledě na jejich pozici v topologii sítě, a to včetně funkcí rádiové přístupové

		mechanismus bude prověřovat dodavatele aktiv, která jsou kritickou částí stanoveného rozsahu. Je to patrné i z toho, že v tezí vyhlášky jsou nepominutelné funkce stanovené pro síť a služby elektronických komunikací, ale nikoli pro subjekty v ostatních odvětvích stanovených v § 27 odst. 1. Požadujeme tak zrušit zákonné zmocnění úřadu vydat prováděcí právní předpis stanovující nepominutelné funkce stanoveného rozsahu. Rozsah mechanismu je navíc nutné zaměřit pouze na taková aktiva, u nichž má jejich nedostupnost přímý okamžitý dopad na nedostupnost strategicky významné služby, což je nejvýznamnější hrozba.	sítě, bez níž by nedošlo k propojení uživatelů, včetně IZS, s jádrem sítě. Připomínkové místo s vypořádáním souhlasí.
303. Asociace malých a středních podniků a živnostníků ČR	Z	K § 28 odst. 3c) <u>Cíl:</u> Požadujeme lépe definovat, kdo je dodavatelem a kdo je poddodavatelem <u>Odůvodnění:</u> Problém je, že v současné podobě návrhu dopadá prověřování bezpečnosti dodavatelského řetězce takřka na každého malého a středního lokálního a regionálního poskytovatele služeb či sítí elektronických komunikací, protože NÚKIB definuje extrémně široce “kritickou část stanoveného rozsahu” v sektoru elektronických komunikací tak, že představuje prakticky celou síť, včetně částí a systémů, které nejsou tak kritické (jako rádiová část sítě, transportní část sítě nebo různé fakturační systémy a podobně). Sektor elektronických komunikací je extrémně propojen řadou dodavatelsko-odběratelských vztahů právě v oblasti okrajových částí sítě (velcí národní operátoři si dílí velmi lokální služby nakupují od lokálních subjektů a naopak). Zjevně nejde o služby, které je možné označit za “kritické” při zachování principu proporcionality, ale přesto je úřad chce regulovat. To by mělo zásadní vliv na podnikání malých a středních regionálních firem, který není zohledněný v RIA (která má dle obecných zásad pro hodnocení dopadů regulace hodnotit dopad na podnikatelské prostředí „zejména s ohledem na osoby samostatně výdělečně činné a malé a střední podniky“).	Vysvětleno - nyní § 29 odst. 3 písm. c) S tvrzením, že současné podobě návrhu dopadá prověřování bezpečnosti dodavatelského řetězce takřka na každého malého a středního lokálního a regionálního poskytovatele služeb či sítí elektronických komunikací se nelze ztotožnit. Návrh zákona dopadá pouze na poskytovatele strategicky významných služeb, mezi které výše uvedení poskytovatelé nespádají. V případě označení některého z dodavatelů či poddodavatelů za rizikové na ně úprava dopadne v tom smyslu, že pokud dodávají bezpečnostně významné dodávky do kritické části strategicky významné služby, poskytovatelé strategicky významných služeb budou moci těchto dodávek využívat buď s omezeními nebo vůbec. To je však podstatou celého mechanismu, kdy, pokud je dodavatel (či poddodavatel) shledán rizikovým, dojde k jeho omezení ve strategicky významných službách. Definice dodavatele a poddodavatele potom zcela koresponduje s naznačeným cílem. Záměrně není definována hloubka dodavatelského řetězce, protože to by mohlo vést k obcházení povinností stanovených v návrhu zákona, a tak k zmaření jeho cíle. Naopak

			riziko pro strategicky významnou službu může přijít z kterékoliv úrovně dodavatelského řetězce. Připomínkové místo s vypořádáním souhlasí.
304. Asociace malých a středních podniků a živnostníků ČR	Z	K § 30 <u>Cíl:</u> Požadujeme významné omezení rozsahu mechanismu a jeho provádění orgánem s politickou odpovědností, jako je například Ministerstvo průmyslu a obchodu, které má podobnou pravomoc v podobě prověřování zahraničních investic, které je funkčně podobné (posuzování konkrétní firmy na základě konkrétních kritérií). <u>Odůvodnění:</u> Kritéria pro hodnocení rizikovosti dodavatelů určená ve vyhláškách se netýkají kybernetické ani informační bezpečnosti (ale jen právního systému země mající vliv na dodavatele a podobně), není tak jasné, proč by měl jejich vyhodnocení provádět Národní úřad pro kybernetickou a informační bezpečnost a nikoli ústřední orgán státní správy, který již obdobný úkol plní v oblasti prověřování zahraničních investic (což je také pravomoc, která není svěřena např. Úřadu pro ochranu hospodářské soutěže). Navrhovaný rozsah a velikost mechanismu je navíc zjevně byrokratické monstrum. V důvodové zprávě se uvádí, že jen na prověřování dodavatelů bude mít NÚKIB a další orgány enormní personální požadavky - dohromady asi 53 lidí. Další “vyšší desítky” míst bude úřad chtít kvůli kontrolování souladu se zákonem nad rámec schválené koncepce rozvoje úřadu, která i tak počítá s jeho rozšiřováním. Po účinnosti zákona se dá očekávat na úrovni poskytovatelů regulovaných služeb vysoká okamžitá poptávka po zaměstnancích či kontraktorech, kteří pomohou daným organizacím zajistit soulad s požadavky zákona (který je vymáhán poměrně drakonickými pokutami). V Česku přitom panuje extrémní nedostatek pracovníků v oblasti IT.	Neakceptováno - nyní § 31 Ministerstvo průmyslu a obchodu je dle § 30 odst. 1 navrhovaného zákona zapojeno přímo do procesu posuzování rizikovosti dodavatele. Navíc opatření obecné povahy o případném omezení či zákazu dodavatele NÚKIB rovněž projedná mimo jiné s ministerstvem průmyslu a obchodu (§ 30 odst. 2), aby byly získány všechny relevantní pohledy a perspektivy pro proporcionální stanovení povinností daným opatřením obecné povahy. V souvislosti s politickou odpovědností je nutno zmínit, že úkol řešit bezpečnost dodavatelského řetězce byl NÚKIB dán Bezpečnostní radou státu, která se bude podílet i na samotném mechanismu bezpečnosti dodavatelského řetězce. Dále se NÚKIB za svou činnost zodpovídá vládě, respektive ředitel NÚKIB předsedovi vlády. Stejně tak je NÚKIB pod dozorem poslaneckého výboru pro bezpečnost. Připomínkové místo s vypořádáním souhlasí.
305. Svaz měst a obcí České republiky	Z	Úvodem je Svaz měst a obcí ČR (dále jen „Svaz“) povinen akcentovat, že návrh jako celek včetně doprovodných materiálů (tj. tezí prováděcích předpisů) je strukturován a vyjádřen nesrozumitelně a zmatečně. I pro profesionály (osoby vzdělané v oboru právo a právní věda či v oblasti IT) je svízelné materiál	Neakceptováno Co se týče srozumitelnosti materiálu máme za to, že jej není nutné přepracovávat. Tak jako je podstatou Vaší připomínky jeho možná nepřehlednost, nedostatek vnitřní konzistence a nepochopitelnost,

		pročíst a pochopit jej včetně jeho provazeb na prováděcí právní předpisy. <i>Navrhujeme přepracování materiálu jako celku tak, aby byl přehledný, vnitřně konzistentní a pochopitelný.</i> <i>Současně navrhujeme, aby materiál jako celek (tj. návrh včetně prováděcích právních předpisů) respektoval princip právní jistoty a nebyly zásadní záležitosti předmětem úpravy podzákonými právními předpisy.</i> <i>Rovněž navrhujeme zvážení výlučné působnosti NÚKIB, zejména v hodnocení dodavatelského řetězce, bez ingerence dalších ústředních orgánů státní správy. Vnímáme jako zásadní zachování principu zákazu omezení podnikání, principu předvídatelnosti a právní jistoty.</i>	stejně tak získáváme průběžně zpětnou vazbu chválící opak. Návrh zákona je vnitřně strukturován na jednotlivé hlavy, přičemž ty jsou strukturovány tak, aby se nejdříve zaměřovaly na ta ustanovení, která budoucí adresáty normy předpisem provedou a následně pak ta ustanovení, která jsou svou povahou spíše doprovodná. Na vhodných místech předpis odkazuje na prováděcí právní předpisy, které jsou tvořeny ústavně souladně právě na základě tohoto zákona. Struktura návrhu má navíc svůj předobraz i v současném znění zákona č. 181/2014 Sb., o kybernetické bezpečnosti a zákona č. 240/2000 Sb., krizový zákon, přičemž poznatky z jeho čitelnosti a problémů adresátů s jeho pochopením byly předobrazem úprav, které návrh zákona obsahuje. Jak vyplývá z připomínek níže, pokud by i přesto přetrvávaly problémy s jeho budoucí aplikací, je zde Úřad tak jako doposud k dispozici pro pomoc s jeho výkladem. V případě hodnocení dodavatelského řetězce už ani současný návrh nepočítal s výlučnou působností NÚKIB, jak připomínka uvádí. Do procesu jsou zapojeny další subjekty státní správy, zejm. pokud je jejich působnost spojena s bezpečností České republiky. V průběhu tohoto mezirezortního připomínkového řízení byly zmíněné procesy opět přezkoumány a návrh dále upraven. Připomínkové místo s vypořádáním souhlasí.

306. Svaz měst a obcí České republiky	Z	Vnímáme snahu předkladatele o zajištění co nejvyšší pružnosti co do případných legislativních změn této oblasti, je však ale nemyslitelné, aby některé otázky byly řešeny v podzákoných právních předpisech [viz např. okruh povinných subjektů a zařazení obcí mezi ně versus právo na samosprávu dle čl. 100 Ústavy ČR ve spojení s § 7 zákona č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů]. Obcím jsou tak ukládány povinnosti v samotném důsledku až podzákoným právním předpisem. <i>Navrhujeme provést změny ve smyslu výše uvedeného, a to tak, že všechny zásadní legislativní otázky budou řešeny přímo v návrhu, nikoliv v podzákoných právních předpisech, tj. včetně, nikoliv výlučně, povinných subjektů.</i>	ROZPOR Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech [§ 3 a § 2 písm. d)], tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby [§ 3, ve spojení s § 2 písm. i) a k) a § 22a]. Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon [§ 4 odst. 1 písm. d) se spojení s § 2 písm. i), k), l) a m)], a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá [§ 3 a § 2 písm. b)]. Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Reakce připomínkového místa: Vyjádření předkladatele k připomínce obsahuje zejména srovnání s předchozí právní úpravou, nikterak však nesouvisí s nově předloženým návrhem. Nelze se ztotožnit s tvrzením, že konkrétní okruh

			povinných subjektů je v samotném důsledku definován podzákoným právním předpisem. JE PONECHÁN ROZPOR.
307. Svaz měst a obcí České republiky	Z	Současně v návrhu zcela absentuje srovnání s implementací směrnice NIS2 s ostatními státy EU a není ani řádně odůvodněno, proč je v řadě případů postupováno nad rámec stanovený směrnicí NIS2 (viz dodavatelský řetězec či vymezení povinných subjektů). <i>Navrhujeme doplnit materiál o jasné vyjádření důvodů u jednotlivých ustanovení včetně důvodové zprávy, které předkladatele vedly</i>	ROZPOR Vysvětleno 1. V části připomínky týkající se srovnání implementace směrnice NIS2 v České republice a ostatních členských státech je možné uvést, že od

		<i>k formulování daného návrhu nad rámec povinností dle směrnice NIS2 (natož, když nejsou zajištěny finanční, věcné ani personální prostředky na realizaci návrhu).</i> <i>Navrhujeme provést srovnání navrhované implementace v ČR s dalším státy EU a doplnit v tomto směru důvodovou zprávu.</i>	počátku přípravy návrhu nového zákona docházelo k monitorování stavu implementace. V druhé polovině roku 2022 provedl NUKIB konzultace se zástupci relevantních úřadů ve vybraných členských státech Evropské unie. Po jednání se zástupci Slovenska, Polska, Rakouska, Německa, Slovinska, Francie a Estonska (jak je uvedeno také v Závěrečné zprávě RIA, s. 72), v tomto období bylo obecným závěrem, že žádný z těchto členských států s implementací směrnice NIS2 nezačal. Nebylo tedy co srovnávat. Podle aktuálních veřejně dostupných informací (např. zde https://www.twobirds.com/en/trending-topics/cybersecurity/nisd-tracker?fbclid=IwAR0wGu2HVeEjEjrvuWlWmxJoEH-W_WltHTR2OIAZdic9CUHQKIltnNVADQ0) začalo přípravu transpozice jen několik členských států, jejichž postup je aktuálně v případě návrhu (tj. fáze konzultace). Většina členských států ani žádné veřejné kroky ani v tuto chvíli ještě nezahájila. K části připomínky týkající se odvětví Veřejná správa - odůvodnění zařazení obcí mezi poskytovatele regulovaných služeb je součástí odůvodnění vyhlášky o regulovaných službách, které projde vlastním mezirezortním připomínkovým řízením. V současné době je toliko ve formě tezí. Nicméně k vámi namítanému lze sdělit následující: Směrnice NIS2 poprvé přichází s požadavkem na regulaci veřejné správy. V rámci svého rozsahu pak má regulace dopadat na veřejnou správu na ústřední a regionální úrovni. V současné době je veřejná správa již široce regulována prostřednictvím významných informačních systémů a v značné míře tak nová podoba okruhu povinných osob v rámci odvětví veřejné správy odpovídá původnímu nastavení vyhlášky o významných informačních systémech. V

		rámci této vyhlášky měly dlouhodobě obce z důvodů uvedených ve vaší připomínce výjimku. S ohledem na současnou situaci na poli kybernetické bezpečnosti, a tedy, že právě místní samosprávy jsou stále častějším cílem hackerských útoků, a že se jedná o osoby, které jsou svým okruhem služeb nejbližší samotným občanům, by bylo ignorování významu obcí s rozšířenou působností do budoucna naprosto neudržitelné a nekonceptní. Oproti vyhlášce o významných informačních systémech, které byly zabezpečovány na úroveň více se blížící současnému okruhu vyšších povinností, je nyní majorita obcí s rozšířenou působností zahrnuta mezi poskytovatele regulovaných služeb v režimu nižších povinností, které představují skutečné minimální zabezpečení. Stát i prostřednictvím obcí s rozšířenou působností pracuje s daty svých občanů, kteří, pokud potřebují se státem komunikovat, si nemohou vybrat, zda státu tato svá data poskytnou, měl by tedy s těmito daty nakládat se závazkem k zajištění alespoň minimální úrovně jejich zabezpečení. 2. Vojenský průmysl byl nad rámec odvětví uvedených ve směrnici NIS2 do vyhlášky doplněn zejména proto, že se jedná o odvětví, které má z hlediska bezpečnosti státu významný dopad a rovněž je to odvětví, které by se vzhledem k výluce národní bezpečnosti z dosahu práva Evropské unie nikdy nemohlo a nemělo objevit jako regulované odvětví ze strany samotné Evropské unie, tedy jeho zařazení by mělo vždy náležet jako varianta toliko členským státům. Jedná se rovněž o odvětví, které má v rámci České republiky dlouhodobě značný význam v rámci národního hospodářství a vzhledem k regulaci dalšího množství odvětví by působilo disproporčně, kdyby

			takto stěžejní odvětví nebylo součástí regulace kybernetické bezpečnosti. 3. V případě mechanismu prověřování dodavatelského řetězce lze uvést, že ten byl do zákona vložen nad rámec transpozice s ohledem na pověření uložené Úřadu usnesením č. 41 Bezpečnostní rady státu ze dne 21. 6. 2022. Tímto usnesením se Úřadu ukládá předložit návrh zákona upravujícího regulaci dodavatelského řetězce. Mechanismus je součástí návrhu zákona proto, že využívá stejné instituty, pojmy a dopadá na stejnou množinu povinných osob (poskytovatelé strategicky významných služeb, hodnocení aktiv a další). Zároveň s tím mechanismus navazuje a doplňuje transponované povinnosti povinných osob v oblasti řízení dodavatelů. Reakce připomínkového místa: Ad) 1 K tomu ze strany připomínkového místa nezbyvá než dodat, že je otázka vhodnosti za současného tristního stavu veřejných financí zaujímat takto urychlený postup se závažným dopadem na soukromý i veřejný sektor. Opět zdůrazňujeme, že ze strany předkladatele nebyla předložena žádná analýza počtu bezpečnostních incidentů, k nimž došlo za určitý časový úsek ve vztahu k municipalitám. Jakákoliv argumentace je pak bez jakékoliv pádné opory a gold-plating tak není odůvodněn. Předkladatel nezohledňuje ani stav na trhu práce, ani stav veřejných financí. Jakákoliv právní úprava podzákonými právními předpisy ve vztahu k definici, resp. upřesnění povinných subjektů je nepřijatelná. JE PONECHÁN ROZPOR.
308. Svaz měst a obcí České republiky	Z	Současně je dlužno dodat, že s ohledem na rozsah návrhu, jenž je nabobtnán o související právní předpisy (jak teze prováděcích	ROZPOR

	předpisů, tak prováděcí zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti), je Svaz toho názoru, že lhůta pro mezirezortní připomínkové řízení (jež probíhá v době letních prázdnin, státních svátků a dovolených) měla být zvolena odlišně, přinejmenším s předchozí konzultací k paragrafovému znění s dotčenými připomínkovými místy, byť například neformální cestou. Neformální prodloužení lhůty k podání připomínek k návrhu připsan ze strany NÚKIB ze dne 03.07.2023 a rozsah připomínek řady připomínkových míst pouze potvrzuje výše uvedené, a to celkovou neprodiskutovanost a nepřipravenost návrhu. <i>Navrhujeme, aby návrh jako celek byl podroben odborné diskuzi a byl přepracován ve smyslu uplatněných připomínek po širší diskuzi s připomínkovými místy, včetně analytického vyjádření nákladů na realizaci návrhu a předpokládaného finančního zajištění.</i>	Neakceptováno Lhůta pro mezirezortní připomínkové řízení byla zvolena standardním způsobem v souladu s Legislativními pravidly vlády a harmonogramem stanoveným pro projekt přípravy nového zákona o kybernetické bezpečnosti. Veřejnost byla o projektu transpozice směrnice NIS2 a následně vzniku nového zákona o kybernetické bezpečnosti informována průběžně již od roku 2021. V první řadě byla odborná veřejnost informována o možnosti zapojit se na stránkách úřadu (https://www.nukib.cz/cs/infoservis/aktuality/1748-narodni-urad-pro-kybernetickou-a-informacni-bezpecnost-nukib-vyzyva-odbornou-verejnost-k-zasilani-navrhu-na-zmeny-zakona-c-181-2014-sb-o-kyberneticke-bezpecnosti/) a https://www.nukib.cz/cs/infoservis/aktuality/1831-nukib-vyzyva-odbornou-verejnost-k-zasilani-navrhu-na-zmeny-zakona-c-181-2014-sb-o-kyberneticke-bezpecnosti/), dále úřad spustil osvětovou internetovou stránku nis2.nukib.cz, v rámci které vyzýval veřejnost k zapojení se, a ještě před začátkem mezirezortního připomínkového řízení se obrátil na veřejnost s žádostí o zasílání podnětů, přičemž zveřejnil první verzi návrhů budoucí právní úpravy. Svaz měst a obcí byl nad to adresně osloven dopisem ze dne 12. září 2022, č. j. 9959/2022-NÚKIB-E/350 prostřednictvím datové schránky, s nabídkou spolupráce a pozvánka na společné setkání nad tématem směrnice NIS2, na kterou nereagoval. Touto optikou je návrh podroben odborné diskuzi těch, kteří se zapojili již dlouhodobě, a není proto důvod rozšiřovat diskuzi nad rámec aktuálně probíhající nebo formálně požadované Legislativními pravidly vlády.

			Reakce připomínkového místa: S ohledem na celkový rozsah připomínek k návrhu a současně s ohledem na závažnost těchto připomínek není možné se s argumentací předkladatele ztotožnit. Současně je na místě doplnit, že Svaz informoval své členy o možnosti se vyjádřit a zasílat podněty dle návrhu předkladatele. Nicméně veřejnost se tak mohla vyjádřit k NIS2, nikoliv k paragrafovému znění zákona v závěrečné verzi. Konečně, předkladatel ve svém vyjádření k připomínce neřeší připomínku samotnou. JE PONECHÁN ROZPOR.
309. Svaz měst a obcí České republiky	Z	K bodu 3.4 Územní dopady na územní samosprávné celky: Navrhujeme, aby se v tomto bodě zmínila i nutnost dotčených územních samosprávných celků vypořádat se s novými povinnostmi, resp. jejich plněním, personálně, věcně, technicky i finančně. K tomu je nezbytné přidat i pomyslné za b), a to že odborníků v oblasti kyberbezpečnosti je v ČR velice málo (zcela absentuje vyjádření odhadovaného počtu odborníků na oblast kyberbezpečnosti a volných pracovních sil) a možnost platové nabídky územních samosprávných celků je pro tyto pracovníky nesrovnatelná se soukromým sektorem. K tomu je nezbytné přidat i pomyslné za c), a to že je plánováno snížení příspěvku na výkon přenesené působnosti, kdy již nyní obce v mnohém na výkon této služby pro stát doplácí. Je více než zjevné, že tak budou i jejich finanční možnosti zkráceny a omezeny. Z uvedeného tak jednoznačně vychází, že nároky na zajištění povinností, jež jsou nad rámec Směrnice NIS2, jsou nepřiměřené, s čímž lze propojit i fakt, že municipality NEMUSÍ BÝT dle Směrnice NIS2 povinným subjektem.	ROZPOR Neakceptováno Dopad na veřejné rozpočty je vysvětlen v části 3.1., kde je nejdůležitější věta "jen regulovaná organizace samotná by měla být schopná identifikovat své vlastní náklady na zavedení a udržování přiměřené úrovně kybernetické bezpečnosti". Úřad nemůže vyčíslovat finanční nákladnost návrhu u jednotlivých ÚSC, protože např. některá obec má svoje vlastní odpadové hospodářství a jiná obec tuto agendu kompletně svěřila soukromé společnosti, která není touto obcí zřízena. Rovněž se významně liší úroveň zavedených opatření, což je zejména ve vztahu k režimu nižších povinností výrazně rozhodující stran nutných nákladů. Jak správně navrhovatel podotýká, směrnice NIS2 neuvádí, že by municipality ve všech členských státech musely být povinnými osobami, mluví pouze o regulaci veřejné správy na úrovni státní (ústřední) a regionální, což odpovídá povaze NIS2 jako směrnice a také navazuje na významnou rozdílnost jednotlivých

	Shodně tak k tomuto navazuje i vyhodnocení možných variant řešení (viz bod 2. Závěrečné zprávy z hodnocení dopadů regulace), kdy je na místě zvažovat alespoň Variantu II (minimální transpozice směrnice) či Variantu III (Transpozice směrnice bez zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce, ovšem při odstranění zjištěných nedostatků a reflexe dosavadních zkušeností). Stranou nelze ponechat ani plánované navýšení pracovních míst jak na úrovni municipální, tak ale i na úrovni jiných orgánů veřejné moci, jež budou povinnými subjekty (viz např. bod 7.1.6 Shrnutí dopadů na státní rozpočet a ostatní veřejné rozpočty). S ohledem na cíl snížit byrokratické zatížení státu a municipalit včetně s tím souvisejícího personálního zatížení se pak návrh stává vnitřně rozporným (srovnej viz znění návrhu nad rámec stanovený Směrnicí NIS2 a s tím spojené personální, věcné i finanční zatížení dotčených subjektů). <i>Navrhujeme zvážení doplnění RIA a Závěrečné zprávy ve smyslu zvážení personálního zajištění plnění povinností dle návrhu dotčenými municipalitami (včetně zajištění metodického proškolení příslušných zaměstnanců) a s tím spojenými zvýšenými náklady včetně jejich řádové definice (nejen personálními, ale ve smyslu zvolené varianty řešení i věcnými – viz prověřování dodavatelského řetězce).</i> <i>Již v tomto okamžiku navrhujeme vypořádat se se skutečností, proč jsou municipality zavedeny jako povinné subjekty nad rámec Směrnice NIS2.</i> <i>Závěrem navrhujeme doplnit Závěrečnou zprávu a RIA o hodnocení faktické proveditelnosti povinností nastavených návrhem pro jednotlivé povinné subjekty včetně municipalit (z různých aspektů – personálních, finančních, věcných, technických atd.).</i> RIA a Závěrečná zpráva se tak vůbec nevyrovnává s dopady návrhu na regionální úrovni – více viz níže.	úprav soustavy veřejné správy napříč členskými státy. Ne ve všech členských státech mají municipality svěřenu tzv. přenesenou působnost (jak ji známe v ČR, ostatně ČR původně rovněž dnešní přenesenou působnost realizovala formou okresních úřadů), ale právě tato přenesená působnost je primárním důvodem regulace obcí s rozšířenou působností. Nároky kladené na ÚSC, tedy povinnosti v nižším režimu jsou nezbytné a zcela přiměřené agendě, kterou tyto v přenesené působnosti zajišťují, která je tím, co je ze strany obyvatelstva nejčastěji potřeba. Právě proto do regulace primárně nespádají všechny ÚSC, ale pouze ORP a kraje. V režimu nižších povinností, kam budou spadat po úpravě vyhlášky o regulovaných službách všechny ORP, budou náklady na zajištění povinností dle návrhu významně nižší, než jaké by byly, pokud by např. tyto obce měly zavádět opatření na úrovni významných informačních systémů dle současně platné úpravy. Nezařazení obcí vykonávajících významnou správní agendu v situaci, kdy právě obce jsou jedním z významných cílů kybernetických útoků, protože mají velké množství agendy a užitečných dat, by bylo ze strany státu nezodpovědné vůči zajišťování základních potřeb občanů, které tyto realizují nejčastěji a nejběžněji právě prostřednictvím ORP. K připomínce ohledně personálního zajištění a proškolení zaměstnanců jednotlivých ÚSC lze toliko uvést, že toto nelze řešit paušálně, protože každý budoucí povinný subjekt je natolik specifický, že si toto bude muset řešit individuálně, nicméně Úřad již nyní mnohokrát po dohodě se Svazem prováděl osvětovou činnost právě směrem k obcím a v této činnosti hodlá i napříště pokračovat. Co se týče snížení příspěvku pro obce za výkon přenesené působnosti, to

			není bohužel něco, co by Úřad mohl ze své pozice ovlivnit. Reakce připomínkového místa: Jak již uvádíme výše, předkladatel se nevyrovnává argumentačně s připomínkou. Nelze se ztotožnit s postojem, že ani řádově nelze vyčíslit finanční dopady na municipality. Touto argumentací by bylo možné pak operovat v řadě legislativních návrhů. Srovnání v rámci jiných států není přiléhavé, když k argumentaci již předkladatel uvedl, že ze strany jiných států nebylo aktivně k implementaci ještě přikročeno. Opětovně zdůrazňujeme, že ze strany předkladatele nebylo ani vyjádřeno, v jakém rozsahu byly v určitém časovém úseku dotčeny municipality kybernetickými incidenty. JE PONECHÁN ROZPOR.
310. Svaz měst a obcí České republiky	Z	Lze současně konstatovat, že NÚKIB neprovedl řádně vyhodnocení dopadů na regulované subjekty. Není naprosto jasné, jaké konkrétní povinnosti dopadnou na obce, kraje, jimi zřizované organizace, jakým způsobem budou posuzovány dobrovolné svazky obcí atd. Není ani provedena analýza očekávaných nákladů (který by logicky navazovala na analýzu povinností, jež budou nově povinným subjektům uloženy). <i>Navrhujeme provedení analýzy nákladů pro jednotlivé povinné subjekty.</i>	ROZPOR Neakceptováno Úřad provedl hodnocení dopadů dostatečným způsobem a závěry prezentované v důvodové zprávě a zprávě hodnocení dopadů odpovídají nejpřesnějšímu možnému závěru, jaký je v této věci možné učinit. Jak je v důvodové zprávě uvedeno, množství proměnných vedlo po několika letech a odhadech finančních nákladů prováděných při přijímání právních předpisů v oblasti kybernetické bezpečnosti k závěrům, které jsou shrnuty ve zmíněné důvodové zprávě a hodnocení dopadů, i s obsáhlým komentářem. Není možné, aby kdokoliv jiný než samotná povinná osoba provedl analýzu nákladů ve větším detailu, než je v těchto dokumentech uvedeno, protože jenom samotná povinná osoba zná přesný rozsah služeb které poskytuje, zná svoje aktiva a zná svoji současnou

			úroveň zabezpečení z pohledu kybernetické bezpečnosti. Reakce připomínkového místa: Vypořádání připomínky se jeví vnitřně rozporným a nesrozumitelným. Odkazujeme na výše uvedené vyjádření. JE PONECHÁN ROZPOR.
311. Svaz měst a obcí České republiky	Z	Návrh se věnuje mimo implementace Směrnice NIS2 i úpravě “prověřování dodavatelského řetězce”. V žádném ohledu si nedovolujeme zpochybnit záměr státu prověřovat dodavatele do kritických částí infrastruktury. V RIA ani důvodové zprávě jsme ale bohužel nenalezli vyhodnocení dopadů na regionální podnikání především v sektoru elektronických komunikací, kterých se dotkne mechanismus nejvíce. Zároveň nevíme důvod, proč při měření dopadů na podnikatelské prostředí nepoužil NÚKIB Metodiku měření administrativní zátěže podnikatelů, která byla vládou schválena roku 2017 a která je závaznou metodikou pro analýzu dopadů regulace. Lze předpokládat, že v důsledku prověřování dodavatelského řetězce může dojít k řadě problémů s nevyčíslitelnými náklady, avšak na druhé straně bude na bedlivém zvážení, zda prověřování bude završeno kýženým výsledkem. Podle tezí vyhlášek budou mezi subjekty mechanismu prověřování patřit jen operátoři s více než 350 000 SIM karet nebo 100 000 aktivních pevných přípojek. Už 100 000 aktivních přípojek však znamená, že celá řada větších regionálních operátorů se stane subjektem mechanismu prověřování. Předkladatel se však nevypořádává v návrhu s vysokou mírou propojenosti sektoru pomocí dodavatelsko-odběratelských vztahů.	ROZPOR Neakceptováno Navrhovatel v připomínce navrhuje několik věcí. V první řadě analýzu dopadů na malé a střední podnikatele podle Metodiky měření administrativní zátěže. K tomu lze uvést to, že zmíněná úprava mechanismu prověřování dodavatelského řetězce nemá žádný vliv na administrativní zátěž pro malé a střední podniky. Byť se i jich může v případě, že budou zahrnuty do dodavatelských řetězců poskytovatelů strategicky významných služeb, nějakým způsobem navrhovaná úprava dotknout, administrativní zátěž, tedy řízení dodavatelských řetězců a hlášení bezpečnostně významných dodávek a dodavatelů, se dotkne pouze poskytovatelů strategicky významných služeb. Mezi ně žádný malý či střední podnikatelský subjekt není v navrhované úpravě zařazen. Dále navrhovatel navrhuje zúžení rozsahu mechanismu pouze na kritickou část sítě a vyjmutí okrajových a transportních částí sítě. Okrajové a transportní části sítě jsou zahrnuty do rozsahu vyhláškou o nepominutelných funkcích. Nepominutelné funkce stanoví, společně s aktivy

	Celá řada národních operátorů má jako dodavatele regionální hráče různé velikosti, na které se formálně mechanismus nebude vztahovat, ale protože “kritickou částí stanoveného rozsahu” je dle návrhu vyhlášky o nepominutelných funkcích fakticky celá síť, budou regulovanými subjekty i desítky malých a středních firem, protože se stanou dodavateli a jejich dodavatelé subdodavateli. Jejich obchodní partneři na ně mohou vyvíjet tlak na výměnu dodavatele, pokud jej předkladatel označí za vysoce rizikového. Výsledkem se pak zcela bez pochyb může stát, že namísto budování vysokorychlostního internetu v obcích pro co největší množství zákazníků z řad domácností, firem i veřejné správy, budou nuceni investovat do výměny řešení, která jsou plně funkční, jen jsou postavené na technologiích od dodavatelů, které předkladatel považuje za vysoce rizikové, a to aniž by byli sami tito dodavatelé regulovaným subjektem. Toto je vážný důsledek regulace vyjádřené v návrhu, který vůbec nevidíme zohledněný v důvodové zprávě a v RIA. Významně v obou dokumentech chybí zhodnocení, jak implementace směrnice i mechanismus budou mít vliv na investice především do míst s nízkou návratností, jako jsou malé obce (mediánová velikost obce v ČR je přibližně 380 obyvatel). Předkladatel by tak měl bezesporu zohlednit na jedné straně nutnost zajištění bezpečnosti sítí, ale na straně druhé rozvoj regionů a vliv na podnikatelské prostředí především malých a středních regionálních a lokálních podniků. Jen tak je možné zhodnotit, zda je rozsah a forma regulace proporcionální problému, který chce předkladatel řešit především co se týče národní úpravy, která nevyplyvá z nutnosti implementace Směrnice NIS2. <i>Svaz tak navrhuje, aby NÚKIB provedl RIA podle postupů, které předpokládají legislativní pravidla vlády (tedy především analyzoval dopad na podnikatelské prostředí podle příslušné metodiky). Zásadní</i>	určenými samotnou povinnou osobou, množinu aktiv, na kterou dopadají povinnosti mechanismu prověřování bezpečnosti dodavatelského řetězce. Nepominutelné funkce do analýzy rizik, resp. řízení aktiv dle vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, nezasahují, ale pouze ji doplňují. Tyto funkce jsou důležité z důvodu značné komplexity veřejných komunikací a jejich tzv. kaskádovitého efektu, tedy přímého dopadu na další strategicky významné služby, které jsou na telekomunikacích závislé. Z toho důvodu NÚKIB ve vyhlášce určuje funkce, které musí být považovány za kritické z hlediska jejich dopadu na funkčnost sítí, a to nehlédě na jejich umístění v rámci architektury sítě. K namítanému dopadu na municipality lze uvést to, že mechanismus prověřování dodavatelských řetězců na municipality nedopadá. K poslední připomínce v rámci mechanismu prověřování dodavatelského řetězce lze uvést to, že je-li orgán veřejné správy pouze uživatelem strategicky významné služby, jejímž poskytovatelem je jiný orgán veřejné správy, neplynou mu z návrhu mechanismu žádné povinnosti. Reakce připomínkového místa: Svaz navrhuje, aby byla důvodová zpráva doplněna s ohledem na výše uvedené o výslovné určení, že byt' bude daná municipalita využívat ve svých systémech prostředky, které nebudou souladné s prověřováním dodavatelského řetězce, nebude stížena žádnými povinnostmi a bude moci dále stanovené systémy využívat.

		<i>je především zpracovat dopad na regionální poskytovatele internetu jako možné subjekty mechanismu z důvodu, že jsou dodavateli velkých subjektů.</i> <i>Dále Svaz navrhuje, aby se regulace týkala skutečně jen “kritické části” sítě poskytovatelů a nedopadala na okrajové části sítě a transportní část sítě, což jsou právě ty části, které pro velké národní operátory poskytují menší regionální a lokální hráči formou velkoobchodních dodávek služeb. V tomto ohledu považujeme za žádoucí změnit § 28 a navazující ustanovení návrhu a příslušnou vyhlášku.</i> <i>Opětovně zdůrazňujeme, že Svaz je přesvědčen, že není důvod, aby mezi povinné subjekty byly zařazeny municipality. Proto navrhuje, aby i s tímto postupem nad rámec implementace Směrnice NIS2 se předkladatel důkladně vypořádal a zohlednil všechny vstupní faktory včetně externalit.</i> <i>Konečně, není ani vysvětleno, zda v případě, kdy veřejná správa je pouze uživatelem regulované služby a poskytovatelem jsou jiné ústřední orgány státní správy, budou pro danou veřejnou správu plynout nějaké povinnosti.</i>	JE PONECHÁN ROZPOR.
312. Svaz měst a obcí České republiky	Z	K bodu 7.2. Důvodové zprávy: Tento bod se zabývá dopady na územní samosprávné celky (dále jen „ÚSC“) ve vztahu ke směrnici NIS2. NIS2 jednoznačně stanovuje, že regulovány mají být nově ty subjekty veřejné správy na regionální úrovni, pokud tak budou v rámci národní právní úpravy stanoveny (konkrétně viz článek 2 Směrnice NIS2, písm. f), který zní: „subjekt je subjektem veřejné správy: i) <u>ústřední vlády, jak je vymezena členským státem podle vnitrostátního práva; nebo ii) na regionální úrovni, jak je vymezena členským státem podle vnitrostátního práva, a na základě posouzení rizik poskytuje služby.</u>	ROZPOR Neakceptováno Obce s rozšířenou působností (ORP) nejsou do regulace zahrnuty nad rámec směrnice NIS2, ale zcela v souladu s touto směrnicí. Je to z toho důvodu, že ne ve všech členských státech mají municipality (obdoby ORP a krajů) svěření tzv. přenesenou působnost (jak ji známe v ČR), kdy právě tato přenesená působnost je hlavním důvodem pro zařazení ORP do regulace. Nároky kladené na ORP, tedy primárně nižší úroveň povinností, jsou nezbytné a zcela přiměřené agendě, kterou tyto v přenesené působnosti zajišťují. Právě

	<u>jejichž narušení by mohlo mít významný dopad na kritické společenské nebo hospodářské činnosti.</u>“). Nově jsou stanoveny povinnými subjekty obce s rozšířenou působností s tím, že je tento postup odůvodněn současnými trendy a zkušenostmi a jsou zařazeny do režimu nižších povinností (vyjma dotčených municipalit, jež spadají do režimu vyšších povinností). V žádném z podkladů však není řádně zdůvodněno, z jakého důvodu se k tomuto kroku, tj. k zahrnutí ÚSC, přistoupilo. Je vágně uvedeno, že došlo k v některých obcích ke kybernetickým bezpečnostním incidentům, což není ale číselně (ani řádově) podepřeno (tj. v kolika případech a s jakou závažností pro určitý časový horizont) a není tak určeno, zda se nejedná pouze o marginální záležitost, zejména s ohledem na náklady, které budou ÚSC nuceny vynaložit na realizaci svých povinností dle návrhu (odhlížeje od absence personálních kapacit, finančních a věcných prostředků, návaznosti na prověřování dodavatelských řetězců a z toho možných důsledků atd.). Jednoznačně se tak nabízí, aby byla důvodová zpráva (a v této souvislosti i RIA jako celek) v tomto směru řádně doplněna a bylo vyjádřeno, jakým způsobem a v jaké míře byly ÚSC dosud dotčeny kyberbezpečnostními incidenty a jaká je relevance těchto incidentů k tomu, aby byly ÚSC zařazeny nad rámec Směrnice NIS2 mezi povinné subjekty. Jejich zařazení i s ohledem na s tím spojené nároky na prověřování a další aktivity není plně odůvodněno. <i>Navrhujeme doplnění důvodové zprávy dle výše uvedeného a odůvodnění zařazení ORP mezi povinné subjekty.</i> <i>Současně opětovně v této chvíli (a následně dále v textu) se ohrazujeme proti zařazení ORP, resp. ÚSC jako celku mezi povinné</i>	proto do regulace nespádají všechny obce, ale pouze ORP. Jak je v důvodové zprávě uvedeno, je pouze zrušena výslovná výjimka oproti současné právní úpravě, kdy jsou všechny typy obcí mimo regulaci. Posláním důvodové zprávy není informovat o všech kybernetických incidentech, které se vztahují k tomu kterém odvětví, proto považujeme současné odůvodnění v tomto ohledu za dostatečné. Nicméně před meziresortním připomínkovým řízením týkajícím se samotné vyhlášky o regulovaných službách dojde v tomto ohledu k doplnění důvodové zprávy, která zejména detailněji popíše, že jsou ORP v rámci státu právě těmi, kdo občanům zajišťují kontakt se státem nejčastěji. Vzhledem k rozsahu služeb, které ORP v přenesené působnosti poskytují, je zcela zřejmé, že narušení dostupnosti, důvěrnosti nebo integrity informací by ohrozilo poskytování těchto služeb. K zmíněnému zařazení obcí mezi subjekty, kterých se dotýká prověřování dodavatelského řetězce bychom rádi uvedli, že ORP se tato povinnost dotýkat nebude. Reakce připomínkového místa: S ohledem na již vyjádřené výše ze strany připomínkového místa JE PONECHÁN ROZPOR.

		<i>subjekty nad rámec směrnice NIS2 a navrhujeme jejich vynětí z návrhu jako celku.</i>	
313. Svaz měst a obcí České republiky	Z	K § 2 návrhu: Ustanovení § 2 návrhu je věnováno vymezení pojmů, avšak nejsou zahrnuty veškeré pojmy, jež se v návrhu objevují, a řada z nich není nikde ani dílčím způsobem vysvětlena. Příkladem lze uvést pojmy spojené s dodávkami a dodavateli – viz dodavatel bezpečnostně významné dodávky a bezpečnostně významná dodávka (viz § 32) a další. Ostatně, návrh jako celek operuje řadou nepřesných a vágních pojmů a cílem by mělo být tyto nepřesnosti odstranit. <i>Navrhujeme, aby byl návrh podroben revizi a neosvětlené pojmy použité v návrhu byly v rámci § 2 osvětleny tak, aby i laik byl s to pochopit, co je myšleno jednotlivými vyjádřeními.</i>	ROZPOR Neakceptováno Zmíněné pojmy jsou definovány vždy pro potřeby použití v dané části zákona, v tomto případě konkrétně pro potřeby využití v mechanismu prověřování dodavatelského řetězce. Oba zmíněné pojmy jsou v §32 popsány a vysvětleny tak, aby jejich využití v mechanismu prověřování dodavatelského řetězce bylo jasné a bezproblémové. Jejich definování na úrovni §2 (Definice) není účelné, neboť návrh zákona jako takový nemá ambici ani potřebu definovat tyto pojmy mimo specializovaný prostor, kde je tomu potřeba (tj. pro potřeby mechanismu prověřování dodavatelského řetězce). Reakce připomínkového místa: Nesouhlasíme s vypořádáním a odkazujeme na již výše uvedenou nepřehlednost a nejasnost návrhu jako celku, což se tímto pouze potvrzuje. Případně navrhujeme, nechť předkladatel v rámci § 2 zakotví ustanovení, že ostatní pojmy jsou definovány napříč celým zákonem, příp. v prováděcích předpisech. JE PONECHÁN ROZPOR.
314. Svaz měst a obcí České republiky	Z	K § 2 odst. 1 písm. e) návrhu: Je naprosto potřebné zpracovat a stanovit postup k hodnocení významnosti regulované služby, váhu, hodnocení parametru (dopadu) a stanovit model výpočtu, popřípadě stanovit model analýzy tak, aby bylo zřejmé s ohledem na právní jistotu a regulační jistotu, co je	ROZPOR Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných

		regulovanou službou. Vyjádření v podzákoně právním předpise se jeví naprosto nevhodným. <i>Navrhujeme zapracování dle výše uvedeného do návrhu.</i>	osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech (§ 3 a § 2 písm. d)), tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby (§ 3, ve spojení s § 2 písm. i) a k) a § 22a). Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon (§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)), a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá (§ 3 a § 2 písm. b)). Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Reakce připomínkového místa: Opět uvádíme, že s ohledem na výše uvedené JE PONECHÁN ROZPOR.
315. Svaz měst a obcí České republiky	Z	K § 2 odst. 2 písm. c) návrhu: Výraz kybernetická hrozba se vyjma tohoto ustanovení v zákoně ani v prováděcích vyhláškách nevyskytuje a návrh dále s takovým výrazem nepracuje. <i>Navrhujeme vysvětlit zavedení tohoto pojmu v návrhu.</i>	ROZPOR Vysvětleno S pojmem kybernetické hrozby (nyní po úpravách již jen „hrozby“ nebo „významné hrozby“) pracují kromě § 2 např. § 16, § 18, § 20, § 21 a další. S tímto pojmem dále pracuje i návrh vyhlášky o bezpečnostních

			opatření poskytovatele regulované služby v režimu vyšších povinností. Reakce připomínkového místa: JE PONECHÁN ROZPOR.
316. Svaz měst a obcí České republiky	Z	K § 2 odst. 2 písm. f) návrhu: Ustanovení § 2 odst. 2 písm. f) návrhu stanovuje, že kybernetickým bezpečnostní incidentem se rozumí narušení bezpečnosti informací v rámci aktiv. Definice je však formulována nad rámec implementované směrnice, jež operuje s pojmem „incident“ bez bližšího vymezení. Není pak racionální důvod využívat sousloví dle dotčeného ustanovení návrhu, ale je naopak přiléhavé využít pojem definovaný směrnicí NIS2 a natož, pokud v návrhu je dále tento pojem využíván jen ve formě „incident“. <i>Navrhujeme respektovat pojmosloví směrnice a nahradit dotčený pojem pouze prostým „incident“.</i>	ROZPOR Neakceptováno Pojem "incident" je používán i v dalších právních předpisech, např. zákon č. 127/2005 Sb., o elektronických komunikacích, nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS) a nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR). S ohledem na uvedené je tedy žádoucí upřesnit, s jakým typem incidentu zákon pracuje. Reakce připomínkového místa: JE PONECHÁN ROZPOR.
317. Svaz měst a obcí České republiky	Z	K § 2 odst. 2 písm. g) návrhu: Dle dotčeného ustanovení návrhu je definováno zvládání kybernetického bezpečnostního incidentu úkony vedoucími k zajištění prevence, detekce, analýzy, omezení dopadů incidentu, reakce na incident a následného zotavení. Opětovně zdůrazňujeme, že ÚSC mají důvodné obavy ze zajištění dostatečného počtu odborníků a z finančního a materiálního zajištění.	ROZPOR Akceptováno jinak K problematice kybernetických bezpečnostních incidentů bude Úřad vydávat příslušné metodické materiály, které budou mít doporučující charakter. Tyto materiály budou, s ohledem na specifika každé organizace, zaměřeny obecně. Vzhledem k tomu, že řada povinných subjektů může mít postupy k hlášení/zvládání incidentů již zavedeny, bude způsob

		<i>Navrhujeme, aby byly zpracovány metodické pomůcky, vzorové dokumenty a jednoznačné postupy, jež by byly považovány za závazné pro povinné subjekty.</i>	použití metodických materiálů ponechán na uvážení povinných subjektů. Reakce připomínkového místa: JE PONECHÁN ROZPOR.
318. Svaz měst a obcí České republiky	Z	K § 4 a § 5 návrhu – rozdíl mezi identifikací a určením: Nadpisy u § 4 a § 5 jsou zmatečné, shodně tak obsah a vysvětlení jejich obsahu. Jednoznačný rozdíl mezi „identifikací“ a „určením“ je složitě pochopitelný. <i>Navrhujeme upřesnit znění dotčených ustanovení návrhu tak, aby byl jasný rozdíl mezi věcnou stránkou jednotlivých paragrafů.</i>	ROZPOR Akceptováno jinak K části připomínky odkazující na srozumitelnost návrhu viz výše. K části připomínky odkazující k rozdělení a obsahu pojmů identifikace služby a určení služby - úvodní ustanovení návrhu, stejně tak jako definiční ustanovení budou v průběhu tohoto mezirezortního připomínkového řízení upřesněny a upraveny. Reakce připomínkového místa: JE PONECHÁN ROZPOR – K DOVYSVĚTLENÍ PO DOPRACOVÁNÍ JEDNOTLIVÝCH DOKUMENTŮ.
319. Svaz měst a obcí České republiky	Z	K § 4 odst. 2 návrhu: V dotčeném ustanovení jsou stanovena kritéria pro identifikaci regulované služby jejich výčtem (nad rámec směrnice NIS2). Bohužel v návrhu je jejich vyjádření heslovité a z důvodové zprávy není zřejmé, co má být konkrétním obsahem jednotlivých odvětví (ani rámcově) s tím, že mají být prováděcím právním předpisem stanoveny kritéria pro identifikaci regulované služby. Jedná se o naprosto zásadní ustanovení, které určuje okruh subjektů, jichž se bude návrh dotýkat a které budou nuceny plnit povinnosti z návrhu vyplývající. Provázanost s velkým množstvím prováděcích předpisů pravděpodobně s cílem zaručení určité pružnosti v případě	ROZPOR Neakceptováno. Co se týče srozumitelnosti materiálu, máme za to, že jej není nutné přepracovávat. Struktura návrhu má navíc svůj předobraz i v současném znění zákona č. 181/2014 Sb., o kybernetické bezpečnosti, přičemž poznatky z jeho čitelnosti a problémů adresátů s jeho pochopením byly předobrazem úprav, které návrh nového zákona obsahuje. Pokud by i přesto přetrvávaly problémy s jeho budoucí aplikací, je zde Úřad tak jako doposud k dispozici pro pomoc s jeho výkladem. Jednotliví poskytovatelé regulovaných služeb plynule naváží na to, že byli správci kritické

	nezbytnosti další právní úpravy však spíše způsobuje zmatky, nejasnosti a zejména právní i regulační nejistotu. V tomto bodě se ani návrh, ani důvodová zpráva, ani návrh tezí prováděcích právních předpisů nevypořádává s otázkou, jak budou posuzovány dobrovolné svazky obcí, místní akční skupiny a další obdobné entity. <i>Navrhujeme, aby byl návrh upřesněn v definici identifikace regulované služby a důvodová zpráva byla doplněna o vysvětlení použitých pojmů aspoň demonstrativním výčtem.</i> <i>Navrhujeme, aby z návrhu byly vypuštěny ÚSC ve všech směrech jako celek. Pokud by nebylo této připomínce vyhověno, požadujeme, aby bylo stanoveno, jakým způsobem bude personálně, finančně a technicky zajištěna kontinuální činnost ÚSC a plnění povinností uložených na bedra ÚSC ze strany státu, jenž je takto nad rámec unijní legislativy stanovuje povinným subjektem.</i> K poslednímu návrhu ještě podotýkáme, a v tomto mj. Svaz vystupuje konzistentně, že v případech, kdy stát legislativně ukládá jakékoliv povinnosti ÚSC, musí zvažovat jejich užší (finanční, věcný, personální) dopad, ale i dopad v širším pohledu (v daném případě dodavatelské služby v této oblasti, nepokrytí vysokorychlostním internetem území ČR jako celku, fungování vyloučených lokalit, vylidňování menších obcí a další), jenž je řešen v dalších dimenzích. Bohužel výsledky těchto úvah předkladatel ani se zárukami státu, že se bude podílet v jakékoliv formě na realizaci implementaci v úrovni ÚSC, nedemonstruje.	informační infrastruktury, významných informačních systémů nebo provozovatelé základní služby. Detailně jsou jednotlivá kritéria uvedena v připravované vyhlášce o regulovaných službách, kde se každý poskytovatel regulované služby bude moci identifikovat. Nadto Úřad hodlá pokračovat ve své metodické a osvětové činnosti a v rozhodném období chce samozřejmě napomáhat jistotě adresátů normy i zodpovídáním jednotlivých dotazů týkajících se jejich identifikace i dalších povinností, které budou poskytovatele regulovaných služeb vázat. Dobrovolný svazek obcí je samostatnou právnickou osobou (§ 49 zákona č. 128/2000), proto bude posuzován, v případě naplnění kritérií, jako samostatný poskytovatel regulované služby, a jako takový se bude muset i samostatně registrovat, to se týká i dalších organizací, které jsou zřízeny jednotlivými ÚSC. Pro informaci - dobrovolný svazek obcí (popř. jiný subjekt zřízený ÚSC) nemůže poskytovat regulovanou službu v odvětví veřejná správa, protože mu žádným zákonem není svěřen výkon pravomocí. Vypuštění ÚSC z regulace je již zodpovězena v odpovědích na další připomínky navrhovatele a problematika zajištění povinností je již rovněž řešena výše. Část připomínky týkající se vylidňování obcí, fungování ve vyloučených lokalitách, apod. není řešena, protože nesouvisí s navrhovaným předpisem. Reakce připomínkového místa: Předkladatel se nevypořádal s připomínkou – odkaz na předobraz předcházející právní úpravy není přiléhavý, shodně tak ani návrh výkladové pomoci. Zákon má být vždy připraven a vyhlášen tak, aby byl naprosto

			srozumitelný všem. V dalším odkazujeme na již uvedené. JE PONECHÁN ROZPOR.
320. Svaz měst a obcí České republiky	Z	K předchozímu pro doplnění jen dodáváme, že u bodu § 4 odst. 2 návrhu, dle písm. l) je stanovena jako regulovaná služba „Věda, výzkum a vzdělávání“ (dle návrhu Vyhlášky o regulovaných službách se jedná o bod 19.1 přílohy). Zde je již ale hovořeno o „výzkumné organizaci“ bez bližšího určení, jež dle Směrnice NIS2 pak spadají do režimu nižších povinností. Předkladatel však definoval výzkumnou organizaci tak, že mj. je poskytovatelem regulované služby v režimu vyšších povinností v případě, že většina prováděných výzkumných projektů je financována z více než 50 % z veřejných zdrojů. Opět se tak jedná o návrh zakotvení právní úpravy směřující nad rámec znění Směrnice NIS2, bez jakéhokoliv vyjádření dopadu takto navrhované právní úpravy a s jasným zatížením dotčených subjektů nad racionální vnímání (srovnej znění směrnice NIS2, Příloha II, Další kritická odvětví). <i>Navrhujeme provést implementaci plně v souladu se zněním Směrnice NIS2, nikoliv nad její rámec (vyvarování se goldplatingu obecně).</i>	ROZPOR Neakceptováno Výběr služeb a subjektů regulovaných v rámci odvětví 19. Výzkum a vývoj nad rámec požadavků směrnice NIS2 proběhl na základě vyhodnocení aktuální úrovně kybernetické bezpečnosti odvětví, posouzení strategičnosti a relevance subjektů, které by do regulace měly být zařazeny, a v neposlední řadě i po konzultaci se subjekty, na které regulace bude dopadat. Odvětví výzkumu a vývoje je strategickým odvětvím, v němž jsou jednak investovány nemalé veřejné prostředky, na jejichž ochraně má stát logický zájem, jednak v něm vzniká a je uchováváno obrovské množství strategicky cenných informací. Výsledky výzkumů jsou v posledních letech častým terčem kybernetických útoků, jež mají za cíl odcizit dosažené poznatky a využít je buďto komerčně (bez nutnosti financovat jejich legální opatření), nebo pro působení proti zájmům České republiky. S ohledem na skutečnost, že výzkumné instituce a vysoké školy soustřeďují v rámci svých kapacit nadkritické množství materiálních, lidských a finančních zdrojů potřebných pro dosahování průlomových poznatků, které přinášejí znalostní řešení socioekonomických výzev, je tak veřejný zájem na zajištění dostatečné úrovně jejich kybernetické bezpečnosti zcela zřejmý a odůvodněný. Zároveň však došlo k přehodnocení rozřazení regulovaných subjektů do jednotlivých režimů a také k redukci regulovaných osob. Došlo tedy k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1.

			Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji. Kritérium financování z veřejných zdrojů však zůstalo zachováno, a to právě za účelem ochrany veřejných prostředků investovaných do výzkumné činnosti. Reakce připomínkového místa: JE PONECHÁN ROZPOR – K DOVYSVĚTLENÍ PO DOPRACOVÁNÍ JEDNOTLIVÝCH DOKUMENTŮ.
321. Svaz měst a obcí České republiky	Z	K § 4 a § 5 návrhu ve spojení s návrhem vyhlášky o regulovaných službách: <i>Navrhujeme upřesnit odvětví veřejné správy, resp. povinné subjekty, v tom směru, zda se jedná o počet obyvatel na území obce s rozšířenou působností, tedy o počet obyvatel obce, nebo o počet obyvatel ve správním obvodu ORP.</i> <i>V této souvislosti je nezbytné a navrhujeme doplnit i upřesnění v jednotlivých odvětvích regulované služby, příkladmo v odvětví vodovody, kanalizace, odpadové hospodářství, technické služby a další, dle jakých kritérií (i ve spojení s dobrovolnými svazky obcí) dojde k dotčení návrhem a zahrnutí mezi povinné subjekty.</i> Důvodová zpráva je v tomto ohledu pojata velice laxně a nepřesně a s ohledem na míru zásahu do činnosti těchto subjektů by mělo být požadavkem právního státu s poukazem na princip právní jistoty jasně stanovit mantinely pro právní úpravu realizovanou návrhem a prováděcími právními předpisy.	ROZPOR Neakceptováno Pro lepší orientaci byla připomínka rozdělena do samostatných bodů: 1) Vyhláška o regulovaných službách uvádí, že se jedná o počet obyvatel obce s rozšířenou působností (ORP). Správní obvod ORP není nikde zmiňován, proto se k počtu obyvatel v tomto správním obvodu ORP nepřihlíží. 2) Jednotlivá kritéria pro identifikaci regulované služby jsou definována v příloze vyhlášky o regulovaných službách. Dobrovolný svazek obcí je samostatnou právnickou osobou (§ 49 zákona č. 128/2000), proto bude posuzován, v případě naplnění kritérií, jako samostatný poskytovatel regulované služby, a jako takový se bude muset i samostatně registrovat. 3) Není zřejmé, kterou část důvodové zprávy navrhovatel považuje za laxní a nepřesnou. Každý

			subjekt musí samostatně posoudit (tzn. obec samostatně, dobrovolný svazek obcí samostatně), zda naplňuje některé z kritérií pro identifikaci regulované služby dle vyhlášky o regulovaných službách, resp. přílohy této vyhlášky. Rovněž bychom rádi doplnili, že vyhlášky jsou spolu se zákonem toliko ve formě tezí, tedy detailní dopracování důvodové zprávy stejně jako textu těchto vyhlášek bude ještě následovat před jejich samostatným meziresortním připomínkovým řízením, který všechny prováděcí předpisy ještě čeká. Počítáme, že v mezidobě dojde k jejich dalšímu dopracování. Reakce připomínkového místa: JE PONECHÁN ROZPOR – předkladatel se opět nevypořádává s připomínkou – viz odst. 2 – mimo DSO je třeba se zabývat i nyní projednávanou novelou zákona č. 128/2000 Sb., o obcích a návrhem společenství obcí, shodně tak je třeba se věnovat otázce, kdy obce společně založí právní subjekt k řešení otázek vodovodů, odpadového hospodářství atd.
322. Svaz měst a obcí České republiky	Z	K § 5 návrhu: Dotčené ustanovení se zabývá kritérii pro určení regulované služby. Z navrhovaného znění není však patrné, zda kritéria jsou určena tak, že musí být splněna všechna najednou či nikoliv. Současně není ani určeno, do jaké míry musí být stanovena možnost ohrožení definovaných cílů v bodě b) dotčeného ustanovení. Uvedené nejasnosti nejsou vysvětleny ani v důvodové zprávě. <i>Navrhujeme doplnění jak samotného ustanovení, tak důvodové zprávy, aby bylo znatelné, jaké jsou podmínky pro splnění kritérii pro určení regulované služby.</i>	ROZPOR Akceptováno jinak K první části připomínky - podmínky jsou alternativní, tedy stačí ke splnění i jen jediná z nich [v právním textu je pro alternativní výčet standardně použita spojka "nebo", v tomto případě v § 5 písm. a) mezi body 3. a 4., stejně tak jako mezi písm. c) a d)]. K druhé části připomínky - ustanovení § 5 písm. b) je obrazem kritéria vycházejícího z nařízení vlády č. 423/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Toto kritérium má již dlouhou dobu

			zažitou praxi v posuzování a vždy bude nutné naplnění tohoto kritéria ze strany Úřadu řádně odůvodnit. Dojde k doplnění důvodové zprávy o bližší výklad k těmto pojmům. Reakce připomínkového místa: JE PONECHÁN ROZPOR – K DOVYSVĚTLENÍ PO DOPRACOVÁNÍ JEDNOTLIVÝCH DOKUMENTŮ.
323. Svaz měst a obcí České republiky	Z	K § 6 odst. 3 návrhu: Dotčené ustanovení se dotýká režimu poskytovatele regulované služby s tím, že v odst. 3 je dán odkaz na prováděcí právní předpis, v daném případě zejména na vyhlášku o regulovaných službách. S ohledem na princip právní a regulační jistoty není na místě, aby tak zásadní záležitost byla řešena v podzákonném prováděcím právním předpise. Navrhujeme, aby vyhláška o regulovaných službách včetně svých příloh, jež definují jednotlivé povinné subjekty, byly součástí návrhu, tj. zákona o kyberbezpečnosti. K tomuto odkazujeme na již výše uvedené a znění Směrnice NIS2 co do článku 2, odst. 2, písm. f), bodu ii), kdy implementaci předkladatel opět míří nad rámec Směrnice NIS2, a to bez prokazatelného důvodu. Dle kritérií navržených předkladatelem se do režimu vyšších povinností dostanou ÚSC Praha, Brno, Ostrava a Plzeň a do režimu nižších povinností všech 205 ORP. Dle přesvědčení Svazu postupuje v implementaci NÚKIB chybným způsobem. Před tím, než stanovuje ORP za subjekty podléhající návrhu, měl provést posouzení rizik, zda poskytují služby, jejichž narušení by mohlo mít významný dopad na kritické společenské nebo hospodářské činnosti a výsledek tohoto posouzení rizik promítnout do Důvodové zprávy a závěrečné zprávy RIA (viz již připomínka výše).	ROZPOR Neakceptováno Pro lepší orientaci byla připomínka rozdělena do samostatných bodů: 1) Smyslem prováděcích právních předpisů (v tomto případě vyhlášky o regulovaných službách) je upřesňovat, konkretizovat a podrobně rozvádět zákon, pokud to ústavní zákon (např. č. 2/1993, čl. 11, nebo čl. 39) nezakazuje. Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech (§ 3 a § 2 písm. d)), tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby (§ 3, ve spojení s § 2 písm. i) a k) a § 22a). Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon (§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)), a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá (§ 3 a § 2 písm. b)). Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními

		Navíc dle článku 5 Směrnice NIS2 je vztažení povinností vyplývajících ze směrnice na subjekty veřejné správy na místní úrovni zjevně dobrovolné (“členské státy <u>mohou</u> stanovit...”). ORP, stejně jako ostatní obce, poskytují ze zákona celou řadu služeb v samostatné působnosti, zároveň ale poskytují služby v přenesené působnosti státní správy, jako například evidenci obyvatel, vydávání občanských průkazů a pasů, vydávání řidičských průkazů, živnostenskoprávní agendu, vedení živnostenského rejstříku, silniční správní úřad, dopravní úřad a další. Zda by narušení těchto služeb mohlo mít významný dopad na kritické společenské nebo hospodářské činnosti, musí předkladatel odůvodnit před tím, než učiní obce povinnými osobami podle zákona (viz již připomínka výše k tomu, že není vysvětlena hierarchie požadavků v případě, kdy ÚSC je pouze uživatelem určité služby s vyhrazenými právy). Svaz k tomuto ustanovení považuje za nutné uvést, že není možné se vypořádat s nutností vypočítat dopad regulace na subjekty, kterých se zákon dotkne, odstavcem v následujícím znění: <i>“Nevýhodou otázky analýzy finančních dopadů na organizace, a to i mimo státní správu, je skutečnost, že distribuce nákladů na kybernetickou bezpečnost není plošná a že existuje informační asymetrie ve směru od subjektů samotných k regulačnímu orgánu (tj. jen regulovaná organizace samotná by měla být schopná identifikovat své vlastní náklady na zavedení a udržování přiměřené úrovně kybernetické bezpečnosti).”</i>, více viz RIA str. 2. NÚKIB měl po dobu několika měsíců, po které zákon připravoval, možnost tuto analýzu udělat různými způsoby, které doporučují vládní materiály, jako je např. “Měření celkových nákladů na plnění povinností vyplývajících z regulace”, případně ve spolupráci s organizacemi samospráv, jako je Svaz, Asociace krajů ČR či SMS ČR, vypočítat alespoň řádově náklady, které ORP vzniknou. Svaz se	předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. 2) Prokazatelným důvodem je zajištění kybernetické bezpečnosti a v návaznosti na to i dostupnost, důvěrnost a integrita těchto poskytovaných regulovaných služeb v oblasti veřejné správy. Je to z toho důvodu, že ne ve všech členských státech mají municipality (obdoby ORP a krajů) svěřenu tzv. přenesenou působnost (jak ji známe v ČR), kdy právě tato přenesená působnost je hlavním důvodem regulace. Nároky kladené na ÚSC jsou nezbytné a zcela přiměřené agendě, kterou tyto v přenesené působnosti zajišťují - jedná se o úroveň nižších povinností. Právě proto do regulace primárně nespádají všechny ÚSC, ale pouze ORP a kraje. Do vyššího režimu povinností bude po dalších diskuzích zařazena pravděpodobně jen Praha (a to kvůli tomu, že vystupuje zároveň i jako "kraj", vede se diskuze o zrušení hranice počtu obyvatel nad 125 tis. jako kritéria pro zařazení do vyššího režimu povinností. 3) S ohledem na výskyt a zvyšující se četnost kybernetických bezpečnostních incidentů v informačních systémech obcí se přístup směrnice NIS2 jeví minimálně jako diskutabilní. Posouzení rizik musí každý subjekt provést samostatně, protože nikdo jiný nezná nemůže komplexně posoudit aktiva,

	samozřejmě nebrání faktickému zajišťování kybernetické bezpečnosti na všech úrovních samospráv, nicméně formální regulace dle návrhu s sebou beze sporu ponese velmi významné náklady a produkuje personální i technické zvýšené nároky a opětovně a Svaz stále důrazněji upozorňuje, že stát povinnosti ukládá, ale nijak neinicuje sanování podmínek k jejich plnění (ani finančně, ani personálně, ani věcně). I vzhledem k tomu, že v předběžném návrhu rozpočtu na rok 2024 plánuje Ministerstvo financí zcela nepřijatelně snížení objemu prostředků na platy o 4 %, snížení stupnic platových tarifů pro všechny zaměstnance veřejného sektoru o 5 % a pětiprocentní snížení příspěvku na výkon státní správy ve vazbě na snížení stupnic platových tarifů pro rok 2024 (<u>na což jsme upozornili v dopise předsedovi vlády z 6. 6. 2023</u>), je třeba mít jasné podchyceno, kdo bude a v jaké podobě povinnou osobou podle zákona. Obce budou muset na tuto agendu vyčlenit zaměstnance. Ve vyhlášce stanovuje předkladatel požadavky na osoby odpovědné za kybernetickou bezpečnost a následně na stanovení konkrétních opatření, které budou povinné subjekty muset kontrolovat a provádět, což vše bude znamenat pro obce nemalé náklady. Svaz je povinován jménem svých členů vyjádřit důvodnou obavu, že stát na obce uvalí novou povinnost, aniž by zajistil její financování. Upozorňujeme, že obecně je v České republice nedostatek odborných pracovníků v oblasti IT, kdy podle různých veřejně dostupných dat chybí mezi 20 až 30 tisíci pracovníků. Sám předkladatel uvádí, že k plnění povinností vyplývajících z návrhu bude potřebovat vyšší desítky nových pracovních míst, kromě těch, které předpokládá v již schválené koncepci rozvoje úřadu. Další místa v odvětví kybernetické bezpečnosti budou bezpochyby poptávat nově kontrolované subjekty. Stát je přitom už nyní v oboru IT velmi špatně konkurenceschopný, podle <u>dat Českého statistického úřadu</u> v roce 2022 pobírali například analytici a vývojáři softwaru a počítačových aplikací ve mzdové sféře 87 tisíc Kč v porovnání s 52 tisíci Kč ve sféře platové. Předkladatel	která jsou nezbytná k poskytování regulované služby. Toto platí pro všechny regulované subjekty včetně veřejné správy (tedy i obcí a krajů). Další otázky problematizace výpočtů nákladů viz připomínka výše. Otázkou snižování objemu plateb státu jednotlivým ÚSC za služby poskytované v přenesené působnosti nebude Úřad zabývat, protože nijak nesouvisí s návrhem zákona. Co se týká zmíněné konzultace přístupu k regulaci je potřeba podotknout, že Svaz měst a obcí byl adresně osloven dopisem ze dne 12. září 2022, č. j. 9959/2022-NÚKIB-E/350 prostřednictvím datové schránky s nabídkou spolupráce a pozvánka na společné setkání nad tématem směrnice NIS2, na kterou nereagoval. Reakce připomínkového místa: Opět odkazujeme na již výše uvedenou argumentaci k obdobným připomínkám a jejich vypořádání ze strany předkladatele. Současně upozorňujeme, že Svaz je zájmovou organizací, jehož členy jsou nejen municipality, ale i jiné právnické osoby. A k tomu upozorňujeme, že Svaz využil nabídky NÚKIB a společně jsme uspořádali i webinář na téma NIS2. Proto se důrazně ohrazujeme vůči opakované argumentaci ze strany předkladatele ve směru nevyužití nabídky. A k tomu akcentujeme, že veškerá komunikace do doby zahájení MPŘ byla vedena ke směrnici NIS2, nikoliv k paragrafovému znění a se závaznými důsledky. JE PONECHÁN ROZPOR.

	by měl při tvorbě regulace zhodnotit i to, zda a jak ji vůbec bude mít u regulovaných subjektů, zvláště ve veřejné správě, kdo plnit. Kritérium ORP je navíc podle přesvědčení Svazu velmi špatně zvolené. ORP je v České republice 205 a velikost těch, které mají méně než 125 tisíc obyvatel, se pohybuje od necelých 107 tisíc (Liberec) až po např. 2700 (Konice). NÚKIB neuvažuje přímé dopady na spotřebitele, ale zároveň uvádí, že lze očekávat tlak regulovaných orgánů na promítnutí nákladů na zavádění bezpečnostních opatření do cen služeb. To znamená negativní vliv na spotřebitele. Úřad by měl do RIA doplnit odhad toho, jak bude tento potenciální vliv na ceny vypadat, protože regulované služby jsou v odvětvích, která zasahují velkou část společnosti, která je na ceny velmi citlivá (jde např. o energetiku, ale i telekomunikace). Sociální dopady jsou tak naprosto zjevné. Celá řada ORP se pohybuje kolem 5 tisíc obyvatel. Je úplně absurdní se domnívat, že obce této velikosti budou mít kapacity na formální plnění požadavků ze zákona a prováděcích právních předpisů, ač jde o regulovanou službu v režimu “nižších povinností”, avšak s enormním byrokratickým zatížením (více dále). <i>Na základě výše uvedeného požadujeme, aby předkladatel provedl posouzení rizik, zda obce poskytují služby, jejichž narušení by mohlo mít významný dopad na kritické společenské nebo hospodářské činnosti (viz již výše) a dle tohoto posouzení stanovil, která úroveň územních samosprávních celků je vhodná pro regulaci, pokud vůbec nějaká - zvláště s ohledem na to, že subjekty veřejné správy na místní úrovni (tedy města) nejsou ve směrnici uvedené jako povinné subjekty (viz již výše) a současně navrhuje s ohledem na řečené, aby byly ÚSC jako celky vypuštěny jako povinné subjekty v dané fázi legislativního procesu k návrhu.</i>	

		<i>K tomuto navrhuje, aby předkladatel zvážil, analyzoval a vyhodnotil sociální dopady návrhu.</i>	
324. Svaz měst a obcí České republiky	Z	K § 10 odst. 2 návrhu: Dle uvedeného ustanovení poskytovatel regulované služby zapsaný v evidenci poskytovatelů regulovaných služeb je povinen plnit všechny povinnosti plynoucí mu ze zákona vůči zapsaným regulovaným službám od okamžiku doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb až do okamžiku doručení vyrozumění o výmazu z evidence poskytovatelů regulovaných služeb podle § 11. S ohledem na již uvedené, zejména z pohledu nutnosti zajištění personálních kapacit, platových možností ve veřejné správě a s poukazem na již nyní zjevný nedostatek odborníků v této oblasti, současně s ohledem na nutnost provést celkové posouzení u daného poskytovatele regulované služby (odhlížíme od prověřování dodavatelů) je časová lhůta nastavená dle dotčeného ustanovení nerealizovatelná. <i>Navrhujeme prodloužit časovou lhůtu min. na 6 měsíců ode dne doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb.</i>	ROZPOR Vysvětleno Den doručení písemného vyrozumění o zápisu do evidence regulovaných služeb je rozhodným datem, se kterým celý zákon pracuje i na jiných místech a počítá se od něj běh některých lhůt. Například jedna z hlavních povinností zavádět bezpečnostní opatření má na zavedení podle § 14 odst. 3 návrhu zákona lhůtu v délce jednoho roku a začíná běžet od tohoto rozhodného data. Neplatí tedy, že by tato povinnost začala platit ihned po doručení vyrozumění o zápisu do evidence. Toto ustanovení pouze říká, že od vyrozumění zápisu do evidence platí, že daná služba je regulovanou službou a poskytovatel regulované služby vůči ní musí plnit své povinnosti. Jednotlivé povinnosti pak vyplývají z dalších ustanovení a mají své samostatné lhůty. Reakce připomínkového místa: Setrváváme na připomínce – není vysvětleno, z jakého důvodu není možné přijmout navrhovanou úpravu § 10 odst. 2 návrhu bez odkazu na jiné lhůty. JE PONECHÁN ROZPOR.
325. Svaz měst a obcí České republiky	Z	K § 12 odst. 5 návrhu: Dle dotčeného ustanovení je poskytovatel regulované služby povinen zajistit dostatečnou zastupitelnost fyzických osob, které jsou oprávněny jednat za poskytovatele regulované služby ve věcech upravených tímto zákonem.	ROZPOR Akceptováno Důvodová zpráva k tomuto ustanovení již nyní říká že "Počet kontaktních osob není určen, jelikož bude souviset s velikostí a kapacitami regulované organizace, případně počtem regulovaných služeb. V

		Předkladatel však nedefinuje, co míní souslovím „dostatečná zastupitelnost“. Zda se jedná o jednoho zástupce za fyzickou osobu uvedenou při registraci poskytovatele či je třeba určité větší hierarchické zastoupení, příp. i určením jednotlivých rolí. <i>Navrhujeme dle výše uvedeného doplnit důvodovou zprávu.</i>	praxi se však doporučuje uvést minimálně dvě nebo tři kontaktní osoby, aby byla zajištěna jejich zastupitelnost." Tento text bude mírně doplněn, aby bylo zjevnější, k čemu je třeba přihlédnout při zajišťování dostatečné zastupitelnosti, resp. co se tímto pojmem myslí. Reakce připomínkového místa: JE PONECHÁN ROZPOR – K DOVYSVĚTLENÍ PO DOPRACOVÁNÍ JEDNOTLIVÝCH DOKUMENTŮ.
326. Svaz měst a obcí České republiky	Z	K § 15 návrhu ve spojení s tezemi prováděcích právních předpisů: Návrh, jenž je následně doplněn v rámci tezí prováděcích právních předpisů, obsahuje i pro povinné subjekty v režimu nižších povinností obsáhlou řadu povinností, k nimž budou povinné osoby muset vést dokumentaci pro předmětné oblasti. Zpracování projektu k plnění povinností tak dle návrhu bude generovat finanční náklady, stejně tak provozování nové agendy a plnění dalších povinností. Důvodová zpráva předpokládá (dále nezdůvodněné) náklady cca kolem 800 tis. Kč až 1,5 mil. Kč. Není však určeno, zda povinné subjekty, jež jsou zahrnuty ve veřejné správě, na plnění těchto povinností obdrží finanční či jiné prostředky (např. technická opatření, personální zajištění nových povinností, platové náklady, vzdělávací kurzy atd.). Jedná se o navýšení byrokratických povinností pro všechny povinné subjekty. Opět zdůrazňujeme, že USC dle směrnice NIS2 vůbec povinnými subjekty být nemusí. <i>Navrhujeme, aby pro povinné subjekty byly připraveny vzorové intuitivní dokumenty, systém vzdělávání (vstupního i soustavného) a náklady pro povinné subjekty ve veřejné správě byly sanovány státem.</i>	ROZPOR Akceptováno NÚKIB se dlouhodobě věnuje přípravě podpůrných materiálů (https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/), poskytování metodického výkladu, stejně tak jako vzdělávání (https://osveta.nukib.cz/local/dashboard/). Část z těchto činností je dostupná již nyní a bude využitelná i v budoucnu. Část je v plánu a jejich příprava započne jakmile bude návrh nového zákona o kybernetické bezpečnosti v pokročilejší fázi. V otázce financování je zejména v případě povinností pro režim nižších povinností upozornit na skutečnost, že tato úroveň kybernetické bezpečnosti stanovuje skutečně minimální požadavky odpovídající současné době a měly by být zavedeny už jen z důvodu běžného fungování, nikoliv z důvodu veřejnoprávní regulace. Pro dodatečné financování vznikají průběžně jak dotační programy EU pro implementaci směrnice NIS2 (zde je výhodou, že veřejná správa je také

			směrnicí NIS2 předpokládána v čl. 2 odst. 5 písm. a)), případně jako tomu bylo doposud i na národní úrovni. Reakce připomínkového místa: S ohledem na stav veřejných financí je jakákoliv predikovatelnost dotací na národní úrovni téměř nemožná. Shodně tak se nelze ztotožnit se závěry, že minimální požadavky negenerují zvýšené náklady. Je třeba vskutku přihlédnout k možnostem hypoteticky dotčených obcí a k jejich současné situaci. Dotační programy na úrovni EU jsou nyní nastavovány nárazově, nikoliv jako kontinuální – náklady však budou generovány kontinuálně. Opět apelujeme na vyjmutí municipalit jako povinných subjektů jako celku. JE PONECHÁN ROZPOR.
327. Svaz měst a obcí České republiky	Z	K § 21 návrhu: Dle navrhovaného § 21 odst. 1 je úřad po konzultaci s dotčeným poskytovatelem regulované služby z důvodu ochrany vnitřního či veřejného pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn veřejnost informovat <u>o kybernetickém bezpečnostním incidentu či o porušování povinností daných tímto zákonem</u>, nebo dotčenému poskytovateli regulované služby rozhodnutím uložit, aby tak učinil sám. Směrnice NIS2 však tuto otázku pojímá odlišně ve svém čl. 23 odst. 7, dle kterého pokud je nezbytné informovat veřejnost, aby se <u>významnému incidentu</u> zabránilo nebo aby se probíhající významný incident vyřešil, nebo pokud je zveřejnění významného incidentu jinak ve veřejném zájmu, může tým CSIRT některého členského státu nebo případně jeho příslušný orgán, případně týmy CSIRT nebo příslušné orgány jiných dotčených členských států po konzultaci	ROZPOR Vysvětleno - nyní § 22 Od použití sousloví "významný incident" bylo upuštěno, protože má v kontextu zákona o kybernetické bezpečnosti jiný obsah (jedná se o incident, který naplňuje kritéria daná vyhláškou pro určení míry významnosti v kontextu hlášení incidentů ze strany poskytovatelů regulované služby v režimu nižších povinností). Významnost incidentu pak indikuje formulace "z důvodu ochrany vnitřního či veřejného pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu", která stanoví, že Úřad musí mít pro zveřejnění incidentu některý z těchto závažných důvodů, a právě zveřejněním incidentu by bylo možné těmito dopadům předejít, což okruh možností, kdy lze zveřejnění incidentu odůvodnit omezuje v závislosti na jeho

		s dotčeným subjektem informovat veřejnost o významném incidentu nebo požadovat, aby tak učinil daný subjekt. Dotčené ustanovení návrhu je opět formulováno nad rámec směrnice NIS2, byť tento přesah není odůvodněn. <i>Navrhujeme, aby znění bylo zúženo na významný incident v souladu se směrnicí NIS2.</i>	významnosti. Běžně je totiž incident a informace o něm v rozsahu informací, pro které platí i výjimka ze zákona o svobodném přístupu k informacím obsažená v zákoně o kybernetické bezpečnosti. Jedná se tedy skutečně o prostředek ultima ratio a výjimku z pravidla o neposkytování informací o incidentech a svévoli Úřadu tak zabraňuje množství dalších ustanovení zákona o kybernetické bezpečnosti. Rovněž lze říci, že se jedná o institut, který již v obdobném znění byl součástí institutu varování i v současném znění zákona o kybernetické bezpečnosti a Úřad k takovému zveřejnění doposud nikdy neshledal dostatek důvodů. Reakce připomínkového místa: Vysvětlení není v souladu s připomínkou. JE PONECHÁN ROZPOR.
328. Svaz měst a obcí České republiky	Z	K § 22 návrhu: Dotčené ustanovení návrhu se týká tzv. varování, jež vydává NÚKIB, dozví-li se o závažné kybernetické hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti. V odst. 2 je současně uloženo, že poskytovatel regulované služby v režimu vyšších povinností zohlední varování v rámci stanoveného rozsahu, <u>pokud NÚKIB nebo jiný právní předpis nestanoví jinak</u>. Primárně je třeba uvést na pravou míru, že varování jako institut není vůbec ve Směrnici NIS2 obsaženo. Neboť se opět jedná o implementaci nad rámec Směrnice NIS2 a současně není ani v Důvodové zprávě řádně vysvětleno, z jakého důvodu je v poslední části věty odst. 2 stanoveno rozšíření na, ve své podstatě, bezbřehost, je na místě vypustit celý § 22 jako celek, příp. v minimalistické formě aspoň § 22 odst. 2 návrhu.	ROZPOR Vysvětleno – nyní § 23 Varování je institutem, který byl obsažen již v původním znění zákona o kybernetické bezpečnosti, který byl v platnosti ještě před účinností jakéhokoliv předpisu na úrovni EU. Varování je institut, kterým lze stanovit hodnotu hrozby či zranitelnosti, kterou následně do své analýzy rizik poskytovatelé regulované služby v režimu vyšších povinností zapracovávají. Nestanovují se jím tedy žádné další povinnosti, například k zavedení konkrétního opatření, pouze je nutné v rámci analýzy rizik příslušně naložit s výsledným rizikem dle potřeb té které organizace. Varování je stále úkonem dle správního řádu, a tedy musí být řádně odůvodněno tak, aby se nejednalo o formálně nezákonný zásah, který

		<i>Navrhujeme vypustit § 22 jako celek, příp. vypustit v minimalistické formě aspoň § 22 odst. 2 návrhu.</i>	by bylo možné namítat u soudu. Úřad tak tento institut používá jako prostředek ultima ratio, což lze obhájit i dosavadní praxí, která nespočívá v jeho používání na denní bázi. Rovněž se tento institut netýká poskytovatelů regulovaných služeb v režimu nižších povinností, kteří neprovádí klasickou analýzu rizik, kam by mohli zavést hodnotu hrozby či zranitelnosti obsaženou ve vydaném varování, tedy i zde má varování svou významnou limitu a nedopadá na celý okruh subjektů povinných dle nového zákona o kybernetické bezpečnosti. Co se týče odst. 2, k tomu lze dodat následující: Úřad nikdy neměl v úmyslu rozšiřovat okruh subjektů, kterých se varování týká nad zákonem stanovenou úroveň, tedy ani globálně, ani vůči poskytovatelům regulovaných služeb v režimu nižších povinností. Úřad toto ustanovení zahrnul pouze proto, aby v případech, kdy je zejména hrozba relevantní pouze pro některé odvětví, mohl navázat varování vůči naopak úžeji vymezenému počtu subjektů. Rozšířit varování na subjekty mimo zákon o kybernetické bezpečnosti pouhým rozhodnutím Úřadu by nebylo legální a rozšíření na poskytovatele regulované služby v režimu nižších povinností je neúčelné, jelikož tito neprovádějí povinně analýzu rizik, do které by mohli tuto změnu hodnoty hrozby či zranitelnosti implementovat. Tedy tato varianta není rovněž z pozice Úřadu relevantní. Toto je také příslušně doplněno do důvodové zprávy, aby o úmyslu Úřadu s použitím tohoto ustanovení nebylo pochyb. Co se týká jiného právního předpisu, který může subjekty zavázat k aplikaci varování, to vychází z faktu, že vzrůstá trend sektorové regulace, která zahrnuje mimo regulaci sektorovou i regulaci

			kybernetické bezpečnosti. Při její implementaci ze strany sektorových regulátorů zaznává, že by těmto regulátorům připadalo účelné ve svých předpisech zavázat některé subjekty, u kterých to systém řízení bezpečnosti umožňuje (jde o řízení prostřednictvím rizik) a jsou zároveň postaveni mimo dosah zákona o kybernetické bezpečnosti k tomu, aby se tyto organizace řídily varováními vydanými Úřadem. Z tohoto důvodu je tu ponechán prostor pro jiný právní předpis stejné právní síly, tedy zákon, k tomu, aby zavázal další povinné osoby k dodržování varování. Reakce připomínkového místa: Vysvětlení není v souladu s připomínkou. JE PONECHÁN ROZPOR.
329. Svaz měst a obcí České republiky	Z	K dílu 5 návrhu jako celku: K celému Dílu 5 si dovoluujeme poukázat na článek 22 Směrnice NIS2, dle kterého se na unijní úrovni může ve spolupráci s Komisí a agenturou ENISA provést koordinované posouzení bezpečnostních rizik dodavatelských řetězců u specifických kritických služeb IKT, systémů IKT nebo produktů IKT, přičemž se zohlední technické, případně netechnické rizikové faktory. Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA a případně s příslušnými zúčastněnými stranami určí specifické kritické služby IKT, systémy IKT nebo produkty IKT, jež mohou být předmětem koordinovaného posouzení bezpečnostních rizik podle odstavce 1 dotčeného článku. <i>S ohledem na možnost celoevropského hodnocení dodavatelů ve smyslu dotčeného článku 22 Směrnice NIS2, současně s poukazem na konsolidaci veřejných financí a záměr dále nepřístupovat k další hypertrofii byrokratického aparátu, a s ohledem na nedostatečně provedené posouzení dopadů a vysvětlení celého kontrolního prověřovacího mechanismu na národní úrovni a v souladu</i>	ROZPOR Neakceptováno Koordinované posouzení rizik dle čl. 22 NIS2 představuje proces posouzení rizik spojených s dodavateli na úrovni Evropské unie, kdežto mechanismus prověřování bezpečnosti dodavatelských řetězců, obsažený v aktuálním návrhu zákona o kybernetické bezpečnosti, představuje vnitrostátní proces hodnotící kritéria důležitá pro bezpečnost České republiky, přičemž druhý z uvedených není implementací toho prvního. Tyto dva systémy posuzování rizik, resp. hrozeb, se proto procesně i co do kritérií posuzování liší, byť v obecnosti míří ke stejnému cíli. Z tohoto důvodu nelze při zachování potřeby omezování hrozeb specifických pro Českou republiku spoléhat pouze na posouzení dle čl. 22 směrnice a odkazovaný díl návrhu zákona vypustit.

		<i>s uvedenými argumenty v těchto připomínkách navrhuje vypustit celý díl 5 návrhu jako celek bez náhrady.</i> <i>V případě, že by nedošlo k vypuštění tohoto dílu, navrhuje provést důkladnou analýzu Dílu 5 v Důvodové zprávě včetně nastínění procesních kroků a odůvodnění nepřipojení se k možnosti celoevropského hodnocení v porovnání s implementačními opatřeními jiných států EU.</i>	Co se týče odůvodnění výše naznačeného postupu, odkazujeme na zpracované odůvodnění návrhu zákona, závěrečnou zprávu hodnocení dopadů regulace a na rozdílovou tabulku. Reakce připomínkového místa: JE PONECHÁN ROZPOR.
330. Svaz měst a obcí České republiky	Z	K § 28 odst. 4 návrhu: Tzv. nepominutelné funkce stanoveného rozsahu a kritéria rizikivosti dodavatele a způsob jejich vyhodnocení je dle návrhu předmětem definice prováděcího právního předpisu. Jak už jsme v tomto textu uvedli, řada zásadních záležitostí (vč. definice okruhu povinných subjektů) je bez racionálního důvodu, bez ohledu na regulační a právní jistoty zařazena do prováděcích právních předpisů, tj. podzákonných právních předpisů. Z hlediska právní jistoty je však takové řešení zásadních otázek nemyslitelné. <i>Navrhujeme, aby nepominutelné funkce stanoveného rozsahu a kritéria rizikivosti dodavatele za předpokladu, že nebude vyhověno vypuštění dílu 5 návrhu jako celku byly definovány přímo v návrhu a dále rozvedeny v Důvodové zprávě, nikoliv v podzákonném právním předpise.</i>	ROZPOR Neakceptováno - nyní § 29 Nepominutelné funkce stanoveného rozsahu v aktuální variantě tezí doprovázejících nZKB míří na užší skupinu služeb než celý mechanismus bezpečnosti dodavatelského řetězce. Jejich zaměření je natolik specifické, že je nelze přenést do zákona. Na základě četných připomínek se pak NÚKIB rozhodl, že kritéria rizikivosti dodavatele ve formě prováděcího právního předpisu nevydává. Reakce připomínkového místa: Naprosto nesouhlasíme s vypořádáním – přenášení zásadní právní úpravy do podzákonných právních předpisů je nepřijatelné. JE PONECHÁN ROZPOR.
331. Svaz měst a obcí České republiky	Z	K § 40 odst. 1 písm. d) návrhu: Dle § 40 odst. 1 písm. d) návrhu je ředitel Úřadu v době kybernetického nebezpečí za účelem jeho řešení oprávněn nařídít práci v pohotovostním režimu. Z uvedeného znění návrhu není zjevné, komu konkrétně může ředitel NÚKIB v daném případě nařídít práci v pohotovostním režimu.	ROZPOR Akceptováno - nyní § 41 Ustanovení bylo upraveno a zpřesněno. Reakce připomínkového místa:

		Navrhujeme v tomto směru doplnit návrh včetně důvodové zprávy.	JE PONECHÁN ROZPOR – K DOVYSVĚTLENÍ PO DOPRACOVÁNÍ JEDNOTLIVÝCH DOKUMENTŮ.
332. Svaz měst a obcí České republiky	D	K § 53 odst. 2 písm. b) návrhu: Úřad a provozovatel Národního CERT při zpracování osobních údajů, na které se vztahuje přímo použitelný předpis Evropské unie upravující ochranu osobních údajů, mohou v rámci výkonu své působnosti využít osobní údaje i pro jiné účely, než pro které byly shromážděny. Výjimka z pravidel stanovených v GDPR je definována neurčitě, byť samo nařízení GDPR má stanoveny mechanismy pro slučování účelů, dle nichž lze v případě zpracování osobních údajů postupovat. <i>Navrhujeme doplnit dotčené ustanovení ve smyslu nařízení GDPR.</i>	Neakceptováno - nyní § 56 Podmínky pro užití osobních údajů pro jiné účely jsou již stanoveny v článku 6 odst. 4 nařízení GDPR a § 6 zákona o zpracování osobních údajů. Reakce připomínkového místa: JE PONECHÁN ROZPOR – K DOVYSVĚTLENÍ PO DOPRACOVÁNÍ JEDNOTLIVÝCH DOKUMENTŮ. Závěr Připomínka je vypořádána.
333. Svaz měst a obcí České republiky	Z	K 55 odst. 1 návrhu: § 55 odst. 1 návrhu definuje okruh záležitostí, jež budou upraveny prováděcím právním předpisem prostřednictvím Úřadu a formou vyhlášky. <i>Ve smyslu výše uvedeného navrhujeme provést opětovné hodnocení těchto záležitostí, jež budou s ohledem na principy právního státu včetně principu právní jistoty upraveny v podzákoně právním předpisu.</i> <i>Ve smyslu výše uvedených připomínek v případě jejich akceptace navrhujeme upravit i příslušné prováděcí právní předpisy.</i>	ROZPOR Neakceptováno - nyní § 58 Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech (§ 3 a § 2 písm. d)), tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby (§ 3, ve spojení s § 2 písm. i) a k) a § 22a). Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon (§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)), a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá (§ 3 a § 2 písm. b)). Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je

			považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Reakce připomínkového místa: JE PONECHÁN ROZPOR
334. Svaz měst a obcí České republiky	Z	K § 58 návrhu jako celku: <i>Pokud nebude vyhověno vynětí ÚSC z povinných subjektů, navrhuje jejich plné vynětí z přestupkové odpovědnosti.</i> <i>Současně navrhuje snížení pokut pro orgány veřejné správy, neboť tyto jsou stanoveny likvidačně bez ohledu na neziskovost orgánů veřejné správy.</i>	ROZPOR Neakceptováno - nyní § 60 Vyjmout organizace z přestupkové povinnosti vede pouze ke vzniku imperfektních norem, které jsou tedy ve své podstatě nevymahatelné a neexistuje tak žádný imperativ, který by dané organizace nutil povinnosti jim dané plnit. Vrchní hranici výměry sankcí pak stanovuje sama směrnice NIS2 a vzhledem ke své povaze jsou tyto hranice při implementaci nepodkročitelné. Nicméně při stanovování samotné výše předmětné sankce Úřad postupuje v souladu se správními předpisy tak, aby sankce byla přiměřená finančním možnostem daných organizací, kterým je tato sankce vyměřována, tedy rozhodně nelze předpokládat, že by neziskové organizaci s malým rozpočtem, byť i za stejný přestupek, bylo vyměřeno stejně jako organizaci ziskového charakteru s násobně vyšším rozpočtem.

			Reakce připomínkového místa: JE PONECHÁN ROZPOR.
335. Svaz měst a obcí České republiky	Z	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností <i>Obecně navrhuje doplnění vrcholné o to, kdo konkrétně bude nést zodpovědnost za vedení (viz návrh samotný a např. § 5 vyhlášky - povinnosti vrcholného vedení).</i>	ROZPOR Vysvětleno Řízení organizace je individuální záležitostí, v rámci regulace je proto nutné volit obecné formulace, aby bylo jasné, na koho tento požadavek směřuje (jednatel, statutár, ředitel, předseda, hejtman apod.), každá povinná osoba má jinou právní formu a strukturu, může být osobou soukromého i veřejného práva, v každé organizaci je míra stanovení odpovědnosti za vedení rozdílná. Nelze proto předvídat všechny možné situace a jít do větší míry detailu. Následné povinnosti vrcholného vedení, které jsou z pohledu transpozice významné jsme zpracovali přehledně, včetně nové kategorie možného dovození individuální odpovědnosti vrcholného vedení, pokud k této krajní variantě dojde tuto skutečnost nebude posuzovat Úřad ale soud (§ 61 nZKB). Reakce připomínkového místa: JE PONECHÁN ROZPOR.
336. Svaz měst a obcí České republiky	Z	K § 9 odst. 2 návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností: Dle dotčeného ustanovení povinná osoba pro ověření identit administrátorů a uživatelů využívá autentizační mechanismy, které jsou založeny na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů. K tomuto je nezbytné upozornit, že zpravidla je pro druhý faktor ověření využíván mobilní telefon či token, což je spojeno s dalšími	ROZPOR Vysvětleno Dle aktuální teze § 4 odst. 1 Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností není povinnost zavádění vícefaktorové autentizace bezpečnostním opatřením, které musí poskytovatel regulované služby v režimu nižších povinností zavádět vždy. Přestože Národní úřad pro kybernetickou a informační

		náklady. K tomu upozorňujeme, že pro identifikaci mobilním telefonem nelze využívat mobilní telefony osobní, ale výlučně pracovní, jimiž však nedisponují všichni zaměstnanci. <i>Navrhujeme, aby stát zvážil povinnost vícefaktorového ověření pro povinné subjekty (v návaznosti na zařazení ÚSC mezi povinné subjekty) a vyjádřil způsoby vícefaktorového ověření včetně věcných a souvisejících nákladů.</i>	bezpečnosti klade velký důraz na zavádění vícefaktorové autentizace, tento prováděcí předpis bere v potaz věcné i související náklady, které mohou být častou příčinou komplikací při (nemožnosti) zavádění některých bezpečnostních opatření. Z tohoto důvodu je stěžejním požadavkem v tomto prováděcím předpise tzv. přehled bezpečnostních opatření (§ 4 odst. 2), ve kterém je nutné evidovat i nezavedená bezpečnostní opatření (jako např. vícefaktorovou autentizaci), včetně odůvodnění jejich nezavedení. Pokud bude poskytovatel regulované služby mít řádně odůvodněné nezavedení dílčích bezpečnostních opatření, nejlépe i s plánem nápravy do budoucna, nejedná se o nesoulad s tímto prováděcím předpisem, a to např. i v případě aktuálního faktického stavu nezavedení vícefaktorové autentizace. Reakce připomínkového místa: JE PONECHÁN ROZPOR.
337. Odbor kompatibility (vláda)	Z	<u>Po stránce formální:</u> Předkladatel splnil pouze částečně formální náležitosti týkající se vykazování slučitelnosti s právem EU, jak vyplývají zejména z Legislativních pravidel vlády, v platném znění, a z přílohy k usnesení vlády ze dne 12. října 2005 č. 1304, o <i>Metodických pokynech pro zajišťování prací při plnění legislativních závazků vyplývajících z členství České republiky v Evropské unii</i>, v platném znění. Předkladatel se ke vztahu návrhu k právu EU vyjadřuje v důvodové zprávě na str. 68 až 70. Tam uvádí – vedle návrhem implementované <i>směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)</i> i několik nařízení, na které je na určitých místech	Akceptováno jinak Srovnávací tabulky k nařízením uvedeným v bodě 1 a 2 byly doplněny a vloženy do ISAP a budou přiloženy k návrhu. Výkaznictví Vámi navrhovaných ustanovení bylo již provedeno v rozdílové tabulce. Pokud jde o nařízení (bod 3) a rozhodnutí (bod 4), které jsou v gesci Ministerstva dopravy, byly srovnávací tabulky k těmto předpisům vytvořeny a po zaslání a kontrole gestorem budou vloženy do ISAP. V případě ostatních předpisů EU, které jsou uvedeny v důvodové zprávě, se domníváme, že skutečnost, že návrh zákona je v souladu s těmito předpisy nemusí nutně znamenat jejich implementaci do českého právního řádu.

	v návrhu odkazováno, resp. je s nimi návrh provázán. <u>K uvedeným nařízením ale nebyly přiloženy srovnávací tabulky</u>, a tak není možné překontrolovat, která ustanovení jakých nařízení EU přesně byla do návrhu implementována. Přiložena byla pouze srovnávací tabulka ke směrnici NIS 2. 1. K nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) chybí aktualizace srovnávací tabulky. Implementace je zřejmě provedena v § 41 odst. 4, § 46 odst. 1 až 3, a pak do příslušných sankčních ustanovení. Aktualizovanou srovnávací tabulku je třeba přiložit. 2. K nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center, rovněž chybí přiložená aktualizovaná srovnávací tabulka. Implementace má být zřejmě provedena v § 41, § 47 a násl., a pak příslušných v sankčních ustanoveních. Aktualizovanou srovnávací tabulku je třeba přiložit. 3. Ani k nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zavádí Kosmický program Unie a zřizuje Agentura Evropské unie pro Kosmický program a zrušují nařízení (EU) č. 912/2010, (EU) č. 1285/2013 a (EU) č. 377/2014 a rozhodnutí č. 541/2014/EU, nebyla srovnávací tabulka přiložena. Jsme si vědomi, že gestorem předpisu je Ministerstvo dopravy. Nicméně pokud je nějaká část uvedeného nařízení návrhem zapracovávána, je nutné i v případě, kdy je gestor zapracovávaného předpisu EU jiný orgán státní správy, než je předkladatel daného návrhu, vykázat v příslušné srovnávací tabulce, jaká ustanovení by měla být v předloženém návrhu implementována. Uvedené nařízení je	Připomínkové místo s vypořádáním souhlasí.

	navíc v databázi ISAP hodnoceno jako přímo aplikovatelné, tedy srovnávací tabulka tam chybí zcela. Jediným relevantním ustanovením návrhu bude asi § 41 odst. 4, soudě podle informací v rozdílové tabulce. 4. Stejná je situace i v případě rozhodnutí Evropského parlamentu a Rady č. 1104/2011/EU ze dne 25. října 2011 o podmínkách přístupu k veřejné regulované službě nabízené globálním družicovým navigačním systémem vytvořeným na základě programu Galileo – i zde srovnávací tabulka chybí zcela, a to i v databázi ISAP. Rozhodnutí je hodnoceno jako přímo aplikovatelné, což evidentně – vzhledem ke kompetenčním provzbám – není, a je v gesci Ministerstva dopravy. 5. V neposlední řadě důvodová zpráva zmiňuje i směrnici Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES, která je v gesci Ministerstva vnitra a údajně je teprve implementační předpis k této směrnici připravován. Uvedená směrnice ale není uvedena ani v rozdílové tabulce (a srovnávací tabulka rovněž nebyla přiložena), takže není zřejmé, jaká ustanovení z této směrnice by měla být návrhem implementována. Jsme si vědomi, že směrnice NIS 2 na směrnici (EU) 2022/2557 odkazuje, výkaznictví však musí být provedeno řádně. 6. Dále důvodová zpráva na str. 68 zmiňuje nařízení DORA, kterým je nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011. Uvedené nařízení je v gesci Ministerstva financí a je podle databáze ISAP vyhodnocováno jako přímo aplikovatelné. Není jasné, jak je návrh na toto nařízení adaptován, resp. která ustanovení návrhu jsou pro řádnou aplikaci nařízení DORA rozhodná.	

		To samé platí pro v důvodové zpráva na str. 70 uvedené <i>nařízení Evropského parlamentu a Rady (EU) 2019/452 ze dne 19. března 2019, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie</i> (v gesci Ministerstva průmyslu a obchodu), ke kterému je v databázi ISAP přiložena srovnávací tabulka, ta však neodkazuje na předložený zákon. Důvodová zpráva pak odkazuje i na další předpisy EU (například směrnici 2018/1972, kterou se stanoví evropský kodex pro elektronické komunikace), a návrh nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020. Není jasné, nakolik se požadavky těchto dalších předpisů EU, resp. návrhů nových předpisů EU, v návrhu v konkrétních ustanoveních odrážejí.	
338. Odbor kompatibility (vláda)	Z	<u>Po stránce materiální:</u> Stav relevantní právní úpravy v právu EU: Návrh zákona je implementační k tomuto předpisu EU: - Směrnici Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (dále také jenom „směrnice NIS 2“). V souladu s přijetím směrnice NIS 2 se ruší původní <i>směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii</i>. Návrhu zákona se – se zohledněním vyjádření předkladatele v důvodové zprávě, avšak s výhradou výše uvedeného vyjasnění	Bereme na vědomí Připomínkové místo s vypořádáním souhlasí.

		implementačních ustanovení - týkají následující předpisy EU: - v širším kontextu se návrhu týkají ustanovení primárního práva: • čl. 49 SFEU o svobodě usazování, • čl. 4 odst. 2 SEU týkající se národní bezpečnosti, • čl. 16 LZP EU o svobodě podnikání. - v sekundárním právu EU se pak návrhu dotýká: • Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“), • Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center, • Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES, • Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011, • Nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zavádí Kosmický program Unie a zřizuje Agentura Evropské unie pro Kosmický program a zrušují nařízení (EU) č. 912/2010, (EU) č. 1285/2013 a (EU) č. 377/2014 a rozhodnutí č. 541/2014/EU,	

		• Rozhodnutí Evropského parlamentu a Rady č. 1104/2011/EU ze dne 25. října 2011 o podmínkách přístupu k veřejné regulované službě nabízené globálním družicovým navigačním systémem vytvořeným na základě programu Galileo, • Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), • Nařízení Evropského parlamentu a Rady (EU) 2019/452 ze dne 19. března 2019, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie, v platném znění, • Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, • Doporučení Komise (EU) 2019/534 ze dne 26. března 2019 Kybernetická bezpečnost sítí 5G, • Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace, • Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. února 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES, resp. další zakázkové směrnice, • Návrh nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020. Návrhu se týkají také další právně nezávazné akty orgánů a agentur Evropské unie (např. z činnosti ENISA) a strategické dokumenty EU.	

339. Odbor kompatibility (vláda)	Z	Návrh zákona považujeme pro adresáta normy obtížně srozumitelný, jelikož obsahuje množství technicistických termínů a definic, které jsou navíc formulovány kruhem. Důležité instituty předkladatel plánuje definovat až v prováděcích právních předpisech. Takové řešení se jeví problematické nejenom z pohledu kontroly správné implementace práva EU, ale také z ústavněprávního hlediska, jelikož práva a povinnosti subjektů mají být jasně stanoveny zákonem. Konkrétně například k § 4 odst. 2, podle kterého má být prováděcím právním předpisem stanovena kritéria pro identifikaci regulované služby v daných odvětvích, má být zapracován osobní a věcný rozsah směrnice NIS 2 (uvedený v čl. 2 odst. 1 a 2 této směrnice), včetně diskrece členského státu podle čl. 2 odst. 5 této směrnice. Obdobně § 6 odst. 3 návrhu stanoví, že režim poskytovatele regulované služby je stanoven prováděcím právním předpisem, přičemž z rozdílové tabulky vyplývá, že do prováděcího předpisu by měl být zapracován klíčový článek 3, jenž rozlišuje mezi tzv. „základními“ a „důležitými“ subjekty, případně „subjekty poskytující služby registrace jmen domén“. Zdá se tedy, že základní vymezení důležité pro naplnění směrnice bude až v prováděcím právním předpise. Z přiložených tezí prováděcích právních předpisů pak je patrné, že tyto prováděcí předpisy mají <i>de facto</i> zákon doplňovat. To je ale nepřipustná legislativní technika již z hlediska ústavních limitů, navíc ale znemožňuje posoudit míru zapracování směrnice NIS 2 v celém jejím rozsahu.	Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech [§ 3 a § 2 písm. d)], tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby [§ 3, ve spojení s § 2 písm. i) a k) a § 22a]. Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon [§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)], a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá [§ 3 a § 2 písm. b)]. Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Připomínkové místo s vypořádáním souhlasí.
340. Odbor kompatibility (vláda)	Z	V návaznosti na výše uvedené uvádíme, že návrh zákona nesleduje jasné určení osobního rozsahu směrnice NIS 2, kdy se podle článku 3 rozlišují „základní“ subjekty a „důležité“ subjekty případně „subjekty	Akceptováno

		poskytující služby registrace jmen domén“. Místo toho návrh zákona v § 3 operuje s regulovanou službou, přičemž není zcela jasný vztah regulované služby a rozlišením subjektů v kontextu směrnice NIS 2.	Návrh zákona se cíleně odklání od výslovného okopírování směrnici stanoveného rozdělení povinných osob na „essential“ a „important“ (snahou bylo tuto informaci uvést již na začátku důvodové zprávy - např. s. 51: „Požadavky stanovené směrnicí NIS 2 jsou ve svém důsledku takové povahy, že návrh zákona musí s ohledem na změnu dosavadního přístupu k oblasti kybernetické bezpečnosti upravit nejen některé dílčí oblasti tak, aby bylo možné sladit požadavky směrnice NIS 2 s dosavadním způsobem regulace kybernetické bezpečnosti, ale především musí dojít k podstatným změnám v oblasti stanovení a identifikace povinných osob, změn interních procesů a dalších náležitostí, které přinesly požadavky na další dílčí úpravy zákona o kybernetické bezpečnosti.“ apod.). Důvodem pro odklon od směrnici používaného pojmenování subjektů bylo jak to, že výsledné množiny subjektů ve vyšším a nižším režimu povinností jsou širší, než množiny dané směrnicí, protože nad rámec směrnice reflektují také národní požadavky na kybernetickou bezpečnost (např. z důvodů národní bezpečnosti, tedy mimo působnost směrnice nebo primárního práva EU). Podstatou tedy je, že režim nižších povinností odpovídá množině „important“ a dalším národním požadavkům, režim vyšších povinností odpovídá množině „essential“ a dalším národním požadavkům. Tento postup je sám směrnicí NIS2 předvídan zejména čl. 5 Princip minimální harmonizace. Odklon od používání pojmů „essential“ a „important“ ze směrnice byl podpořen také tím, že v českém jazyce není pojmosloví využívané směrnicí vhodné a odpovídající. „Základní“ subjekty jsou fakticky významnější než subjekty „důležité“, což dlouhodobě způsobuje nepochopení mezi adresáty. Výše uvedené jsme se snažili podchytit v důvodové

			zpráve zejm. na s. 103. V návaznosti na tuto připomínku uvedeme výše uvedené vysvětlení ještě výslovně v tomto textu. Typ povinné osoby „subjekty poskytující služby registrace jmen domén“ obsahuje stejně jako v případě směrnice NIS2 jinou sadu povinností (čl. 28) a i když se mohou subjekty fakticky překrývat (např. registr domén nejvyšší úrovně bude jak poskytovatelem regulované služby v režimu vyšších povinností (ve smyslu „essential“), tak má také povinnosti jako subjekt poskytující registrace jmen domén ve smyslu § 36 a násl. Máme za to, že tento postup je se směrnicí souladný. Připomínkové místo s vypořádáním souhlasí.
341. Odbor kompatibility (vláda)	D	Předkladatel na mnoha místech návrhu zákona vykazuje úpravu jako implementační, přičemž postrádáme ustanovení směrnice, které by takovou úpravu po členském státu vyžadovalo, k tomu viz dále.	Viz vypořádání konkrétních připomínek Připomínkové místo s vypořádáním souhlasí.
342. Odbor kompatibility (vláda)	Z	K § 1: Formulace ustanovení neodpovídá Legislativním pravidlům vlády, kde je uvedena standardní formulace (článek 48). Navrhujeme odstavce spojit. Dále za relevantní pro implementaci v případě odstavce 2 považujeme ustanovení předpisů EU vyžadující tzv. referenční odkaz (článek 41 směrnice NIS 2), naopak ustanovení o rozsahu působnosti směrnice či platnosti nařízení nejsou pro § 1 relevantní. Požadujeme upravit.	Akceptováno Odstavce 1 a 2 byly spojeny a nový odstavec 1 zní: „(1) Tento zákon zapracovává příslušný předpis Evropské unie¹⁾, zároveň navazuje na přímo použitelné předpisy Evropské unie²⁾ a upravuje práva a povinnosti orgánů a osob a působnost a pravomoci Národního úřadu pro kybernetickou a informační bezpečnost (dále jen "Úřad") a dalších orgánů veřejné moci v oblasti kybernetické bezpečnosti. Vykazován bude tento odst. pouze čl. 41 odst. 1 a 2 směrnice NIS 2. Připomínkové místo s vypořádáním souhlasí.
343. Odbor kompatibility (vláda)	Z	K § 2 odst. 2 písm. c): Článek 6 bod 10) v definici kybernetické hrozby odkazuje na čl. 2 bod 8 nařízení 2019/881. Podle něj se kybernetickou hrozbou rozumí	Vysvětleno Aktiva navazují na pojem informační a komunikační systémy používaný v dosavadním zákoně (a tedy i v

		„jakákoliv potenciální okolnost, událost nebo čin, které mohou poškodit, narušit nebo jinak nepříznivě ovlivnit <i>sítě a informační systémy</i>, jejich uživatele a další osoby“. Navržené implementační ustanovení v § 2 odst. 2 písm. c) obsahuje definici kybernetické hrozby zjevně širší, když operuje s „ovlivněním aktiv“, jež jsou definována velmi široce v odst. 1 písm. a). Je nutné vyjasnit, jaký je rozsah ve vztahu k definici ve směrnici. Také se domníváme, že není možné definici nad rámec směrnice libovolně měnit, resp. rozšíření může mít vliv zejména v přeshraničním (nadmárodním) kontextu.	směrnicích NIS1 a NIS2) a jeho prováděcích předpisech a odpovídají tomuto pojmu tak, jak jej Úřad ve vztahu k současné právní úpravě konstantně vykládá. Informačním systémem ve smyslu současného zákona o kybernetické bezpečnosti nelze chápat pouze úzkou množinu technických aktiv (ve smyslu HW a SW), ale množinu celé řady primárních a podpůrných aktiv, která v souhrnu tvoří kompaktní a funkční celek umožňující zpracování informací a dat, jinými slovy také množinu aktiv relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě. Aktiva tvoří naprostý základ úvah o kybernetické bezpečnosti, resp. jejím řízení, v rámci jakékoli organizace, a tento pojem tak slouží jako základní stavební kámen pro celý obsah návrhu zákona. Jde o pojem převzatý z vyhlášky č. 82/2018 Sb., kterým se za účinnosti současného zákona o kybernetické bezpečnosti definují hranice řízení bezpečnosti informačních systémů v organizaci. Odklon od pojmu informační a komunikační systémy byl proveden z praktických důvodů, kdy záměrem nového zákona je postavit najisto, že předmětem zajišťování kybernetické bezpečnosti jsou všechna primární a podpůrná aktiva sloužící k poskytování regulovaných služeb, nikoli pouze technická aktiva, jak se mnohdy adresáti současného zákona snaží tento zákon interpretovat. Lze tedy shrnout, že pojmy informační a komunikační systémy, jak s nimi pracuje směrnice NIS2, a aktiva ve smyslu § 2 odst. 1 písm. a) vyjadřují shodnou množinu aktiv, která má být chráněna a která má být předmětem

			bezpečnostních opatření ve smyslu čl. 21 směrnice NIS2. Připomínkové místo s vypořádáním souhlasí.
344. Odbor kompatibility (vláda)	Z	K § 2 odst. 2 písm. d): Obdobně, jak je výše uvedeno pro definici kybernetické hrozby, to platí pro definici významné kybernetické hrozby. Podle čl. 6 bodu 11) směrnice NIS 2 se významnou kybernetickou hrozbou rozumí kybernetická hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál vážně ovlivnit síť a informační systémy určitého subjektu nebo uživatelů služeb takového subjektu tím, že způsobí značnou hmotnou nebo nehmotnou újmu. Naopak podle navrženého § 2 odst. 2 písm. d) se významnou kybernetickou hrozbou rozumí kybernetická hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál závažně ovlivnit <i>aktiva poskytovatele regulované služby nebo uživatelů regulovaných služeb</i> natolik, že způsobí značnou majetkovou nebo nemajetkovou újmu. Směrnice nemluví o aktivech poskytovatele regulované služby nebo/a (aktivech) uživatelů regulovaných služeb. Směrnice definice je tak ve výsledku (zjevně) užší. Žádáme tuto diskrepanci vysvětlit a případně navrženou formulaci upravit.	Vysvětleno Aktiva navazují na pojem informační a komunikační systémy používaný v dosavadním zákoně (a tedy i ve směrnici NIS1 a NIS2) a jeho prováděcích předpisech a odpovídají tomuto pojmu tak, jak jej Úřad ve vztahu k současné právní úpravě konstantně vykládá. Informačním systémem ve smyslu současného zákona o kybernetické bezpečnosti nelze chápat pouze úzkou množinu technických aktiv (ve smyslu HW a SW), ale množinu celé řady primárních a podpůrných aktiv, která v souhrnu tvoří kompaktní a funkční celek umožňující zpracování informací a dat, jinými slovy také množinu aktiv relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě. Aktiva tvoří naprostý základ úvah o kybernetické bezpečnosti, resp. jejím řízení, v rámci jakékoli organizace, a tento pojem tak slouží jako základní stavební kámen pro celý obsah návrhu zákona. Jde o pojem převzatý z vyhlášky č. 82/2018 Sb., kterým se za účinnosti současného zákona o kybernetické bezpečnosti definují hranice řízení bezpečnosti informačních systémů v organizaci. Odklon od pojmu informační a komunikační systémy byl proveden z praktických důvodů, kdy záměrem nového zákona je postavit najisto, že předmětem zajišťování kybernetické bezpečnosti jsou všechna primární a podpůrná aktiva sloužící k poskytování

			regulovaných služeb, nikoli pouze technická aktiva, jak se mnohdy adresáti současného zákona snaží tento zákon interpretovat. Lze tedy shrnout, že pojmy informační a komunikační systémy, jak s nimi pracuje směrnice NIS2, a aktiva ve smyslu § 2 odst. 1 písm. a) vyjadřují shodnou množinu aktiv, která má být chráněna a která má být předmětem bezpečnostních opatření ve smyslu čl. 21 směrnice NIS2. Připomínkové místo s vypořádáním souhlasí.
345. Odbor kompatibility (vláda)	D	K § 2 odst. 2 písm. g): Návrh zákona používá českému jazyku cizí slova jako například „prevence“ nebo „detekce“. Navrhujeme zde použít směrnicových výrazů, které používají výrazů „předejít“ nebo „odhalit“ (čl. 6 bod 8 NIS 2).	Neakceptováno Oba pojmy jsou obsaženy v internetové jazykové příručce (https://prirucka.ujc.cas.cz/), které jsou běžně užívané v souvislosti se zvládáním incidentů. Nadto jsou oba termíny obsaženy v již existujících právních předpisech, např.: zákon č. 109/2002 Sb., o výkonu ústavní výchovy nebo ochranné výchovy ve školských zařízeních a o preventivně výchovné péči ve školských zařízeních; § 16a zákona č. 289/2005 Sb., o vojenském zpravodajství; § 5 zákona č. 281/2002 Sb., o některých opatřeních souvisejících se zákazem bakteriologických (biologických) a toxických zbraní. Smyslem připravovaného zákona je vytvořit moderní předpis pro mezinárodní odvětví, které se z velké části inspirované mezinárodními standardy psanými v angličtině, např. Computer Security Incident Handling Guide (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf). V mezinárodně uznávaných publikacích jsou ve spojení s kybernetickým bezpečnostním incidentem zaužívané pojmy „prevention“ a „detection“, CERT jednotlivých členských států mezi sebou budou komunikovat

			převážně v angličtině, proto se nejví jako přínosné, aby byly pojmy „prevence“ a „detekce“ nahrazovány pojmy "odhalování" a "předcházení". Připomínkové místo s vypořádáním souhlasí.
346. Odbor (vláda)	kompatibility	Z	K § 2, § 3, § 4 a § 5 – vymezení osobního a věcného rozsahu (v návaznosti na obecnou připomínku č. 1 výše): V návrhu zákona chybí jasné vymezení regulované služby i poskytovatele regulované služby. Nadpis dílu 1 v § 3 zní: „Stanovení regulované služby a režimu poskytovatele regulované služby“. Dále se upravuje regulovaná služba, a v § 6 jsou již uvedeny pouze příslušné režimy poskytovatelů regulované služby, resp. registrace. Není tedy vůbec jasné, kdo je poskytovatelem regulované služby. Je otázkou, nakolik se má tímto ustanovením upravovat poskytovatel regulované služby, a nakolik pouze regulovaná služba. Navíc poskytovatel je podle § 2 odst. 1 písm. f) návrhu ten, kdo poskytuje regulovanou službu - úprava je nejasná, protože je definována kruhem. Navíc pokud § 3 návrhu stanoví, že regulovaná služba je <i>stanovena kritérii</i> pro identifikaci regulované služby nebo <i>kritérii</i> pro <i>určení</i> regulované služby, je nejasné, kým, resp. čím bude tato služba stanovena, resp. určena. Předkladatel má zřejmě za to, že ke „stanovení“ dojde prováděcím právním předpisem podle § 4 odst. 2, a k určení dojde podle § 5 návrhu. Takové řešení ale dává širokou působnost jak prováděcímu právnímu předpisu, tak i „určení“ rozhodnutím Úřadu. Směrnice NIS 2 v článku 2 vymezuje svou působnost odkazem na svou přílohu I a II, popřípadě i na doporučení 2003/361/ES (čl. 2 odst. 1 a 2 směrnice NIS 2), a pak do osobní působnosti zahrnuje subjekty určené podle směrnice 2022/2557 (čl. 2 odst. 3 směrnice NIS 2), subjekty poskytující registrace jmen domén, případně fakultativně stanovené subjekty podle čl. 2 odst. 5 směrnice NIS 2. Další možné výjimky, resp. omezení upravují další odstavce

Neakceptováno

Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech [§ 3 a § 2 písm. d)], tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby [§ 3, ve spojení s § 2 písm. i) a k) a § 22a]. Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon [§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)], a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá [§ 3 a § 2 písm. b)]. Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Z hlediska lepší možnosti kontroly správného provedení transpozice směrnice NIS 2 do českého právního řádu došlo také k

		článku 2. Rámeček zákona je mnohem širší, navíc nejasný, a to zřejmě i proto, že část transpozice má být v podstatných rysech, zejména ve vymezení osobního a věcného rozsahu (§ 4 odst. 2), provedena až prováděcími právními předpisy. To je postup již z ústavního hlediska nepřijatelný, navíc z hlediska řádného provedení směrnice nekontrolovatelný.	výslovnému uvedení vymezení osobní působnosti dané směrnicí do kritérií pro vydání prováděcího právního předpisu. Připomínkové místo s vypořádáním souhlasí.
347. Odbor kompatibility (vláda)	D	K § 5 písm. b): Ač části navrženého ustanovení zapracovává určité požadavky článku 2 směrnice NIS 2, není v celém svém rozsahu implementací. Část ustanovení, která nemá přímou oporu ve směrnici NIS 2, nemá být vykazována. Konkrétně podle navrženého ustanovení regulovanou službou je (dále) služba stanovená u orgánu nebo osoby rozhodnutím Úřadu v případě, že její narušení může způsobit závažný zásah do života postihující více než 125 000 osob, a to prostřednictvím ohrožení života, zdraví, majetkové hodnoty, vnitřního či veřejného pořádku, bezpečnosti nebo životního prostředí. Vykázán je zde čl. 2 odst. 6 směrnice NIS 2, podle kterého směrnicí není dotčena <i>odpovědnost členských států za ochranu národní bezpečnosti ani jejich pravomoc chránit jiné základní funkce státu, včetně zajišťování územní celistvosti státu a zachování veřejného pořádku</i>. Jsme názoru, že (příkladmo) slova „může způsobit závažný zásah do života postihující více než 125 000 osob, a to prostřednictvím ohrožení života, zdraví, majetkové hodnoty“, ačkoliv zde jsou užita v souladu s postulátem směrnice, jejich užití nepředstavuje přímou implementaci. Žádáme odpodtrhnout.	Akceptováno Ustanovení nebude vykazováno jako implementační. Připomínkové místo s vypořádáním souhlasí.
348. Odbor kompatibility (vláda)	D	<u>K § 5 písm. d):</u> Zde upozorňujeme, co se týká obsahu pojmů „krizové řízení a kritická infrastruktura“, na propojení se směrnicí 2022/2557, na kterou vykazovaný čl. 2 odst. 3 směrnice NIS 2 odkazuje. Příslušný zákon o kritické infrastruktuře je ale teprve připravován, gesci má MV. Je tedy věci zřejmě probíhajících legislativních prací k zákonu o kritické	Akceptováno Děkujeme za upozornění. V souladu s připomínkou již dlouhodobě probíhá spolupráce mezi týmy připravujícími jak transpozici směrnice NIS2 za NÚKIB, tak transpozici směrnice CER za MV -

		infrastruktury, aby terminologie měla vzhledem k propojení mezi dvěma směrnicemi (dvěma transpozičními zákony) vždy odpovídající obsah.	GRHZS tak, aby byla v co největší míře zajištěna vzájemná interoperabilita obou předpisů. Připomínkové místo s vypořádáním souhlasí.
349. Odbor kompatibility (vláda)	Z	K § 6 a 7 (v návaznosti na obecnou připomínku č. 2 výše): Ustanovení má implementovat článek 3 směrnice NIS 2. V čl. 3 odst. 1 směrnice jsou definovány základní subjekty. V čl. 3 odst. 2 pak následně důležité subjekty. Uvedené požadavky a rozlišení subjektů ze směrnice NIS 2 v § 6 ani § 7 vůbec nenalzáme. Zřejmě předkladatel hodlá uvedené provádět až prováděcím právním předpisem podle § 6 odst. 3. Příložené teze vyhlášek ale vůbec nedávají jasnou odpověď. Navíc takové řešení, kdy budou základní parametry dotvářeny až prováděcím právním předpisem nepovažujeme za ústavně konformní.	Vysvětleno S ohledem na připomínku výše lze i na tomto místě uvést, že důvodem pro odklon od směrnici používaného pojmenování subjektů bylo jak to, že množiny subjektů pro vyšší a nižší režim povinností dané směrnici nejsou výhradní náplní těchto budoucích množin (tj. z důvodů např. národní bezpečnosti, tedy mimo působnost směrnice nebo primárního práva EU obecně obsahuje množina např. pro vyšší režim i subjekty odlišné od směrnice), tak také to, že v českém jazyce není pojmosloví využívané směrnici vhodné a odpovídající ("základní" subjekty jsou fakticky významnější než subjekty "významné"). Návrh právní úpravy je stanoven tím způsobem, že transpozicí požadavků a vymezení subjektů v rámci "významných subjektů" je režim nižších povinností, transpozicí požadavků a vymezení subjektů v rámci "základních subjektů" je režim vyšších povinností. K otázce způsobu stanovení okruhu povinných osob zasíláme vypořádání níže. Připomínkové místo s vypořádáním souhlasí.
350. Odbor kompatibility (vláda)	Z	K § 8: Podle rozdílové tabulky je v tomto ustanovení promítnut čl. 3 odst. 4 směrnice NIS 2. Navrženou formulaci považujeme za nejasnou. Ve směrnici je přesněji uvedeno, jaké informace mají být příslušným orgánům poskytovány (název subjektu, adresa a aktuální kontaktní údaje, včetně e-mailových adres, rozsahu IP adres a telefonních čísel, atd.). Ani § 8 ve spojení s § 12 není dostatečně konkrétní. Žádáme	Vysvětleno V § 12 odst. 6 je stanoveno, že obsahové náležitosti, formát a způsob provedení hlášení registračních, kontaktních a doplňujících údajů stanoví prováděcí právní předpis. Odst. 2 až 4 nebudou vykazány jako implementační a budou odstraněny z rozdílové tabulky.

		napravit. Na druhou stranu, ač je ustanovení podtrženo celé, směrnice NIS 2 neobsahuje stanovení konkrétních lhůt. Máme za to, že odstavce 2 až 4 nejsou implementačního charakteru, a tudíž by měly být odpodtrženy a vypuštěny z rozdílové tabulky.	Připomínkové místo s vypořádáním souhlasí.
351. Odbor kompatibility (vláda)	D	K § 9: Ustanovení je vykázano v rozdílové tabulce s odkazem na čl. 3 bod 4 směrnice, nicméně ve vlastním návrhu ani není podtrženo a podle našeho názoru ani implementační charakter nemá. Navržené ustanovení tudíž je třeba vypustit z rozdílové tabulky. Dále vznášíme dotaz, na co se směřuje slovy „v případě naplnění kritérií pro identifikaci každé další regulované služby“ v odstavci 1. Jaká kritéria (kde jsou uvedena) se mají na mysli v odstavci 1?	Vysvětleno Jedná se o kritéria pro identifikaci uvedená v § 4. Ustanovení § 9 odst. 1 míří na situace, kdy poskytovatel regulované služby poskytuje více služeb, z nichž každá může být samostatně regulovanou službou a je za potřebí ji takto registrovat. S ohledem na připomínku nebude § 9 vykázan v rozdílové tabulce. Připomínkové místo s vypořádáním souhlasí.
352. Odbor kompatibility (vláda)	Z	K § 10: Zápis do evidence poskytovatelů regulovaných služeb má implementovat čl. 3 odst. 3 směrnice NIS 2. Podle tohoto ustanovení směrnice má být seznam základních a důležitých subjektů, jakož i subjektů poskytujících služby registrace jmen a domén, stanovena do 17. 4. 2025. Odráží se někde toto datum? Zákon má být účinný od 18. října 2024, musejí být tudíž již tímto datem dokončeny registrace? V přechodných ustanoveních relevantní ustanovení nenalézáme, vykázano není nic. Navíc evidence se má podle čl. 3 odst. 3 každé dva roky přezkoumávat.	Vysvětleno Evidence regulovaných služeb ze své podstaty nikdy nebude úplná. Subjekty resp. jimi poskytované služby do evidence na základě naplnění kritérií přicházejí a zase odcházejí (registrace a výmaz). Subjekty přitom mají stanoveny lhůty, ve kterých s právní úpravou mohou seznámit a ve kterých své služby identifikují na základě naplnění kritérií, přičemž následně provedou registraci. Teprve na základě registrace dojde k zápisu do evidence. Čl. 3 odst. 3 směrnice NIS2 směřuje k tomu, aby členské státy pravidelně (každé dva roky) hlásily počty regulovaných subjektů v jednotlivých sektorech, s tím že k prvnímu hlášení má dojít právě k 17. 4. 2025 (půl roku po uplynutí implementační lhůty a zamýšlené účinnosti návrhu zákona).

			Připomínkové místo s vypořádáním souhlasí.
353. Odbor kompatibility (vláda)	D	K § 11: Ustanovení v odstavci 3 používá formulaci „osoba zapsaná v evidenci poskytovatelů“, ve výše uvedených ustanoveních se mluví o poskytovateli. Nemá být v odstavci 3 rovněž poskytovatel, anebo je to (také) jiný subjekt?	Akceptováno jinak Použití označení „orgán nebo osoba zapsaná v evidenci poskytovatelů regulovaných služeb“ místo „poskytovatel regulované služby“ byl na tomto místě zcela záměrně. Tento odstavec totiž říkal, že pokud subjekt nadále neposkytuje žádnou regulovanou službu, Úřad tento orgán nebo osobu vymaže z evidence poskytovatelů regulovaných služeb a o této skutečnosti tento orgán nebo osobu písemně vyrozumí. Jestliže subjekt neposkytuje žádnou regulovanou službu, nejedná se tak logicky o poskytovatele regulované služby, a proto tak nemůže být ani v tomto ustanovení označen. Na základě připomínek však došlo ke změně přístupu. Úkony jako je registrace, změna, zápis a výmaz se nově vždy vztahují pouze ke konkrétní regulované službě. Tím pádem došlo i k přejmenování na evidenci regulovaných služeb. Připomínkové ustanovení se tudíž stalo zcela nadbytečným a bude vypuštěno. Připomínkové místo s vypořádáním souhlasí.
354. Odbor kompatibility (vláda)	Z	K § 12: - viz připomínka k § 8. Ustanovení stanovuje, že poskytovatel regulované služby hlásí registrační, kontaktní a další doplňující údaje. Směrnice NIS 2 ale v čl. 3 odst. 4 uvádí minimální seznam informací, které by se měly poskytovat. Tento seznam se zdá být mimoběžný s § 12, resp. není zřejmé, co kam spadá. Navíc formulace „údaje spojené s“, nebo „údaje potřebné pro“ jsou velmi široké množiny, které zejména v případě § 12 odst. 2 písm. c) mohou představovat leccos. Údaje je	Vysvětleno Výčet požadovaných údajů dle § 12 odst. 3 návrhu se zdá mimoběžný s požadavky čl. 3 odst. 4 NIS2, jelikož bližší specifikace požadovaných údajů je obsažena v prováděcím právním předpise vydaném na základě § 12 odst. 6 (vyhláška o Portálu NÚKIB). Máme za to, že údaje specifikované ve vyhlášce o Portálu zahrnují veškeré údaje zmíněné v čl. 3 odst. 4 směrnice NIS2. Připomínkové místo s vypořádáním souhlasí.

		třeba zkonkretizovat, a to v návaznosti na směrnici NIS 2. Navíc máme za to, že odstavce 3 až 6 nejsou, nebo převážně nejsou, implementační. Požadujeme ustanovení odpodtrhnout a vypustit z rozdílové tabulky.	
355. Odbor kompatibility (vláda)	D	K § 13: Ustanovení je vykázáno k čl. 1 odst. 1 či článku 5 směrnice NIS 2, nicméně takové vykázání není přiléhavé. Spíše lze uvažovat o čl. 21 bod 1 směrnice. Je rovněž otázka, na co přesně navazuje § 13 odst. 2 až 5, které jsou vykázány jako implementační. Zdá se nám, že tato ustanovení spíše implementační nejsou. Navrhujeme odpodtrhnout a vypustit z rozdílové tabulky.	Akceptováno V § 13 bude vykázán jako implementační pouze § 13 odst. 1, který provádí čl. 21 odst. 1 směrnice. Připomínkové místo s vypořádáním souhlasí.
356. Odbor kompatibility (vláda)	Z	K § 14 a 15: K uvedenému ustanovení je vykázána celá škála ustanovení směrnice NIS 2, ale je otázkou, co je skutečně prováděno. Čl. 1 odst. 1 a článek 5 zřejmě nebudou relevantní. Nejvíce relevantní bude zřejmě článek 21 směrnice NIS 2, ten ale vidíme proveden pouze velmi rámcově. Má být například čl. 21 odst. 2 vtělen do § 15? A kde je uvedeno, že se má při zvažování vhodných opatření zohlednit zranitelnost dodavatele (čl. 21 odst. 3 směrnice NIS 2)? Ustanovení § 14 odst. 4 předvídá vydání prováděcího právního předpisu, který stanoví bezpečnostní opatření, což zřejmě bude hlavní těžiště transpozice. Samotné zmocňovací ustanovení ale není implementačního charakteru (tudíž by nemělo být podtrženo a uvedeno v rozdílové tabulce). Takové stanovení povinností by navíc mělo být uvedeno přímo v zákoně, výčet (organizačních a technických) opatření v § 15, ze kterých není zřejmý základní rozsah povinností, se nám nezdá ústavně hájitelný. Situaci ale komplikuje to, že mají být teprve vydávány prováděcí akty Evropské komise, kterými se opatření blíže specifikují. Dále v § 14 odst. 3 je uvedena lhůta 1 roku. Jedná se o směrnicovou	Vysvětleno Ano, páteřním ustanovením pro oba režimy pro bezpečnostní opatření je článek 21 směrnice NIS2. Samotný požadavek na řízení dodavatelů je ve své podstatě reakcí na zranitelnosti plynoucí z dodavatelského řetězce. Cílem řízení dodavatelů má být zavedení bezpečnostního opatření směřující na zajištění bezpečnosti dodavatelského řetězce. Opatření pro řízení dodavatelů je ve své podstatě reakcí na zranitelnosti. V současné chvíli pracujeme na znění zmíněných prováděcích právních předpisů rozvádějící výčet bezpečnostních opatření uvedených v § 15 návrhu zákona. Nesouhlasíme s tím, že rozsah povinností je nutné uvádět v zákoně a že není ústavně obhajitelný, protože nijak nevybočuje ze současné systematiky zákona. Navíc máme za to, že ustanovení § 15 (výčet opatření) zákona je podrobnější než čl. 21 NIS2, který je ještě obecnějšího charakteru. Současný zákon o kybernetické bezpečnosti je účinný 6 let a zvolená systematika § 15, která je dále rozvedena

		věc? Z čeho lhůta 1 roku vyplývá? A neměla by být uvedena v přechodných ustanoveních?	vyhláškou pro režim vyšších i nižších povinností (rozvádí dopodrobna výčet v ustanovení § 15 návrhu zákona), není dle našeho názoru legislativně neobhajitelná. K poslední části Vašeho dotazu k § 14 odst. 3, směřujícímu k lhůtě jednoho roku: nejedná se o novinku, stejným způsobem pracuje s lhůtou jednoho roku i zákon o kybernetické bezpečnosti. Nejedná se o směrnice, ani se nejedná o přechodné ustanovení, jedná se o prostou lhůtu pro zahájení plnění zákonných povinností. Připomínkové místo s vypořádáním souhlasí.
357. Odbor kompatibility (vláda)	D	K § 15: Výkaznictví k tomuto ustanovení je zavádějící, viz výše k § 14. Není jasné, kde lze najít definici obsah pojmu poskytovatele regulované služby v režimu vyšších povinností (odstavec 1) a nižších povinností (odstavec 2). § 6 odst. 2 pouze stanoví, že jsou poskytovatelé v režimu vyšších a v režimu nižších povinností. Pochopení je významné zejména s ohledem na to, že se jedná o implementační úpravu.	Vysvětleno Poskytovatele regulované služby je nutné chápat v obecném slova smyslu. V prvním případě poskytovatel provádí registraci pro naplnění identifikačních kritérií pro identifikaci regulované služby (tím pádem se stane poskytovatelem regulované služby). V případě rozhodnutí Úřadu, provede registraci poskytovatele sám Úřad. Na poskytovatele regulované služby je nutné také nahlížet zejména z pohledu vyhlášky o regulovaných službách, na základě které lze z ohledem na její předmět úpravy dovodit, že poskytovatelem regulované služby je orgán nebo osoba, která naplní kritéria pro identifikaci regulovaných služeb (§ 4 návrhu zákona) Máme definici regulované služby, ten který jí naplní, je tak automaticky poskytovatelem regulované služby, (podobná analogie je například v zákoně o el. komunikacích, kde se také mluví o poskytovateli regulované služby ale není také definován, definována je poskytována služba). V případě zavedení definice poskytovatele regulované služby, by tak došlo v

			současné systematice zákona a prováděcích předpisů k nežádoucí definici kruhem. Připomínkové místo s vypořádáním souhlasí.
358. Odbor kompatibility (vláda)	Z	K § 16: Kdo stanoví rozsah hlášení, které je povinen poskytovatel regulované služby hlásit Úřadu? Také není jasné, jak je ve vztahu ke směrnici „kybernetický bezpečnostní incident“, jenž je vymezen v § 2 odst. 2 písm. f). Například v rozdílové tabulce uvedený čl. 23 odst. 3 směrnice NIS 2 uvádí, co se má považovat za významný incident, což je zřejmě užší vymezení, než v návrhu zákona. Zmocňovací ustanovení v odstavci 3 není implementační, opět je třeba jej odpodtrhnout a vypustit z rozdílové tabulky. Odstavec 4 je opět zřejmě přechodným ustanovením, které navíc není předvídáno směrnicí. Žádáme napravit.	Vysvětleno Obsah hlášení je uveden v § 17. Co se týče definice incidentu, Úřad zvolil širší vymezení, než stanovuje směrnice NIS 2, v souladu s principem minimální harmonizace. Zároveň došlo na základě připomínky k doplnění informací podávaných v prvotním hlášení o identifikační údaje ohlašovatele a základní údaje o kybernetickém bezpečnostním incidentu. Poskytovatelé regulovaných služeb mají povinnost hlásit všechny kybernetické bezpečnostní incidenty, nejen ty s významným dopadem. Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob. Odstavce 3 a 4 nebudou vykazány jako implementační. Připomínkové místo s vypořádáním souhlasí.
359. Odbor kompatibility (vláda)	Z	K § 17 odst. 3 písm. a):	Vysvětleno

		Není zřejmé, co jsou indikátory kompromitace, byť se jedná již o směrniceový pojem. Jaké je propojení s nařízením eIDAS č. 910/2014 v poznámce pod čarou č. 3? Neměl by být uveden spíše odkaz na zákon č. 297/2016 Sb., aby bylo zřejmé, kterého poskytovatele služeb má předkladatel na mysli?	Jako indikátory kompromitace jsou označovány artefakty, které jsou užitečné při identifikaci incidentu nebo události v síti nebo systému (např. IP adresy, domény, URL, hashe souborů, atp.). Definice poskytovatele služeb vytvářejících důvěru je uvedená v přímo použitelném nařízení eIDAS č. 910/2014. Zákon č. 297/2016 Sb. upravuje některé postupy poskytovatelů služeb vytvářejících důvěru, některé požadavky na služby vytvářející důvěru, působnost Digitální a informační agentury v oblasti služeb vytvářejících důvěru a sankce za porušení povinností v oblasti služeb vytvářejících důvěru. Připomínkové místo s vypořádáním souhlasí.
360. Odbor kompatibility (vláda)	Z	K § 17 odst. 3 písm. c): Ustanovení má implementovat čl. 23 odst. 4 písm. d) a e) směrnice NIS 2, kde je uvedeno i to, jaký má být obsah závěrečné zprávy. Na jakém místě je to uvedeno v návrhu?	Vysvětleno Ustanovení § 17 odst. 5 návrhu zákona obsahuje zmocňovací ustanovení pro vydání prováděcího předpisu, který stanoví mj. obsahové náležitosti hlášení incidentu. Tímto předpisem je vyhláška o Portálu Úřadu a požadavcích na vybrané úkony, která v § 3 odst. 1 stanovuje obsahové náležitosti formuláře pro hlášení incidentů, přičemž z odst. 2 písm. d) tohoto ustanovení vyplývá, že jde přes daný formulář vytvořit i závěrečnou zprávu. Náležitosti závěrečné zprávy o vyřešení kybernetického bezpečnostního incidentu jsou uvedeny v § 3 odst. 3 vyhlášky a odpovídají požadavkům čl. 23 odst. 4 písm. d) NIS2. Připomínkové místo s vypořádáním souhlasí.
361. Odbor kompatibility (vláda)	D	K § 17 Odstavec 5 je zmocňovacím ustanovením, tudíž není implementační; je třeba jej odpodtrhnout a vypustit z rozdílové tabulky.	Akceptováno Připomínkové místo s vypořádáním souhlasí.

362. Odbor (vláda)	kompatibility	Z	K § 20: Ustanovení je vykazováno článkem 5 směrnice NIS 2, který se týká minimální harmonizace, a dále čl. 23 odst. 5 téže směrnice. Implementační charakter není jasný. Požadujeme vyjasnit.	Akceptováno jinak - nyní § 21 Ustanovení je vykazováno v rozdílové tabulce článkem 5 směrnice NIS 2. Tento článek upravuje minimální harmonizaci, tedy stanoví, že státy mohou přijmout národní úpravu nad rámec směrnice. Uznáváme, že není vhodné taková ustanovení uvádět jako transpoziční a nadále tomu tak nebude. Připomínkové místo s vypořádáním souhlasí.
363. Odbor (vláda)	kompatibility	D	V § 20 odst. 3 chybí za slovem „protiopatřením“ čárka.	Akceptováno - nyní § 21 Připomínkové místo s vypořádáním souhlasí.
364. Odbor (vláda)	kompatibility	D	K § 20 odst. 3 se také ptáme, co se myslí „státem uznanou povinností mlčenlivosti“. Může se jednat rovněž o mlčenlivost smluvní?	Akceptováno jinak - nyní § 21 Co se týče poskytované součinnosti, tu je možné Úřadu odepřít, bránila-li by tomu zákonná nebo státem uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti. Pojem „zákonná nebo státem uznaná povinnost mlčenlivosti“ v dotčeném ustanovení návrhu významově odpovídá pojmu „státem uložené nebo uznané povinnosti mlčenlivosti“ podle § 38 odst. 3 správního řádu či § 124 trestního zákoníku. Právě posledně zmíněné ustanovení uvádí, že „za státem uloženou nebo uznanou povinností mlčenlivosti se považuje mlčenlivost, která je uložena nebo uznána jiným právním předpisem,“ přičemž „za státem uznanou povinností mlčenlivosti se podle trestního zákona nepovažuje taková povinnost, jejíž rozsah není vymezen jiným právním předpisem, ale vyplývá z právního úkonu učiněného na základě jiného právního předpisu“. Z tohoto definičního pojetí trestního zákoníku lze vyjít také při výkladu tohoto ustanovení návrhu zákona a takto nahlíženo za zákonnou nebo státem uznanou povinností

			mlčenlivosti nelze považovat smluvně sjednanou povinnost mlčenlivosti. V tomto smyslu došlo i k doplnění důvodové zprávy k navrhovanému zákonu. Připomínkové místo s vypořádáním souhlasí.
365. Odbor kompatibility (vláda)	Z	K § 21 až § 34: V návaznosti na připomínku k § 20 máme pochybnosti, nakolik jsou uvedená ustanovení přímo implementační. Ač připouštíme, že určitý rámec může být v některých případech dán (například čl. 32 odst. 4 směrnice NIS 2 v případě § 21, § 22 a § 23; čl. 23 odst. 7 směrnice NIS 2 v případě § 21), sporné je zejména vykazování převážné většiny ustanovení jako nutně implementačních prostřednictvím článku 5 směrnice, který se týká minimální harmonizace. Článek 5 směrnice NIS 2 stanoví, že směrnice představuje svou povahou minimální harmonizaci a nebrání členským státům v tom, aby přijímaly nebo ponechaly v platnosti ustanovení zajišťující vyšší úroveň kybernetické bezpečnosti, jsou-li tato ustanovení v souladu s jejich povinnostmi stanovenými v právu Unie. Přestože článek 5 směrnice obecně umožňuje národní úpravu, která jde nad rámec směrnice, taková úprava je vnitrostátní diskrecí, a proto se příslušná ustanovení nevykazují jako implementační. Výkaznictví je hypertrofované. Ustanovení, která není možné vykázat konkrétními povinnostmi nebo konkrétními diskrecemi vyplývajícími ze směrnice NIS 2, je třeba odpodtrhnout a vypustit z rozdílové tabulky.	Akceptováno nyní § 22 až 35 V rámci celého zákona nebudou ustanovení vykazována jako transpoziční pro čl. 5. Připomínkové místo s vypořádáním souhlasí.
366. Odbor kompatibility (vláda)	D	K § 22 odst. 2 Není jasné, kdo a jak stanoví rozsah varování.	Vysvětleno - nyní § 23 Dotčené ustanovení návrhu stanoví, že varování vydává Úřad, z čehož vyplývá, že právě Úřad stanoví jeho rozsah. Rozsah bude dále vyplývat z okolností konkrétního případu, zejména povahy závažné kybernetické hrozby nebo zranitelnosti, před kterými

			bude varováno. Primárně je rozsah rovněž dán principem, na kterém varování jako institut funguje. Jeho funkcí je ohodnotit na základě informací dostupných Úřadu hodnotu zranitelnosti či hrozby, tento údaj pak sdělit povinným osobám. Ty jsou následně zavázány jej zohlednit v rámci analýzy rizik v rámci rozsahu aktiv v dané organizaci. Rozsahem aktiv v organizaci je pak to, co podporuje danou regulovanou službu. Tedy rozsah varování je implicitně dán jeho navázáním na systém řízení bezpečnosti informací a Úřad tak pouze určí hodnotu hrozby či zranitelnosti a případně navrhne možný postup k mitigaci rizika spojeného s touto hrozbou či zranitelností. Následně byla také důvodová zpráva k tomuto ustanovení doplněna o výklad k jednotlivým druhům mlčenlivosti tak, aby bylo jasnější, jaké limity jsou tomuto ustanovení stanoveny. Pokud se připomínka týkala stanovení odlišného rozsahu adresátů varování, v tomto byla důvodová zpráva doplněna o informaci, že se vztahuje toliko k variantě tento rozsah zúžit, neboť Úřad nemůže varování vlastním rozhodnutím rozšířit na subjekty mimo zákon o kybernetické bezpečnosti a stejně tak není možné varování rozšířit závazně směrem k poskytovatelům regulovaných služeb v režimu nižších povinností, jelikož tito neprovádějí povinně analýzu rizik a nemohou v ní tak ani varování zohledňovat. Připomínkové místo s vypořádáním souhlasí.
367. Odbor (vláda)	kompatibility	D	V § 23 odst. 3, a zřejmě i odstavce 4 až 6 nebudou implementační, navrhuje odpodtrhnout a nevykazovat v rozdílové tabulce. Akceptováno - nyní § 24 Připomínkové místo s vypořádáním souhlasí.
368. Odbor (vláda)	kompatibility	Z	K § 24: Návrh zákona postrádá zhodnocení vztahu ke směrnici 2014/24/EU o Akceptováno jinak – nyní § 25

		zadávání veřejných zakázek. Přitom svými ustanoveními fakticky nepřímo novelizuje ustanovení zákona č. 134/2016 Sb., o zadávání veřejných zakázek, který tuto směrnici implementuje. Ustanovení lze číst tak, že vysoutěžený dodavatel podle zákona o zadávání veřejných zakázek bude muset dodatečně plnit další požadavky z bezpečnostních opatření, které nebyly při vyhlášení výběrového řízení dané. Přitom zřejmě může jít i o zákaz využití plnění dodavatele, který již byl vysoutěžen, případně o možnost vypovědět závazek (§ 30 a § 33 návrhu). To se zdá být zcela proti transparentnosti výběrových řízení a fakticky v rozporu se zadávací směrnicí 2014/24/EU a dalšími zakázkovými směrnicemi.	Ustanovení § 25 návrhu vychází z aktuálně účinného § 4 odst. 4 zákona č. 181/2014 Sb. (změny jsou jen formulačního charakteru), úprava zohledňování požadavků na kybernetickou bezpečnost v dodavatelských vztazích je tedy v právním řádu již obsažena a praxi aplikována. Nadto nejde ani o nepřímou novelizaci zákona č. 134/2016 Sb., zhodnocení vztahu k zákonu tedy není potřeba. Odstavec 1 po povinných osobách požaduje, aby požadavky na bezpečnost svých systémů (konkrétně požadavky vyplývající z bezpečnostních opatření podle § 14 a § 15 návrhu zákona) zohledňovaly při výběru svých dodavatelů. Povinnost zohledňovat požadavky vyplývající z bezpečnostních opatření při výběru svých dodavatelů a zanášet je do uzavíraných smluv je jedním z prostředků řízení bezpečnosti dodavatelského řetězce a také požadavkem směrnice NIS 2, která po členských státech požaduje, aby zajistily začleňování opatření k řízení kybernetických bezpečnostních rizik do smluvních ujednání povinných osob s jejich přímými dodavateli a poskytovateli služeb. I pokud by toto ustanovení v návrhu obsaženo nebylo, povinné osoby by se takto měly chovat, protože jde o jeden ze vstupů do koncipování požadavků na předmět plnění, který bude ve výběrovém řízení (lhostejno zda v režimu zákona č. 134/2016 Sb. či mimo něj) poptáván. Objednatelé (v režimu zákona č. 134/2016 Sb. i mimo něj) při koncipování požadavků na předmět plnění vycházejí jednak ze svých potřeb, jednak z požadavků, které na ně kladou právní předpisy či jiné závazné akty (např. požadavky nadřízených orgánů, odběratelů služeb apod.). Stejně jako požadavky vycházející z bezpečnostních opatření podle tohoto návrhu zákona, zadavatelé musí do svých dodavatelských vztahů

		promítat i požadavky na předmět plnění vyvěrající z jiných předpisů, např. technických norem, požadavků na bezpečnost práce, požadavky vyplývající ze zákoníku práce atd. Odstavec 1 tedy nereguluje proces zadávání veřejných zakázek a tím pádem ani nemodifikuje pravidla podle zákona č. 134/2016 Sb. Aplikace odstavce 1 se u vztahů regulovaných zákonem č. 134/2016 Sb. projeví při aplikaci § 37 tohoto zákona (koncipování zadávacích podmínek a požadavků na předmět plnění). Odst. 1 nelze vnímat jako speciální vůči § 48 ZZVZ, neboť nestanovuje možnost ani povinnost vylučovat (jde o obecně koncipovanou povinnost vybírat dodavatele s ohledem na bezpečnostní potřeby zadavatele). Také odstavec 2 není vázán pouze na vztahy regulované zákonem č. 134/2016 Sb., ale je univerzálně platný pro všechny poskytovatele regulovaných služeb. Primárně se opět bude aplikovat již při výběru dodavatele (tj. ve fázi, kdy je koncipováno znění smlouvy, která je s dodavatelem uzavřena), je však relevantní i pro již existující smluvní vztahy. V takovém případě je poskytovatel regulované služby povinen učinit vše pro to, aby již uzavřené smlouvy uvedl do souladu s požadavky návrhu zákona (požadavky vyvěrajícími z bezpečnostních opatření podle § 14 a § 15 návrhu zákona). V odůvodněných případech, kdy není možné smlouvu změnit či ukončit (z toho důvodu odst. 2 používá formulaci „tam, kde je to možné“), je možné ve smluvním vztahu po nezbytně nutnou dobu pokračovat a požadovanou úroveň kybernetické bezpečnosti zajistit jiným způsobem (zejm. zavedením kompenzačních bezpečnostních opatření). Odstavec 2 nepřináší žádnou, ani nepřímou novelu § 222 nebo § 223 zákona č. 134/2016 Sb. ani jiných jeho

		ustanovení. Naopak je potřeba jej aplikovat v souladu s nimi. Pokud by zadavatel ponechal v platnosti smlouvu, která neodpovídá jeho bezpečnostním potřebám (a zároveň nepřijme žádná kompenzační opatření), bude za to moci být sankcionován podle návrhu zákona, žádným způsobem tím však nebude zasaženo do jeho povinnosti dodržet požadavky stanovené v aktuálním znění ZZVZ. Odstavec 3 přejímá dosavadní právní úpravu a opět žádným způsobem nenovelizuje zákon č. 134/2016 Sb., naopak pouze deklaruje aplikovatelnost § 36 odst. 1 zákona č. 134/2016 Sb. i na vztahy regulované návrhem zákona. Odstavec 3 neříká nic jiného, než že pokud jsou požadavky zadavatele na kybernetickou bezpečnost stanoveny v souladu s požadavky návrhu zákona a jsou odůvodněné, nemohou být shledány rozpornými s § 36 odst. 1 zákona č. 134/2016 Sb. Pokud by odstavec 3 v návrhu zákona nebyl vůbec obsažen, situace by se pro zadavatele nijak nezměnila (pořád by platilo, že požadavky na předmět plnění odůvodněné plněním povinností podle návrhu zákona nemohou být shledány rozpornými s § 36 odst. 1 zákona č. 134/2016 Sb.). Odstavec 3 je tak v zákoně obsažen především pro posílení právní jistoty zadavatelů. Pro posílení právní jistoty adresátů a vyjasnění vztahu se zákonem č. 134/2016 Sb. bude v tomto smyslu upravena důvodová zpráva k zákonu. Co se týče zohlednění omezení nebo zákazu dodavatele podle § 31 návrhu zákona, formálně vzato jde o dva odlišné instituty a je potřeba je nezaměňovat. Bezpečnostními opatřeními, jak o nich hovoří § 25, návrh zákona rozumí technická a organizační opatření podle § 14 a § 15. Od těchto bezpečnostních opatření

		je třeba odlišovat jednak protiopatření Úřadu podle § 21, jednak opatření obecné povahy podle § 31. Protiopatření Úřadu se provádí podle svého charakteru buďto napřímo (typicky reaktivní protiopatření), nebo se zohlední v procesu řízení rizik (typicky varování), tj. v rámci jednoho z bezpečnostních opatření podle § 15. Opatření obecné povahy podle § 31 bude opět podle jeho konkrétního obsahu potřeba buďto zohlednit ve výběru bezpečnostních opatření podle § 15, nebo provést napřímo. Podle toho pak bude potřeba buďto požadavky vyvěrající z opatření obecné povahy podle § 31 zohlednit při výběru dodavatele, potažmo ve smlouvách s dodavateli (za podmínek aplikace § 25 odst. 2 tak, jak je popsána výše), nebo provést napřímo (v tu chvíli jde o postup odlišný od postupu popsaného v § 25). Návrh nadto ustanovuje pro český právní řád nový zákonný důvod pro výpověď závazku ze smlouvy, nejde však o důvod specifický pro smlouvy uzavřené v režimu zákona č. 134/2016 Sb., ale o důvod univerzálně použitelný ve veřejné i soukromé sféře. Tento nový výpovědní důvod představuje speciální úpravu vůči obecným výpovědním důvodům závazkových vztahů upraveným především zákonem č. 89/2012 Sb. a navazuje na § 1998 tohoto zákona, podle kterého „závazek lze vypovědět, ujednají-li si to strany nebo stanoví-li tak zákon“. Nejedná se o nepřímou novelu zákona č. 134/2016 Sb., neboť nereguluje specificky zakázkové vztahy. Nadto § 223 odst. 5 explicitně stanoví, že „právo zadavatele ukončit závazek ze smlouvy na veřejnou zakázku podle jiných právních předpisů není tímto ustanovením dotčeno“, nelze tedy hovořit ani o rozporu se zákonem č. 134/2016 Sb. Nelze hovořit ani o rozporu se zakázkovými směrnici, neboť

			samotný čl. 73 směrnice 2014/24/EU stanovuje seznam důvodů pro ukončení smlouvy demonstrativně, jako nezbytné minimum, které je možné rozšířit („členské státy zajistí, aby veřejní zadavatelé měli možnost alespoň za níže uvedených okolností ...“), navíc tento důvod je stanoven na základě požadavků vycházejících ze zajišťování národní bezpečnosti, tj. oblasti ve výlučné dispozici členského státu. Jiný potenciální rozpor zde nespátřujeme. S ohledem na zaměření § 25 a § 34 výlučně na oblast kybernetické bezpečnosti se nám pak nejeví systémové zařadit tato ustanovení do jiných, obecných právních předpisů (např. do zákona č. 134/2016 Sb. nebo č. 89/2012 Sb.), naopak se držíme přístupu univerzálně aplikovaného v jiných právních předpisech (např. samotný odkazovaný zákon č. 134/2016 Sb. upravuje speciální úpravu vůči zákonu č. 106/1999 Sb., vůči zákonu č. 500/2004 Sb., nebo vůči občanskému zákoníku právě v rozsahu § 223). Připomínkové místo s vypořádáním souhlasí.
369. Odbor kompatibility (vláda)	D	K § 25: Ustanovení je opět vykazováno jako implementační pouze článkem 5 směrnice NIS 2. Je třeba ho odpotrhnout a nevykazovat jako implementační v rozdílové tabulce. Možnost jít nad rámec směrnice není sama o sobě implementační povahy. Podle odstavce 4 jednání o úhradě vynaložených nákladů na předání informací a dat nesmí být překážkou řádného splnění povinnosti předat informace a data. Není zřejmé, na základě čeho bude možné posoudit naplnění podmínek tohoto ustanovení.	Vysvětleno - nyní § 26 Podle tohoto ustanovení není soukromoprávní dohoda o kompenzaci podmínkou předání dat. Toto ustanovení míří na důležitost dat od významných dodavatelů a má zajistit předání (a tedy zajištění kontinuity a dostupnosti poskytované služby) v době uvedené v rozhodnutí. Významný dodavatel se podle tohoto ustanovení nemůže odvolávat na nepředání dat z toho důvodu, že mu nebyla poskytnuta kompenzace. Ustanovení nebude vykázáno jako implementační. Připomínkové místo s vypořádáním souhlasí.

370. Odbor (vláda)	kompatibility	D	K § 26: Žádáme o reformulaci definice strategicky významné služby, která je pojata kruhem. Navíc část definice je asi i v § 27 odst. 2 návrhu.	Akceptováno - nyní § 27 Na základě této i dalších připomínek jsme přistoupili k přeformulování definice strategicky významné služby v § 2 odst. 2 písm. i) návrhu zákona, a to tak, že došlo k jejímu sjednocení s definicí strategicky významné služby obsažené v § 28 návrhu zákona. Nově § 2 odst. 2 písm. i) zní: „<i>Strategicky významnou službou regulovaná služba, jejíž narušení by mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek.</i>“. Platí, že definice v § 2 odst. 2 písm. i) je obecným vymezením toho, co to strategicky významná služba je. Konkrétní kritéria strategicky významné služby jsou řešena v § 27 a 28. Připomínkové místo s vypořádáním souhlasí.
371. Odbor (vláda)	kompatibility	D	K § 27: Ustanovení odstavce 1 je zmocňovacím ustanovením, nemělo by být podtrženo a vykazováno jako implementační. Vztah směrnice NIS 2 k odstavci 2 je nejasný.	Akceptováno - nyní § 28 Celý § 27 nebude vykazován jako implementační. Připomínkové místo s vypořádáním souhlasí.
372. Odbor (vláda)	kompatibility	D	K § 28: Ustanovení navrhuje odpotrhout, zřejmě opět není přímo implementační povahy. Také upozorňujeme na nevhodnost použití slova „prioritizovat“. V odstavci 3 a odstavci 4 není možné delegovat tak významné stanovení kritérií na prováděcí právní předpis. Tyto náležitosti by měl obsahovat zákon.	Akceptováno jinak - nyní § 29 Ustanovení nebude vykazováno jako implementační. Pojem „prioritizace“ bude nahrazen slovem „upřednostňuje“. Odkaz na prováděcí právní předpis týkající se kritérií bude z návrhu zcela vypuštěn. Připomínkové místo s vypořádáním souhlasí.
373. Odbor (vláda)	kompatibility	D	K § 29: Máme za to, že zpravodajské služby či nejvyšší státní zastupitelství, popř. i jiné útvary, nebudou moci vždy na žádost Úřadu poskytnout požadované informace z důvodu plnění svých úkolů. Rovněž opět	Vysvětleno – nyní § 30 Ano, s možností, že spolupracující orgány nebudou vždy s ohledem na plnění svých dalších úkolů schopny poskytnout požadované informace pracujeme. Tato

		nemáme za to, že ustanovení je implementační.	možnost je také zohledněna v dalších ustanoveních návrhu zákona, kdy mají tyto orgány možnost poskytnutí informací odmítnout. V takových případech je pak vždy na zvážení dotčených orgánů, jak zhodnotí proporcionalitu jednotlivých povinností a případných následků, které z nich plynou. Co se týče poznámky, že ustanovení není implementační, lze konstatovat, že skutečně není. Jedná se o jedno z ustanovení, které do zákona vnáší mechanismus prověřování dodavatelských řetězců, což je úkol, který byl NÚKIB uložen usnesením č. 41 Bezpečnostní rady státu ze dne 21. 6. 2022. Připomínkové místo s vypořádáním souhlasí.
374. Odbor kompatibility (vláda)	Z	K § 30: Jak uvádíme výše k § 24, máme pochybnosti, že je navržena úprava, podle které vítězi zadávacího řízení může NÚKIB zakázat plnění po skončení zadávacího řízení, v souladu se směrnicí 2014/24/EU, popř. dalšími zadávacími směrnicemi, a potažmo zákonem o zadávání veřejných zakázek.	Vysvětleno - nyní § 31 Nad rámec vypořádání uvedeného u připomínky k § 25 uvádíme, že NÚKIB nebude prostřednictvím opatření obecné povahy dle návrhu § 31 nového zákona o kybernetické bezpečnosti zakazovat využití plnění z veřejné zakázky, resp. zakazovat dodávku od konkrétního dodavatele <i>en bloc</i>. NÚKIB může pouze zakázat nebo dále podmínit využití této dodávky (resp. její části - bezpečnostně významné dodávky) ve vymezené části infrastruktury - kritické části stanoveného rozsahu, využití dodávky mimo tento rozsah ale opatřením dle § 31 omezit nelze. Případné vyloučení dodavatele na základě vydaného opatření obecné povahy může v tomto ohledu provést pouze zadavatel veřejné zakázky. Tzn. do plnění veřejné zakázky a již uzavřených smluv OOP vůbec zasáhnout nemusí, pokud je možné využít plnění v jiných částech infrastruktury. Pokud by jej jinde možné využít nebylo, smlouva se pro zadavatele stane od určitého okamžiku nepotřebnou a lze

			uvažovat o využití nově konstituovaného výpovědního důvodu. Co se týče potenciálního rozporu nového výpovědního důvodu (faktickou novelou § 223 ZZVZ) s čl. 73 směrnice 2014/24/EU, seznam důvodů pro ukončení smlouvy je zde stanoven demonstrativně, jako nezbytné minimum, které je možné rozšířit („<i>členské státy zajistí, aby veřejní zadavatelé měli možnost alespoň za níže uvedených okolností ...</i>“), navíc tento důvod je stanoven na základě požadavků vycházejících ze zajišťování národní bezpečnosti, tj. oblasti ve výlučné dispozici členského státu. Jiný potenciální rozpor zde nespatřujeme. Tyto závěry byly konzultovány rovněž s Ministerstvem pro místní rozvoj, které je odborným garantem zákona o zadávání veřejných zakázek, a s Úřadem pro ochranu hospodářské soutěže. Připomínkové místo s vypořádáním souhlasí.
375. Odbor kompatibility (vláda)	D	K § 32 odst. 1 písm. a): Žádáme o vysvětlení pojmu „vynaložení přiměřeného úsilí“. Kdo jej bude hodnotit? Navíc je na toto ustanovení navázána sankce v § 58 odst. 3, což u takto vágně stanovené povinnosti není hájitelné.	Vysvětleno - nyní § 33 Pojem „přiměřené úsilí“ je tzv. neurčitým právním pojmem, kterému v zákoně (s nutným dopadem na právní jistotu) opravdu neodpovídá přesná definice, nicméně tento pojem je v zákoně použit záměrně, a to z důvodu potřeby orgánu, který aplikuje konkrétní ustanovení, zohlednit všechna specifika konkrétního případu, více k tomuto najdete níže. Ustanovení § 60 odst. 3 bylo na základě této a dalších připomínek přetextováno a nadále se v něm s pojmem „přiměřeného úsilí“ neuzívá. K posílení právní jistoty přiměřenosti vyvinutého úsilí by měla přispět rovněž výkladová praxe, například v

		podobě metodických a výkladových materiálů, které Úřad vydá. Z uvedeného vyplývá, že přiměřené úsilí lze právě bez přihlédnutí k jednotlivostem konkrétního případu definovat nanejvýš v přibližných obrysech. Na druhou stranu se jedná o pojem, která je zaužíván napříč právním řádem České republiky, a to i vymezením se proti svému opaku (nepřiměřené úsilí, viz níže uvedená soudní rozhodnutí). V tomto smyslu odkazujeme např. na § 14 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, v účinném znění, § 27c zákona č. 121/2000 Sb., autorského zákona, v účinném znění, § 104 odst. 13 zákona č. 127/2005 Sb., o elektronických komunikacích, v účinném znění, § 24e odst. 2 písm. a) bod 2 zákona č. 143/2001 Sb., o ochraně hospodářské soutěže, v účinném znění, právní větu usnesení Nejvyššího soudu České republiky ze dne 27. 3. 2019 sp. zn. 27 Cdo 3855/2017 či právní větu III rozsudku Nejvyššího soudu České republiky ze dne 5. 12. 2013 sp. zn. 9 Aps 11/2013. V této souvislosti je namístě zmínit, že v komentáři [Lavický, P. a kol. Občanský zákoník I. Obecná část (§ 1–654). Komentář. 2. vydání. Praha: C. H. Beck, 2022, s. 85] k uvedenému § 14 odst. 2 občanského zákoníku stojí následující: <i>„Přiměřenost je v tomto případě posuzována měřítkem osoby, která by se nacházela ve stejné situaci. Ustanovení § 14 odst. 2 nesměruje k ryze subjektivnímu chápání přiměřenosti, neboť sice odkazuje na okolnosti konkrétního případu, avšak zároveň se odvolává na osobu nacházející se ve stejném postavení. Je zřejmé, že tato modelová osoba je zásadně průměrným člověkem ve smyslu § 4 odst. 1. Jinak řečeno, přiměřenost se posuzuje sice s ohledem na konkrétní okolnosti každého případu, ale objektivně, tedy tak, jak by se za těchto okolností měla</i>

			<i>přiměřeně zachovat průměrná osoba. Formulace druhého odstavce § 14 není tedy ničím jiným než rozvedením § 4 odst. 1. Zmiňuje-li § 14 odst. 2, že se úsilí a prostředky mají jevit průměrně rozumnému člověku nacházejícímu se na téže místě jako přiměřené, je tím zároveň řečeno, že prostředky a úsilí, které jsou v rámci svépomoci vynakládány, nemusejí být v přísné rovnováze s prostředky, jimiž je veden zásah. Svou roli může hrát překvapení, rozrušení, strach, denní doba a místo, na němž k zásahu dochází, atd., tedy okolnosti v nejširším slova smyslu.“</i> Připomínkové místo s vypořádáním souhlasí.
376. Odbor kompatibility (vláda)	Z	K § 33: V návaznosti na základní připomínku k § 24 a § 30 žádáme o zhodnocení slučitelnosti se směrnicí 2014/24/EU, popřípadě dalšími zakázkovými směrnicemi. Ustanovení máme za rozporné s právem EU.	Vysvětleno - nyní § 34 Nad rámec vypořádání u připomínek k § 25 a § 31, na které plně odkazujeme, uvádíme, že i v případě, kdy by bylo nutné hodnotit vztah návrhu zákona se směrnicí 2014/24/EU, nepovažujeme ustanovení § 25 a 31 za rozporné s touto směrnicí, ani jinými zakázkovými směrnicemi, potažmo zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, který unijní úpravu reflektuje. Státy EU mohou zavádět opatření, která jsou nad rámec povinností vyplývajících ze směrnic a unijního práva vůbec. Sama směrnice 2014/24/EU v bodě 41 úvodních ustanoveních hovoří mimo jiné o tom, že by neměla bránit zavedení nebo uplatňování opatření nutných k ochraně veřejné bezpečnosti, a to zejména s ohledem na udržitelný rozvoj (to však za podmínky, že takováto opatření jsou v souladu se Smlouvou o fungování EU).

			Lze tedy konstatovat, že směrnice 2014/24/EU připouští možnost regulace zadávacích (výběrových) postupů na vnitrostátní úrovni tak, aby byl naplněn bezpečnostní standard daného státu (příčemž obecně lze sledovat trend spíše zvyšující se regulace na poli kybernetické bezpečnosti – jakožto svébytné podmnožiny bezpečnosti státu jako takové – a tudíž lze očekávat přísnější pravidla, která posílí prevenci proti potenciálně hrozcím útokům na regulované služby). S ohledem na uvedené je tedy v zásadě možné považovat navrženou úpravu § 25 a 31 návrhu zákona za souladnou s právem EU, jelikož EU nelimituje bezpečnostní politiku daného státu jinak než pouze minimálními požadavky na takovou bezpečnost. Pokud je v určitém státě vůle vytvořit „přísnější“ podmínky oproti danému minimu, pak by žádná směrnice neměla udávat překážky k jejich přijetí. Jak již bylo řečeno výše, směrnice 2014/24/EU takovou možnost reflektuje zejména v bodě 41 úvodních ustanovení. Rovněž se pak lze odkázat i na základní zásady, na kterých má EU fungovat. Připomínkové místo s vypořádáním souhlasí.
377. Odbor kompatibility (vláda)	D	K § 34: Ustanovení v <u>odstavci 1</u> mluví o „stanoveném rozsahu“, a „stanoveném čase“ a „kvalitě“, nicméně z návrhu není jasné, kdo tento rozsah, časový limit či kvalitu určí. K <u>odstavci 2</u> vznášíme dotaz, jak má poskytovatel <i>testovat</i> schopnost zajištění poskytované strategicky významné služby a kde jsou stanovena kritéria takového testování. <u>Odstavec 3</u> obsahuje svou povahou přechodné ustanovení, které nemá oporu ve směrnici.	Nyní § 35 K odstavci 1: Vysvětleno Připomínkované ustanovení § 35 bylo v odstavci 1 upraveno tak, že „<i>Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v nezbytném rozsahu, v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky.</i>“. Tento nezbytný rozsah pak bude stanoven vyhláškou Úřadu.

		<u>Odstavec 4</u> odkazuje na prováděcí právní předpis, nicméně podle našeho názoru tyto parametry by měly být alespoň rámcově upraveny zákonem. Jak uvádíme výše, ustanovení nepovažujeme za implementační na základě článku 5 směrnice NIS 2.	Stanovený čas a kvalitu si stanovuje poskytovatel strategicky významné služby sám vyhláškou definovaným způsobem, kdy se v návrhu vyhlášky o opatřeních poskytovatele regulované služby v režimu vyšších povinností, a to konkrétně v § 16 odst. 2, stanoví, že: „<i>Cíle řízení kontinuity podle odst. 1 písm. c) tohoto ustanovení jsou stanoveným časem a kvalitou regulované služby podle § 35 zákona. Stanoveným časem je doba obnovení chodu podle odst. 1 písm. c) bod 2. tohoto ustanovení a stanovenou kvalitou regulované služby je minimální úroveň poskytovaných služeb podle odst. 1 písm. c) bod i) tohoto ustanovení.</i>“ K odstavci 2: Vysvětleno Cílem ustanovení § 35 odst. 2 je zajistit, že poskytovatel strategicky významné služby bude pravidelně prověřovat, že má nastavené procesy a opatření k tomu, aby byl v případě potřeby schopen zajistit poskytování strategicky významné služby v nezbytném rozsahu z území České republiky. Požadavky na konkrétní podobu takového prověření zákon nestanoví a ani to není úmyslem navrhovatele. Vzhledem k různorodosti strategicky významných služeb nemá předkladatel ambici stanovovat v tuto chvíli konkrétní požadavky v tomto ohledu a je tedy dána určitá volnost poskytovatelům strategicky významných služeb, aby zvolili takový postup prověřování schopnosti zajistit dostupnosti strategicky významných služeb z území České republiky, který je v případě té či oné služby vhodný. Z pohledu navrhovatele je ale důležité, aby o takovém prověření vznikl dokumentovaný záznam, aby bylo možné ověřit plnění této povinnosti v rámci kontroly.

			K odstavci 3: Vysvětleno Tato přechodná lhůta opravdu nemá oporu ve směrnici, jelikož ani povinnost, jejíž splnění odkládá, nemá oporu ve směrnici. Předkladatel zákona nicméně má za to, že by vymáhání splnění připomínkové povinnosti ihned s účinností zákona představovalo nepřiměřenou zátěž pro poskytovatele strategicky významných služeb. K odstavci 4: Neakceptováno Vzhledem k tomu, že stanovený čas a kvalitu si stanovuje poskytovatel strategicky významné služby sám vyhláškou definovaným způsobem, kdy se v návrhu vyhlášky o opatřeních poskytovatele regulované služby v režimu vyšších povinností, a to konkrétně v § 16 odst. 2, stanoví, že: „<i>Cíle řízení kontinuity podle odst. 1 písm. c) tohoto ustanovení jsou stanoveným časem a kvalitou regulované služby podle § 35 zákona. Stanoveným časem je doba obnovení chodu podle odst. 1 písm. c) bod 2. tohoto ustanovení a stanovenou kvalitou regulované služby je minimální úroveň poskytovaných služeb podle odst. 1 písm. c) bod i) tohoto ustanovení.</i>“. Předkladatel se tak nedomnívá, že by bylo nutné tyto pojmy více rozvádět v textu návrhu zákona. Ustanovení nebude považováno za implementační. Připomínkové místo s vypořádáním souhlasí.
378. Odbor kompatibility (vláda)	D	K § 36: Žádáme nahradit slova „s právními předpisy“ na „s přímo použitelnými předpisy“. Nemá být ale zmíněn rovněž zákon o osobních údajích navazující na GDPR?	Akceptováno - nyní § 37 Odkaz byl upraven následujícím způsobem: „v souladu s právním předpisem upravujícím ochranu osobních údajů a s přímo použitelným předpisem Evropské unie⁷⁾ Poznámka pod čarou č. 7 zní:

			<i>Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).“.</i> Připomínkové místo s vypořádáním souhlasí.
379. Odbor kompatibility (vláda)	D	K § 37: Ustanovení je svou povahou nepřímou novelou zákon o svobodném přístupu k informacím. Žádáme napravit.	Neakceptováno – nyní § 38 V rámci tohoto mezirezortního připomínkového řízení byl osloven gestor problematiky Ministerstvo vnitra nad dalším řešením této otázky. Z pracovního jednání vyplynulo, že na problematiku výjimky ze zákona o svobodném přístupu k informacím pohlíží gestor jako na vhodný způsob řešení. Zákon o svobodném přístupu k informacím slouží dle jeho slov jako obecný předpis zaměřující se především na procesní ustanovení neposkytování informací a neobsahuje všechny výjimky v rámci českého právního řádu. Obdobné výjimky obsahuje zákon o zadávání veřejných zakázek, nebo i nově připravovaná novelizace krizového zákona a další. V případě přesunu daného ustanovení do zákona o svobodném přístupu k informacím se naopak gestor obává rozšíření a znefunkčnění současného stavu, ruku v ruce s nemožností precizně definovat výjimku tak, jak je nyní. Ministerstvo vnitra tedy dle našeho pochopení závěrů tohoto jednání zastává postoj, aby výjimka zůstala ve speciálním zákoně. NUKIB považuje tento postoj gestora za směřodátný. Připomínkové místo s vypořádáním souhlasí.
380. Odbor kompatibility (vláda)	Z	K § 39: Nejeví se jako přípustné, aby o vyhlášení stavu kybernetického	Vysvětleno - nyní § 40

		nebezpečí rozhodoval sám ředitel Úřadu a ne vláda, a to s ohledem na kontext, že po vyhlášení stavu kybernetického nebezpečí může pouze ředitel Úřadu stanovit taková zásadní omezení, jako je například nařízení práce v pohotovostním režimu, či přednostní poskytnutí personálních kapacit nebo věcných prostředků (viz § 40). Pouhým rozhodnutím ředitele NÚKIB může tedy být zásadně zasaženo do práv a povinností zákonem vymezených osob.	Na vhodném znění celé soustavy ustanovení o stavu kybernetického nebezpečí spolupracujeme s Ministerstvem vnitra – Generálním ředitelstvím Hasičského záchranného sboru a návrh bude upraven na základě těchto jednání. Navrhovaná právní úprava nemá za cíl zasahovat do práv způsobem, který by odpovídal nouzovému stavu, tj. zásah v intenzitě nouzového stavu je ponechán vládě a není svěřen do rukou ředitele Úřadu. V případě zmíněných ustanovení došlo s ohledem na výše uvedené k úpravám. Máme za to, že úpravy stavu kybernetického nebezpečí přináší nyní už jen taková opatření, která jsou srovnatelná s např. mimořádným stavem nouze v energetice, a proto je možné, aby jej vyhlášoval ředitel Úřadu sám. Připomínkové místo s vypořádáním souhlasí.
381. Odbor kompatibility (vláda)	D	K § 40 odst. 1 písm. d): Žádáme vysvětlit, jak je myšleno nařízení práce ředitelem NÚKIB v pohotovostní režimu (komu?, co je pohotovostní režim?) a jaký je vztah k zákoníku práce. Jednotlivými krizovými opatřeními může být zasahováno do práv a svobod občanů ČR, které garantují Ústava ČR a Listina základních práv a svobod.	Vysvětleno - nyní § 41 Obsah § 41 byl v rámci spolupráce s gestorem problematiky krizového řízení - Ministerstvem vnitra, Generálním ředitelstvím Hasičského záchranného sboru, upraven. Nově se nebude jednat o práci v pohotovostním režimu, nýbrž o pracovní pohotovost ve smyslu pracovněprávních předpisů. Připomínkové místo s vypořádáním souhlasí.
382. Odbor kompatibility (vláda)	Z	K § 41: <u>V odstavci 1</u> tohoto ustanovení poslední dvě věty nemají implementační povahu. <u>Chybí implementace čl. 31 odst. 4 směrnice</u>, kde je zakotvena funkční nezávislost Úřadu, což tradičně implikuje zákaz přijímání pokynů (viz např. § 17 odst. 3 energetického zákona, i jinde).	Nyní § 44 Ad 1: Akceptováno Ad 2: Vysvětleno Máme za to, že současně účinné znění § 22 zákona o kybernetické bezpečnosti, stejně tak jako navrhované znění § 44 (v původním návrhu § 41) naplňuje

			požadavek na transpozici zmíněného článku. Návrhem zákona je jasně dáno, že kontrola má probíhat podle zákona a v mezích zákona, přičemž není prostor pro ovlivňování výkonu kontroly. NÚKIB je už dnes při výkonu kontroly a ukládání sankcí nezávislý. V minulosti s tímto ani neexistoval náznak pochybnosti, že by tomu tak nemělo být. NÚKIB ukládá pokuty ostatním orgánům státní správy, stejně tak jako celá řada státních orgánů dává sankce jiným státním orgánům, aniž by to muselo být nutně uvedeno podrobným ustanovením o nezávislosti v rámci daného předpisu. Máme také za to, že protože výnosy vlády (která i přesto že je vrcholným orgánem státní správy) nejsou nad zákonem, resp. že předseda vlády je toliko dle současného i navrhovaného znění nadřízeným ředitelem NÚKIB, nicméně jejich role je toliko koordinační a informační, a proto premiér nemá možnost ovlivňovat výkon zákonné působnosti. Připomínkové místo s vypořádáním souhlasí.
383. Odbor kompatibility (vláda)	Z	K § 41 odst. 4 písmeno f) Lze uvést, že uvedené ustanovení má subsumovat několik dílčích povinností, mj. i vysílání zástupců členských států (ČR) do jednotlivých orgánů či skupin (čl. 15 bod 2 a čl. 16 bod 2 směrnice NIS 2) pro účely řešení kybernetických krizí. Máme za to, že ustanovení by mělo být rozepsáno.	Akceptováno - nyní § 44 Ustanovení bylo rozepsáno následujícím způsobem: „f) plní povinnosti vůči Evropské komisi, Agentuře Evropské unie pro kybernetickou bezpečnost, Agentuře Evropské unie pro Kosmický program, Skupině pro spolupráci, Síti Computer Security Incident Response Team (dále jen „Síť CSIRT“), Evropské síti styčných organizací pro řešení kybernetických krizí a dalším subjektům podle příslušného předpisu Evropské unie¹⁴⁾“. Poznámka pod čarou č. 14 odkazuje na směrnice NIS 2. Připomínkové místo s vypořádáním souhlasí.

384. Odbor (vláda)	kompatibility	Z	K § 41 Dále není jasné, co se míní příslušným předpisem Evropské unie v <u>odstavci 4 písm. f) a g)</u>. Mínil se tím přímý odkaz na směrnici? To je nutné vyjasnit a uvést jednoznačně, například v písm. g) doplnit „...je příslušným orgánem pro řešení kybernetických krizí podle...“. Je záměrem udělat odkaz jako v případě poznámky pod čarou č. 20?	Akceptováno - nyní § 44 Do ustanovení § 44 odst. 4 písm. f) a g) byl přidán odkaz na poznámku pod čarou odkazující přímo na směrnici NIS 2. Vypořádání písmene f) výše. V případě písmene g) byl doplněn odkaz na poznámku pod čarou, která obsahuje přímý odkaz na čl. 8 směrnice NIS 2 obsahující jak pojem „jednotné kontaktní místo“, tak pojem „příslušný orgán“, stejně tak jako bylo doplněno ustanovení o vysílání zástupců do těchto organizací. Připomínkové místo s vypořádáním souhlasí.
385. Odbor (vláda)	kompatibility	Z	K § 41 Také v <u>odstavci 4 písm. h)</u> je nutné vyjasnit, na který předpis EU se odkazuje. Má se jednat o hodnocení v rámci skupiny pro spolupráci podle směrnice NIS 2?	Akceptováno - nyní § 44 Do ustanovení § 44 odst. 4 písm. h) byl přidán odkaz na poznámku pod čarou odkazující přímo na směrnici NIS 2. K němu byl doplněn odkaz na poznámku pod čarou, která obsahuje přímý odkaz na čl. 19 směrnice NIS 2 obsahující zmíněné „vzájemné hodnocení“ (opět jako přímý pojem ze směrnice NIS 2). Připomínkové místo s vypořádáním souhlasí.
386. Odbor (vláda)	kompatibility	Z	K § 41 <u>Odst. 4 písm. k)</u> odkazuje na „akt o kybernetické bezpečnosti“, čímž míní nařízení 2019/881. Legislativní zkratku, kterou toto ustanovení přebírá z uvedeného nařízení, takto použít nelze, když není návrhem zákona zavedena. Dále, nemá se odkazovat na článek 51, nikoliv 58? Požadujeme upravit.	Akceptováno jinak - nyní § 44 odst. 4 písm. l) Odkaz na "akt o kybernetické bezpečnosti" byl upraven tak, že byla doplněna poznámka pod čarou a do ní vložen následující text: "Nařízení Evropského parlamentu a Rady (EU) 2019/881". V navrhovaném čl. 51 jsou upraveny cíle evropského systému certifikace kybernetické bezpečnosti, odkaz na něj je v rozdílové tabulce uveden chybně, správně má být vykázan čl. 58 odst. 1. Rozdílová tabulka byla v tomto smyslu upravena. Připomínkové místo s vypořádáním souhlasí.

387. Odbor kompatibility (vláda)	D	K § 41 K odst. 4 písm. m) uvádíme, že toto ustanovení není uvedeno v rozdílové tabulce. Písmeno l) zase v rozdílové tabulce není citováno stejně jako v návrhu (jiný odkaz na poznámku pod čarou).	Akceptováno jinak- nyní § 44 odst. 4 písm. n) § 41 odst. 4 písm. n) je v rozdílové tabulce vykázán jako transpoziční ustanovení pro čl. 29 směrnice NIS 2. V případě písm. m) [dříve l]) bylo upraveno číslo poznámky pod čarou. Připomínkové místo s vypořádáním souhlasí.
388. Odbor kompatibility (vláda)	D	K § 41 K odst. 5 písm. i) uvádíme, že není vhodné stanovovat rozhodnutím vládního CERTu povinnosti všeobecné povahy. Dále není jasné, jaký je vztah národního CERTu k vládnímu CSIRT. To se týká i další připomínky.	Akceptováno- nyní § 44 Vládní CERT je součástí Úřadu a je koncipován jako veřejnoprávní „single point of contact“ pro oblast kybernetické bezpečnosti. Jeho činnosti jsou popsány v § 44 odst. 5 návrhu zákona o kybernetické bezpečnosti, přičemž v rámci své činnosti nakládá s citlivými informacemi. V případě, že je to nezbytné pro zajištění kybernetické bezpečnosti, je možné některé údaje a informace sdílet, přičemž podle povahy sdílených informací je také potřeba tyto informace patřičně chránit. Ustanovení bylo na základě připomínky přeformulováno na stanovení podmínek využití informací (v praxi běžné nastavení TLP). Využití tohoto institutu je zároveň omezeno pouze na případy, kdy je to nezbytné pro zajištění kybernetické bezpečnosti. Národní CERT naproti tomu není orgán veřejné moci a jeho pravomoci jsou odvozeny z veřejnoprávní smlouvy. Národní CERT tedy není omezen zásadou enumerativnosti veřejnoprávních pretenzí a k dosažení účelu navrhovaného zákona může z pozice osoby soukromého práva provádět činnosti z vlastní iniciativy v mezích zákona. Vládní a Národní CERT mezi sebou spolupracují na řešení incidentů týkajících se kybernetické bezpečnosti v sítích provozovaných v České republice. Jednotlivě působí jako kontaktní

			místa pro poskytovatele regulovaných služeb v režimu vyšších či nižších povinností. Základním východiskem je tak spolupráce a vzájemné doplňování těchto dvou týmů, což se promítá i v jejich podílení se na fungování mezinárodních uskupení v oblasti kybernetické bezpečnosti, včetně Sítě CSIRT, případně pak také spolupráce Úřadu a Národního CERT na procesu vzájemného hodnocení. Připomínkové místo s vypořádáním souhlasí.
389. Odbor kompatibility (vláda)	Z	K § 42 Ustanovení paragrafu 42, která se týká provozovatele Národního CERT, jsou vykazována stejnými ustanoveními směrnice NIS 2 (článek 10 či článek 11), jako ustanovení týkající se Vládního CERTu, popřípadě Úřadu. Obojí je tedy vykazováno nejčastěji jako implementační vůči „týmům CSIRT“. Zdá se tedy, že navrhovaná úprava upravuje totéž a dubluje se. Konkrétně například § 42 odst. 3 písm. h) se zdá upravovat to samé, co § 41 odst. 5 písm. j). § 42 odst. 3 písm. i) se zdá upravovat totéž, co § 41 odst. 4 písm. h). Požadujeme vysvětlit.	Vysvětleno - nyní § 45 Príslušná ustanovení obsahují stejné povinnosti, vycházející z čl. 11 směrnice NIS2, přičemž podle odst. 1, věty poslední se týmy CSIRT mohou zapojovat do mezinárodních sítí pro spolupráci. Vzhledem k jejich rozdílným úkolům dle zákona lze očekávat, že se zkušenosti obou týmů budou lišit a může být přínosné, aby v mezinárodních sítích pro spolupráci byly zastoupeny oba. Stejně tak je žádoucí, aby v procesu vzájemného hodnocení byl zapojen jak Úřad jako celek, tak i Národní CERT, neboť oba celky mohou přinést cenné poznatky a doporučení směřující k posílení celkové schopnosti v oblasti kybernetické bezpečnosti dle recitálu 75 směrnice NIS 2. Z výše uvedeného vyplývá, že nelze tyto činnosti více odlišit a konkretizovat, neboť se týkají víceméně stejných oblastí, byť plněných ve spojení s jinou množinou subjektů. Připomínkové místo s vypořádáním souhlasí.
390. Odbor kompatibility (vláda)	Z	K § 42 odst. 1 písm. q)	Vysvětleno - nyní § 45 odst. 4 písm. g)

		Ustanovení stanoví, že provozovatelem Národního CERT může být pouze právnická osoba, která není zahraniční osobou podle jiného právního předpisu. Předpokládáme, že takovéto silné omezení z hlediska přístupu osob k výdělečné činnosti je odůvodňováno bezpečnostními hledisky. Jak bude ale zacházeno s právnickou osobou, která je ovládaná ze zahraničí? Ustanovení zakládá nekonzistentní přístup, který může být problematicky hájitelný z hlediska svobod vnitřního trhu.	Takovéto omezení je odůvodňováno bezpečnostními potřebami a zároveň také jednodušší a efektivnější procesní stránkou s ohledem na jurisdikci. Na základě této připomínky bylo přidáno ustanovení o povinnosti provozovatele Národního CERT být držitelem platného osvědčení podnikatele pro přístup k utajovaným informacím pro stupeň utajení Důvěrné podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, což umožňuje také přehlednější kontrolu nejen ostatních požadavků návrhu zákona na provozovatele Národního CERT, zejména pak podmínky nevyvíjení činnosti proti zájmu České republiky. V rámci tohoto řízení je mimo jiné také zohledňován vliv na rozhodování. Zároveň je na místě podotknout, že dle veřejnoprávní smlouvy uzavřené mezi NBÚ a CZ.NIC (dostupné na stránkách provozovatele Národního CERT) je činnost provozovatele Národní CERT provozována bezúplatně. Nad rámec výše uvedeného došlo na základě připomínek ke změně textu příslušného ustanovení na „<i>nemá sídlo mimo území České republiky</i>“. Připomínkové místo s vypořádáním souhlasí.
391. Odbor kompatibility (vláda)	D	K § 42 Dále upozorňujeme, že není zřejmé, co se rozumí „zahraniční osobou podle jiného předpisu“. Pojem zahraniční osoba používá řada předpisů. Doporučujeme proto slova „podle jiného právního předpisu“ z návrhu vypustit s tím, že lze v daném případě použít obecné pravidlo stanovené v § 26 odst. 1 zákona č. 91/2012 Sb., o mezinárodním právu soukromém.	Akceptováno jinak - nyní § 45 V návrhu zákona přepsáno na "nemá sídlo mimo území České republiky" Připomínkové místo s vypořádáním souhlasí.
392. Odbor kompatibility (vláda)	D	K § 42 odst. 3 písm. h) a i) Viz připomínka k odkazům na konkrétní předpis EU výše.	Akceptováno - nyní § 45 odst. 1 písm. h) a i)

			Byli doplněny odkazy na konkrétní články směrnice NIS 2. V případě § 42 odst. 3 (nově § 45 odst. 3 písm. h) se jedná o čl. 10, v případě písm. i) se jedná o čl. 19. Připomínkové místo s vypořádáním souhlasí.
393. Odbor kompatibility (vláda)	D	K § 44 odst. 2: V odstavci 2 nemá poslední věta implementační charakter. Nepovažujeme za správné ustanovení podtrhávat a vykazovat jako implementační.	Akceptováno - nyní § 47 Připomínkové místo s vypořádáním souhlasí.
394. Odbor kompatibility (vláda)	D	K § 45 odst. 2: Žádáme vysvětlit, jak bude interpretováno „vynaložení přiměřeného úsilí“. Viz i připomínka k „přiměřenému úsilí“ výše.	Vysvětleno - nyní § 48 Pojem „přiměřené úsilí“ je tzv. neurčitým právním pojmem, kterému v zákoně (s nutným dopadem na právní jistotu) neodpovídá přesná definice. Důvodem je potřeba orgánu, který aplikuje konkrétní ustanovení, zohlednit všechna specifika konkrétního případu. Z uvedeného vyplývá, že přiměřené úsilí lze právě bez přihlédnutí k jednotlivostem konkrétního případu definovat nanejvýš v přibližných obrysech. Na druhou stranu se jedná o pojem, který je užíván napříč právním řádem České republiky, a to i vymezením se proti svému opaku (nepřiměřené úsilí, viz níže uvedená soudní rozhodnutí). V tomto smyslu odkazujeme např. na § 14 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, v účinném znění, § 27c zákona č. 121/2000 Sb., autorského zákona, v účinném znění, § 104 odst. 13 zákona č. 127/2005 Sb., o elektronických komunikacích, v účinném znění, § 24e odst. 2 písm. a) bod 2 zákona č. 143/2001 Sb., o ochraně hospodářské soutěže, v účinném znění, právní větu usnesení Nejvyššího soudu České republiky ze dne 27. 3. 2019 sp. zn. 27 Cdo 3855/2017 či právní větu III rozsudku Nejvyššího soudu České republiky ze dne 5. 12. 2013 sp. zn. 9 Aps 11/2013. V této

			souvislosti je namístě zmínit, že v komentáři [Lavický, P. a kol. Občanský zákoník I. Obecná část (§ 1–654). Komentář. 2. vydání. Praha: C. H. Beck, 2022, s. 85] k uvedenému § 14 odst. 2 občanského zákoníku stojí následující: „Přiměřenost je v tomto případě posuzována měřítkem osoby, která by se nacházela ve stejné situaci. Ustanovení § 14 odst. 2 nesměruje k ryze subjektivnímu chápání přiměřenosti, neboť sice odkazuje na okolnosti konkrétního případu, avšak zároveň se odvolává na osobu nacházející se ve stejném postavení. Je zřejmé, že tato modelová osoba je zásadně průměrným člověkem ve smyslu § 4 odst. 1. Jinak řečeno, přiměřenost se posuzuje sice s ohledem na konkrétní okolnosti každého případu, ale objektivně, tedy tak, jak by se za těchto okolností měla přiměřeně zachovat průměrná osoba. Formulace druhého odstavce § 14 není tedy ničím jiným než rozvedením § 4 odst. 1. Zmiňuje-li § 14 odst. 2, že se úsilí a prostředky mají jevit průměrně rozumnému člověku nacházejícímu se na témže místě jako přiměřené, je tím zároveň řečeno, že prostředky a úsilí, které jsou v rámci svépomoci vynakládány, nemusejí být v přísné rovnováze s prostředky, jimiž je veden zásah. Svou roli může hrát překvapení, rozrušení, strach, denní doba a místo, na němž k zásahu dochází, atd., tedy okolnosti v nejširším slova smyslu.“ Uvedený výklad byl na základě Vaší připomínky doplněn do důvodové zprávy, jmenovitě do pasáže týkající se § 33, kde se pojem "přiměřené úsilí" objevuje poprvé. Připomínkové místo s vypořádáním souhlasí.
395. Odbor kompatibility (vláda)	D	K § 46 odst. 2: Obdobně jako u § 41 odst. 4 písm. k) žádáme napravit citaci aktu o	Akceptováno - nyní § 49

		kybernetické bezpečnosti v souladu s výše uvedeným.	Odkaz na "akt o kybernetické bezpečnosti" byl upraven tak, že byla v novém § 49 odst. 1 (původně § 46) zavedena legislativní zkratka pro nařízení Evropského parlamentu a Rady (EU) 2019/881), aby mohlo být na jednotlivé články odkazováno přímo v textu a ustanovení bylo přehledné, vzhledem k tomu, že v ustanovením se objevuje také přímo použitelný předpis Evropské unie přijatý na základě právě aktu o kybernetické bezpečnosti. Připomínkové místo s vypořádáním souhlasí.
396. Odbor kompatibility (vláda)	D	K § 47 odst. 1 – poznámky pod čarou č. 7 a 8, a další poznámky pod čarou: Odkaz na poznámky pod čarou č. 7 a 8 nemusí uvádět datum přijetí předpisů EU, stačí zkrácený název. Po uvedení článků nařízení by mělo následovat malé „n“. Zkrácený název u předpisů EU uvedených již v návrhu zejména v poznámkách pod čarou č. 1 a 2 platí i pro další místa návrhu – poznámku pod čarou č. 14, 15 či 16 a 20.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
397. Odbor kompatibility (vláda)	Z	K § 70 odst. 1: Ustanovení není vyznačeno podtržením, ale zřejmě má navazovat na článek 4 směrnice NIS 2. Toto ustanovení směrnice zakládá nepřímou novelu v rámci práva EU, což je obtížně převoditelné do českého právního řádu. Žádáme nahradit slova „přímo použitelný právní předpis Evropské unie“ slovy „přímo použitelný předpis Evropské unie nebo jiný právní předpis“. Slova přímo použitelný předpis jsou zaužívaná podle LPV. Jiný právní předpis proto, že zřejmě bude potřeba odkázat i na české právní předpisy, do kterých byly transponovány směrnice.	Akceptováno jinak Slova "přímo použitelný právní předpis Evropské unie" byla nahrazena slovy "přímo použitelný předpis Evropské unie nebo jiný právní předpis, který zpracovává příslušný předpis Evropské unie". Stejným způsobem pak byl upraven i odst. 2. Formulace "jiný právní předpis, který zpracovává příslušný předpis Evropské unie" je zpřesňující a jasně stanoví, že se jedná o takový právní předpis, který transponuje evropskou směrnici nebo adaptuje evropské nařízení. Připomínkové místo s vypořádáním souhlasí.

398. Odbor (vláda)	kompatibility	D	K čl. 1 bodu 2 směrnice: Jsme názoru, že provedení tohoto článku není nutné vykazovat.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
399. Odbor (vláda)	kompatibility	D	K čl. 2 bodu 1 směrnice: Jsme názoru, že provedení tohoto článku směrnice pouze prováděcím právním předpisem není dostatečné, viz výše.	Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech [§ 3 a § 2 písm. d)], tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby [§ 3, ve spojení s § 2 písm. i) a k) a § 22a)] Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon [§ 4 odst. 1 písm. d) se spojení s § 2 písm. i), k), l) a m)], a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá [§ 3 a § 2 písm. b)]. Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Připomínkové místo s vypořádáním souhlasí.
400. Odbor (vláda)	kompatibility	D	K čl. 8 odst. 5 a čl. 9 odst. 3 a 4 směrnice:	Vysvětleno

		Není zřejmé, jak je zajištěna implementace článku 9 odst. 3 a 4 (povinnost určit dostatečné kapacity a přijmout národní plán reakce). A zda implementace čl. 8 odst. 5 počítá s propojením na služební zákon (obdobně čl. 9 odst. 1 druhá věta).	Co se týče implementace čl. 8 odst. 5 směrnice, bude tento požadavek zajištěn prostřednictvím alokace příslušné části státního rozpočtu na provoz Národního úřadu pro kybernetickou a informační bezpečnost. Co se týče čl. 9 odst. 3 a 4 směrnice, budou tyto požadavky zajištěny primárně nikoliv prostřednictvím nového zákona o kybernetické bezpečnosti, ale prostřednictvím připravované legislativy v oblasti krizového řízení státu, která primárně není v gesci NÚKIB; ve vztahu k působnosti NÚKIB budou tyto požadavky zajištěny dle § 44 odst. 4 písm. f) a g) návrhu zákona prostřednictvím NÚKIB. Připomínkové místo s vypořádáním souhlasí.
401. Odbor kompatibility (vláda)	D	K čl. 10 odst. 2 směrnice: Není zřejmé, jak je zajištěna implementace čl. 10 odst. 2 směrnice, podle kterého členské státy zajistí, aby měl každý tým CSIRT odpovídající zdroje pro účinné plnění svých úkolů podle čl. 11 odst. 3. Budou členové týmů pod služebním zákonem?	Vysvětleno Zajištění financí na výdaje na zabezpečení plnění úkolů Národního úřadu pro kybernetickou a informační bezpečnost, jehož součástí je vládní CERT, je zahrnuto v příslušné kapitole státního rozpočtu. V případě Národního CERT se jedná o činnost na základě smlouvy, kdy schopnost Národního CERT zajistit svou činnost je součástí schopnosti veřejnoprávní smlouvu uzavřít. V případě že by Národní CERT nebyl schopen vykonávat svou činnost, přebírá jeho činnost Vládní CERT. Tato informace byla doplněna do důvodové zprávy. V souladu s § 2 odst. 2 zákona č. 234/2014 Sb., o státní službě, se tento zákon nevztahuje na zaměstnance Národního úřadu pro kybernetickou bezpečnost. Připomínkové místo s vypořádáním souhlasí.
402. Odbor kompatibility (vláda)	D	K článku 14 směrnice: Podle odstavce 1 článku 14 směrnice s cílem podporovat a usnadňovat	Vysvětleno

		strategickou spolupráci a výměnu informací mezi členskými státy a posilovat důvěru se zřizuje skupina pro spolupráci. Podle odstavce 2 tohoto článku skupina pro spolupráci vykonává své úkoly na základě dvouletých pracovních programů. Odstavec 3 článku 14 směrnice stanovuje, že skupina pro spolupráci je tvořena zástupci členských států, Komise a agentury ENISA. Implementační zákon však tyto tři odstavce směrnice vykazuje jako nerelevantní z pohledu implementace. Není tedy jasné, kdo bude za Českou republiku jmenován do této skupiny pro spolupráci a kým bude jmenován. Má být snad relevantní § 41 odst. 4 písm. f) návrhu? Pak viz připomínka k tomuto ustanovení. Také jsme názoru, že by tento aspekt měl být podrobněji upraven buď zákonem anebo alespoň prováděcím právním předpisem. Podle čl. 14 odst. 5 směrnice totiž členské státy zajistí, aby jejich zástupci ve skupině pro spolupráci účinně, účelně a spolehlivě spolupracovali.	Ano, dotčenou část směrnice - čl. 14 odst. 1 až 5 - provádí navrhovaný § 44 odst. 4 písm. f) nového zákona o kybernetické bezpečnosti, přičemž navrhovaná úprava vychází ze stávající úpravy § 22 písm. s) současného zákona o kybernetické bezpečnosti, která se dlouhodobě osvědčila jako vhodná a funkční. Připomínkové místo s vypořádáním souhlasí.
403. Odbor kompatibility (vláda)	D	K článku 15 směrnice: Podle čl. 15 odst. 1 se zřizuje síť národních týmů CSIRT s cílem přispívat k budování důvěry mezi členskými státy a podporovat jejich rychlou a účinnou operativní spolupráci. Podle odstavce 2 síť CSIRT tvoří zástupci týmů CSIRT určených nebo zřízených podle článku 10 a zástupci týmu pro reakci na počítačové hrozby pro orgány, instituce a jiné subjekty Unie (CERT-EU). Bod je přitom vykázan jako neimplementační. Mělo by být stanoveno, kdo budou zástupci za Českou republiku v těchto týmech CSIRT. Opět se má uplatnit § 41 odst. 4 písm. f)? Viz připomínka k tomuto ustanovení.	Vysvětleno Zástupci v síti CSIRT podle návrhu zákona a požadavků směrnice NIS 2 mohou být Vládní a Národní CERT. Vládní CERT na základě ustanovení § 44 odst. 5 písm. j) a Národní CERT na základě (přečíslovaného) § 45 odst. 1 písm. h) podle požadavků ze směrnice NIS 2. Podle § 44 odst. 4 písm. f) povinnost vůči síti CSIRT plní i Úřad, neboť účast jeho zaměstnanců i mimo vládní CERT je v určitých situacích žádána a může přispívat k zajištění vyšší úrovně kybernetické bezpečnosti. Připomínkové místo s vypořádáním souhlasí.
404. Odbor kompatibility (vláda)	D	<u>K článku 16 směrnice:</u> Podle čl. 16 odst. 1 se zřizuje síť EU-CyCLONE, a to za účelem podpory koordinovaného řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operativní úrovni. Podle odstavce	Vysvětleno Ano, dotčenou část směrnice provádí navrhovaný § 44 odst. 4 písm. f) nového zákona o kybernetické bezpečnosti, přičemž navrhovaná úprava vychází ze

		2 je tato síť tvořena zástupci orgánů členských států pro řešení kybernetických krizí. Mělo by být stanoveno, kdo budou zástupci za Českou republiku, a na základě čeho budou určeni. Opět se má uplatnit § 41 odst. 4 písm. f)? Viz připomínka k tomuto ustanovení.	stávající úpravy § 22 písm. s) současného zákona o kybernetické bezpečnosti, která se dlouhodobě osvědčila jako vhodná a funkční. Připomínkové místo s vypořádáním souhlasí.
405. Odbor kompatibility (vláda)	D	K čl. 19 odst. 6 směrnice: Podle čl. 19 odst. 6 poslední věty odborníci na kybernetickou bezpečnost účastníci se vzájemného hodnocení nesmí sdělit žádné citlivé nebo důvěrné informace získané v průběhu tohoto vzájemného hodnocení žádným třetím stranám. Předkladatel celý bod označil za nerelevantní z pohledu implementace. Žádáme stav napravit a dosažení cíle stanoveného směrnicí zajistit, bude nutné zakotvit povinnost mlčenlivosti.	Vysvětleno Z informací získaných v průběhu přípravy směrnice NIS2 máme za to, že vzájemné hodnocení jako proces je prozatím těžko představitelný a ve směrnici nový. Máme za to, že veškeré náležitosti spojené se stanovením procesu výběru expertů, stejně jako praktické aspekty výkonu jejich funkce (zmiňovaná mlčenlivost), jsou ovládány metodikou podle čl. 19 odst. 1 směrnice NIS2, tj. že tento proces je vytvářen de facto na evropské úrovni. Členské státy se následně mohou do takto vytvořeného rámce už jen zapojit nebo nezapojit [„účast je dobrovolná, a srov. § 44 odst. 4 písm. h)“]. Z tohoto důvodu máme za to, že ustanovení není transpoziční. Připomínkové místo s vypořádáním souhlasí.
406. Odbor kompatibility (vláda)	D	K čl. 19 odst, 7 a 8 směrnice: Článek 19 v odstavcích 7 a 8 je označen jako neimplementační, nicméně podle našeho názoru by bylo vhodné zajistit řádný průběh vzájemných hodnocení ve smyslu tohoto článku právním předpisem. Podle odstavce 7 tytéž aspekty, které již byly v členském státě předmětem vzájemného hodnocení, nepodléhají v tomto členském státě v průběhu dvou let po ukončení vzájemného hodnocení dalšímu posuzování, pokud o to členský stát nepožádá nebo pokud to není výsledkem dohody na základě návrhu skupiny pro spolupráci. Dále mají v kontextu odstavců 8 a 9 členské státy povinnost zajistit proces vznášení námitek a připomínek ke zprávám o vzájemném hodnocení. Domníváme se, že v alespoň v hrubých rysech by bylo vhodné článek	Akceptováno S ohledem na vysvětlení uvedené výše a na současnou nejistotu s budoucím praktickým použitím nového institutu vzájemného hodnocení preferujeme vyřešit tuto připomínku způsobem rozepsání § 44 odst. 4 písm. h) např. takto: „ <i>v případě potřeby se podílí na procesu vzájemného hodnocení podle příslušného předpisu Evropské unie a metodiky a organizačních aspektů vzájemného hodnocení vypracovaných Skupinou pro spolupráci podle tohoto příslušného předpisu Evropské unie</i> “(+ odkaz na směrnici NIS2).

		implementovat, jelikož o přímo použitelný předpis se zde nejedná a fungování mechanismu podle článku 19 směrnice musí být státem zajištěno.	Připomínkové místo s vypořádáním souhlasí.
407. Odbor kompatibility (vláda)	D	K článku 26 směrnice: Není zřejmé, jak je tento důležitý článek týkající se pravomocí implementován.	Akceptováno Odst. 1: Dojde k doplnění explicitního vymezení osobní působnosti zákona a k doplnění speciálního ustanovení o povinnostech osob uvedených v čl. 21 odst. 1 písm. b) směrnice NIS2 (do § 1 návrhu zákona). Odst. 2: Provedeno v § 54 odst. 5 návrhu. Odst. 3: Provedeno v § 67 odst. 1 a 2 návrhu. Odst. 4: Provedeno v § 67 odst. 3 návrhu. Odst. 5: Provedeno v § 54 odst. 1 a 2 návrhu. Připomínkové místo s vypořádáním souhlasí.
408. Odbor kompatibility (vláda)	D	Mnohá další ustanovení, například <u>článek 32 směrnice</u> , nebyla plně provedena.	Vysvětleno Máme za to, že pokrýváme všechny požadavky NIS2 pro oblast dohledu a vymáhání týkající se poskytovatelů regulované služby v režimu vyšších povinností. Považujeme z naší strany budoucí dohledové kompetence za dostatečné a naplňující požadavky článku 32 směrnice NIS2, některé pravomoci jsou však upraveny jinými předpisy, nežli předloženým návrhem zákona, zejména zákonem č. 500/2004 Sb., správní řád a zákon č. 255/2012 Sb. o kontrole (kontrolní řád), ve znění pozdějších předpisů. Článek 32 odst. 1 provádí: § 58 až 63 návrhu zákona včetně kontrolního a správního řádu. Článek 32 odst. 2 provádí:

			Písm. a) provádí: § 58 návrhu zákona. Písm. b) : Máme požadavek na provádění pravidelných cílených auditů u povinných subjektů ve vyhlášce pro režim vyšších povinností, provádíme také samostatně cílené audity v případě potřeby (reakce na incident, spolupráce, nejedná se v tomto případě o kontrolu podle kontrolního řádu). Písm. c): Audit nebo kontrolu na základě incidentů lze provést také, buď na základě domluvy s regulovaným subjektem nebo na základě plánu kontrol, který je pravidelně aktualizován. Písm. d): Zde vycházíme primárně z anglického textu směrnice NIS2, jelikož nám překlad tohoto ustanovení přijde zavádějící a v našem právní řádu se používá v jiném kontextu, tím pádem toto ustanovení dopadá také na běžnou kontrolní činnost úřadu. Jedná se tedy o běžné security scany ve smyslu auditu nebo kontroly za účelem ověření plnění kybernetických bezpečnostních požadavků. Písmena e) a f) provádí: § 8 odst. 1, § 9 odst. 1, § 12 odst. 1, § 16 odst. 1 a 2, § 21 odst. 3, § 57, § 58, § 59 odst. 1 návrhu zákona, včetně kontrolního a správního řádu, který upravuje dohledovou činnost Úřadu (povinnost součinnosti). Písm. g) provádí: vyhláška pro režim vyšších povinností a kontrolní řád. Článek 32 odst. 3 provádí: § 56 návrhu zákona, kontrolní řád a správní řád.

		Článek 32 odst. 4: Písm. a) provádí: § 21 a § 22 návrhu zákona (výstraha). Písm. b) provádí: § 21 a § 24 reaktivní opatření, § 44 odst. 3 písm. v) a § 56 návrhu zákona. Písm. c) provádí: § 59 návrhu zákona nápravné opatření. Písm. d) provádí: nápravné opatření § 59 návrhu zákona. Písm. e) provádí: nápravná opatření § 59 návrhu zákona. Písm. f) provádí: nápravná opatření § 59 návrhu zákona. Písm. g) provádí: zaměstnanci Úřadu na základě pověření k výkonu kontroly v souladu s kontrolním řádem a § 59 návrhu zákona. Písm. h) provádí: § 22 návrhu zákona. Písm. i) provádí: § 21, § 59 prostřednictvím příkazního řízení podle správního řádu. Článek 32 odst. 5: provádí § 62 a § 63 návrhu zákona Článek 32 odst. 6: Pokud jde o oprávnění fyzické osoby jednat za základní subjekt, provedení tohoto ustanovení lze spatřovat v § 161 až 167 občanského zákoníku, které upravují jednání za právnickou osobou. Stanovení odpovědnosti pak lze nalézt v § 159 občanského zákoníku, který upravuje výkon funkce člena voleného orgánu. Článek 32 odst. 7: Nutnost nalezení řešení odpovídajícího okolnostem daného případu, je jednou

		z obecně platných zásad pro činnost veřejné správy a jako tzv. zásada přiměřenosti je zakotvena v § 2 odst. 4 správního řádu. V případě trestání se pak uplatňuje tzv. princip individualizace trestu, který zavazuje k tomu, aby všechny individuální okolnosti a specifika daného případu stejně jako osoba pachatele byly řádně zohledněny tak, aby trest odpovídal těmto specifickým. Pravidla pro ukládání správních trestů zohledňující požadavky daného ustanovení směrnice (určení druhu a výměry správního trestu, povaha a závažnost přestupku, polehčující okolnosti, přitěžující okolnosti, ukládání správních trestů za více přestupků) jsou obsaženy v § 36 až § 41 zákona o odpovědnosti za přestupky a řízení o nich. Článek 32 odst. 7: provádí § 44 odst. 4 písm. g) návrhu zákona a § 66 návrhu zákona. Článek 32 odst. 8 provádí správní řád: Odůvodnění je podle § 68 odst. 1 správního řádu zásadně součástí každého správního rozhodnutí. V odůvodnění se pak podle § 68 odst. 3 správního řádu uvedou důvody výroku nebo výroků rozhodnutí, podklady pro jeho vydání, úvahy, kterými se správní orgán řídil při jejich hodnocení a při výkladu právních předpisů, a informace o tom, jak se správní orgán vypořádal s návrhy a námitkami účastníků a s jejich vyjádřením k podkladům rozhodnutí. V návaznosti na kontrolu může kontrolovaná osoba podle § 13 odst. 1 kontrolního řádu podat námitky proti kontrolnímu zjištění uvedenému v protokolu o kontrole, a to ve lhůtě 15 dnů ode dne doručení protokolu o kontrole. Článek 32 odst. 9 provádí: § 57 návrhu zákona. Článek 32 odst. 10 provádí: § 65 a § 66 návrhu zákona.

			Připomínkové místo s vypořádáním souhlasí.	
409. Nejvyšší úřad	kontrolní	D	K § 28, odst. 2 Z tohoto ustanovení není zřejmé, na základě jakých konkrétních dostupných kapacit bude Úřad prioritizovat činnosti uvedené v odstavci 1. Zda se bude jednat např. o dostupné personální, technické, výpočetní či jiné kapacity Úřadu. Toto ustanovení doporučujeme blíže konkretizovat.	Akceptováno - nyní § 29 V zákoně bylo upřesněno, že se jedná o personální a technické kapacity tak, jak je uvedeno v důvodové zprávě. Připomínkové místo s vypořádáním souhlasí.
410. Nejvyšší úřad	kontrolní	D	K § 36 Podle navrhovaného znění tohoto ustanovení se domníváme, že upravuje povinnosti pouze pro subjekty spravující a provozující registr internetových domén první a druhé úrovně a nevztahuje se na existující správce domén na úrovni třetího řádu. Doporučujeme toto ustanovení doplnit o správce domén na úrovni třetího řádu.	Neakceptováno - nyní § 37 Povinnost uvedená v daném ustanovení vychází ze směrnice NIS2. Úřad ji v tomto znění považuje za dostatečnou, vztahovat ji i na správce domén třetího řádu bylo vyhodnoceno jako neproporční a zbytečně zatěžující pro tyto subjekty. Připomínkové místo s vypořádáním souhlasí.
411. Nejvyšší úřad	kontrolní	D	K § 40 odst. 1 písm. b) až h) Domníváme se, že charakter a rozsah opatření, která v případě stavu kybernetického nebezpečí bude moci nařídít ředitel NÚKIB, a informací, které bude moci požadovat po dalších orgánech a osobách, je natolik obecný a široký, že souvislost s řešením kybernetického nebezpečí může být velmi okrajová. Navíc se v některých případech jedná o poskytnutí citlivých až důvěrných dat, například uložením povinnosti zpřístupnění neveřejných komunikačních sítí. Doporučujeme oprávnění ředitele NÚKIB blíže specifikovat a upravit tak, aby byla stanovena ve vazbě na konkrétní případy kybernetického ohrožení.	Akceptováno - nyní § 41 Na vhodném znění celé soustavy ustanovení o stavu kybernetického nebezpečí spolupracujeme s Ministerstvem vnitra – Generálním ředitelstvím Hasičského záchranného sboru a návrh bude upraven na základě těchto jednání. Navrhovaná právní úprava nemá za cíl zasahovat do práv způsobem, který by odpovídal nouzovému stavu, tj. zásah v intenzitě nouzového stavu je ponechán vládě a není svěřen do rukou ředitele Úřadu. V případě zmíněných ustanovení došlo s ohledem na výše uvedené na vhodných místech k úpravám. Připomínkové místo s vypořádáním souhlasí.

412. Nejvyšší úřad	kontrolní	D	K bodu 16.1. Přílohy k vyhlášce o regulovaných službách - Poskytování veřejně dostupné služby elektronických komunikací Tato část přílohy vyhlášky opomíjí provozovatele IoT sítí (LoRa, NB-IOT, Sigfox, ...), které jsou využívány zejména pro sběr dat z elektroměrů, vodoměrů, přičemž kompromitace sběrných bran nebo vyřazení provozovatele by způsobily dalekosáhlé následky. Z uvedeného důvodu doporučujeme v této části přílohy doplnit následující bod do režimu vyšších povinností: "e) je poskytovatelem veřejně dostupné služby elektronických komunikací pro nejméně 300 000 aktivních zařízení".	Vysvětleno Vámi jmenovaný okruh subjektů je zařazen mezi poskytovatele regulované služby již na základě velikosti, nad to co se týká těch služeb, které podporují právě elektroměry a vodoměry, tedy služeb navázaných na používání těchto IoT sítí, ty jsou v rozsahu samotných regulovaných služeb, například zde distribuce elektřiny a vody. Proto je dále bezpečné zajištění sítí, na kterých závisí chytré elektroměry a vodoměry zajišťováno smluvními závazky ze strany provozovatelů těchto distribučních soustav. Není proto dle našeho názoru nutné další kritérium v rámci vyššího režimu. Připomínkové místo s vypořádáním souhlasí.
413. Nejvyšší úřad	kontrolní	D	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností K §20, Správa a ověřování identit, odst. 5 V kontextu znění odst. 4 není text odstavce 5 srozumitelný. Doporučujeme text odstavce 5 upravit tak, že do doby splnění požadavku podle odstavce 3 je povinnost využít kryptografický klíč nebo certifikát pro jednofaktorové přihlašování.	Vysvětleno Dle našeho názoru textace odstavce 5 dostatečně srozumitelně a přímo uvádí návaznost na odstavec 3 (při nemožnosti jeho plnění) a uvádí požadavky na technická bezpečnostní opatření, které jsou požadovány v případě nemožnosti plnění požadavku dle odstavce 3. Připomínkové místo s vypořádáním souhlasí.
414. Nejvyšší úřad	kontrolní	D	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností §20, Správa a ověřování identit, odst. 6 Při využití jednofaktorového přihlášení pomocí certifikátu/klíče nelze aplikovat hesla. Z tohoto důvodu doporučujeme odstavec 6 přeformulovat	Neakceptováno Dle našeho názoru textace odstavce 6 dostatečně srozumitelně a přímo uvádí návaznost na odstavec 5 (při nemožnosti jeho plnění) a uvádí požadavky na technická bezpečnostní opatření, které jsou požadovány v případě nemožnosti plnění požadavku dle odstavce 5.

		následovně: "... technických aktiv nevyužívající autentizační mechanismus založený na autentizaci pomocí kryptografických klíčů nebo certifikátů podle odstavce 5, ..."	Připomínkové místo s vypořádáním souhlasí.
415. Nejvyšší úřad	kontrolní	D Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností §20, Správa a ověřování identit, odst. 6, bod e) e) povinné změny hesla v intervalu maximálně po 18 měsících, Tento požadavek je u servisních účtů velmi obtížné realizovat. Většina systémů nepočítá s možností automatické změny hesla a s její propagací v rámci velkých systémů. Zejména SCADA infrastruktura je v tomto případě velmi neflexibilní. Požadavek na pravidelnou změnu hesla v rámci běžné praxe již není vyžadován, důraz se klade spíše na dostatečnou délku hesla. Jako vhodnější řešení doporučujeme stanovit požadavek na pravidelné vyhodnocování rizika zneužití hesla pro jednotlivá aktiva. V rámci IT praxe na NKÚ se u servisních účtů explicitně nastavují hesla v maximální možné délce pro jednotlivá aktiva, a po nastavení systému jsou použitá hesla z evidence smazána, takže případný útočník nemůže toto heslo daného systému získat.	Vysvětleno Souhlasíme s Vašimi poznatky ohledně doporučení v oblasti změny potenciálně kompromitovaných hesel, které odráží i navrhované ustanovení. Pokud v praxi zavádění bezpečnostního opatření (např. konkrétně řešené povinné změny hesla v intervalu maximálně po 18 měsících) v určitých situacích nebo prostředích (např. OT/SCADA) není možné nebo by bylo kontraproduktivní ve zvyšování úrovně kybernetické bezpečnosti, je na místě toto bezpečnostní opatření nezavádět (neaplikovat) a tuto skutečnost zohlednit v prohlášení o aplikovatelnosti, včetně odůvodnění a uvedení náhradních přijatých bezpečnostních opatření. V takové situaci se např. při neaplikování tohoto bezpečnostního opatření v prostředí OT/SCADA systémů nejedná o nesoulad s požadavky zákona a jeho prováděcích předpisů, pokud je tato skutečnost náležitě zohledněna v systému řízení bezpečnosti informací, řízení rizik a konkrétně v prohlášení o aplikovatelnosti. Připomínkové místo s vypořádáním souhlasí.
416. Nejvyšší úřad	kontrolní	D Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností §20, Správa a ověřování identit, odst. 7, bod d) Splnění tohoto požadavku zvyšuje riziko kompromitace hesla, neboť nezapamatovatelné heslo bude nezbytné zajistit na bezpečném	Vysvětleno Jelikož se jedná o hesla technických aktiv, kterých bývá zpravidla v organizacích vyšší počet (desítky, stovky, někdy tisíce), který se odvíjí od počtu technických aktiv a jejich účtů, není žádoucí ani lidsky možné, aby tato hesla byla zároveň unikátní,

		úložišti. Připomínáme, že v nedávné době se vyskytlo několik incidentů s kompromitacemi manažerů hesel.	zapamatovatelná a neodvoditelná. Rizik spojených s kompromitací manažerů hesel jsme si vědomi a děkujeme za Vaše podněty, nicméně se jedná o rizika spojená s technickými aktivy, které musí brát organizace v úvahu a předcházet vzniku kybernetických bezpečnostních incidentů (např. zabezpečení offline manažera hesel řízením přístupů k němu), stejně jako u kterýchkoliv jiných technických aktiv. V praxi jsou manažeři hesel (hovorově klíčenky) pro správu autentizačních údajů k technickým aktivům velice hojně využívány. Naopak lze manažery hesel na rozdíl od jiných často zneužívaných technických aktiv (jako např. firewallu a zero-day zranitelností) dostatečně chránit např. na základě zmíněného řízení přístupů. Připomínkové místo s vypořádáním souhlasí.
417. Česká asociace elektronických komunikací	Z	K § 31 – Transparentnost výjimek Původní text § Výjimky z omezení rizik spojených s dodavatelem (1) Úřad může, pokud to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku připouští, povolit výjimku z podmínek či zákazu stanovených opatření obecné povahy podle § 30, jestliže by plnění opatření obecné povahy poskytovatelem strategicky významné služby mohlo podstatným způsobem ohrozit poskytování strategicky významné služby. (2) Řízení o povolení výjimky podle odstavce 1 lze zahájit na žádost poskytovatele strategicky významné služby nebo z moci úřední. Žadatel je povinen v rámci žádosti připojit důkazy prokazující skutečnosti, kterých se dovolává.	Neakceptováno - nyní § 32 Požadavek na doplnění předmětného ustanovení nemůže být akceptován. Problematika utajení informací je již řešena v § 67 nZKB - informace o výjimkách se uchovávají jako neveřejné mimo spis. Pokud by výjimka obsahovala informace klasifikované jako utajované, pak bude takto nakládáno i s celým rozhodnutím. Připomínkové místo s vypořádáním souhlasí.

		(3) Úřad v rozhodnutí o povolení výjimky stanoví podmínky jejího uplatnění. V případě závažného porušení podmínek pro uplatnění výjimky nebo v případě pominutí důvodu, pro který byla povolena, Úřad výjimku rozhodnutím zruší. (4) Úřad výjimku nepovolí, pokud by to zcela zmařilo účel opatření obecné povahy podle § 30. CELEX 32022L2555 Návrh změny Navrhujeme přidat odst. (5) ve znění: (5) <i>Informace týkající se výjimky je v souladu s právními předpisy¹ označována jako utajovaná informace.</i> a poznámku/odkaz na zákon o ochraně utajovaných informací. Odůvodnění Informace o udělených výjimkách obsahuje informace, které mohou mít povahu obchodního tajemství či obsahovat informace, jejichž zveřejnění by mohlo ohrozit bezpečnost poskytování strategicky významné služby. Proto považujeme za vhodné, aby s informacemi týkajícími se výjimky byly zpracovávány v režimu zákona o ochraně utajovaných informací. To umožní řízený a kontrolovaný přístup k těmto informacím a současně zajistí jejich ochranu. Nový text s vyznačením změn § 31 Výjimky z omezení rizik spojených s dodavatelem (1) Úřad může, pokud to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku připouští, povolit výjimku z podmínek či zákazu stanovených opatření obecné povahy podle § 30, jestliže by plnění opatření obecné povahy poskytovatelem strategicky významné služby mohlo podstatným způsobem ohrozit poskytování strategicky významné služby.	

		(2) Řízení o povolení výjimky podle odstavce 1 lze zahájit na žádost poskytovatele strategicky významné služby nebo z moci úřední. Žadatel je povinen v rámci žádosti připojit důkazy prokazující skutečnosti, kterých se dovolává. (3) Úřad v rozhodnutí o povolení výjimky stanoví podmínky jejího uplatnění. V případě závažného porušení podmínek pro uplatnění výjimky nebo v případě pominutí důvodu, pro který byla povolena, Úřad výjimku rozhodnutím zruší. (4) Úřad výjimku nepovolí, pokud by to zcela zmařilo účel opatření obecné povahy podle § 30. (5) <u>Informace týkající se výjimky je v souladu s právními předpisy¹ označována jako utajovaná informace.</u> *1) zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. CELEX 32022L2555	
418. Česká asociace elektronických komunikací	Z	K § 34 - Lokalizace Původní text § 34 (6) Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky. (7) Poskytovatel strategicky významné služby je povinen testovat schopnost zajištění poskytování strategicky významné služby v rozsahu kritické části stanoveného rozsahu z území České republiky nejméně jednou za dva roky. (8) Poskytovatel strategicky významné služby začne plnit povinnosti uvedené v odst. 1 a 2 pro každou strategicky významnou službu nejpozději do jednoho roku ode dne doručení vyrozumění o zápisu strategicky významné	Akceptováno jinak - nyní § 35 Připomínkované ustanovení § 35 bylo v odst. 1 upraveno tak, že "Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v nezbytném rozsahu, ~~v rozsahu kritické části stanoveného rozsahu~~ ve stanoveném čase a kvalitě z území České republiky." Tento nezbytný rozsah pak bude stanoven vyhláškou Úřadu. V této vyhlášce bude specifičtěji rozvedeno, co se v telekomunikačním sektoru rozumí nezbytným rozsahem při zajištění dostupnosti těchto služeb z území ČR. Připomínkové místo s vypořádáním souhlasí.

		služby do evidence poskytovatelů regulovaných služeb nebo od doručení rozhodnutí o určení strategicky významné služby podle § 27 odst. 2. (9) Stanovený čas a kvalitu služby stanoví poskytovatel regulované služby v závislosti na cílech řízení kontinuity činností podle prováděcího právní předpisu. (10) Pro potřeby tohoto ustanovení je kritická část stanoveného rozsahu vymezena v § 28 odst. 3 písm. a). CELEX 32022L2555 Návrh změny Navrhujeme vložit za odstavec (1) nový odstavec (2) a současné odstavce (2), (3), (4) a (5) přechíslovat: <i>(2) Poskytovatel strategicky významné služby v odvětví 16.1 Poskytování veřejně dostupní služby elektronických komunikací a 16.2. Zajišťování veřejně dostupné komunikační sítě elektronických komunikací podle přílohy k vyhlášce o regulovaných službách je povinen v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky zajistit dostupnost jím poskytované strategicky významné služby spočívající v</i> <i>a) poskytování veřejně dostupné mobilní služby elektronických komunikací, nebo</i> <i>b) zajišťování veřejné mobilní komunikační sítě elektronických komunikací, nebo</i> <i>c) poskytování veřejně dostupné služby elektronických komunikací v pevném místě.</i> Odůvodnění Sektor elektronických komunikací je specifickým sektorem s vlastní zákonnou regulací (zákon č. 127/2005 Sb.), regulačním a dozorovým orgánem a se specifickým vztahem k oblasti kybernetické bezpečnosti a zajištění dostupnosti strategicky významných služeb.	

		Protože již během veřejných konzultací a diskusí sektoru s Národním úřadem pro kybernetickou a informační bezpečnost docházelo k různým výkladovým nejasnostem a závěrům i v kontextu další legislativy a představných tezí a návrhů prováděcích právních předpisů, navrhujeme odstranit tyto nejasnosti a možný různý výklad či dezinterpretace upřesněním v podobě speciální úpravy s odkazem na odvětví 16.1 a 16.2 současného návrhu vyhlášky o regulovaných službách. Nový text s vyznačením změn § 34 (1) Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky. (2) <u>Poskytovatel strategicky významné služby v odvětví 16.1 Poskytování veřejně dostupní služby elektronických komunikací a 16.2. Zajišťování veřejně dostupné komunikační sítě elektronických komunikací podle přílohy k vyhlášce o regulovaných službách je povinen v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky zajistit dostupnost strategicky významné služby spočívající v</u> a) <u>poskytování veřejně dostupné mobilní služby elektronických komunikací,</u> b) <u>zajišťování veřejné mobilní komunikační sítě elektronických komunikací,</u> c) <u>poskytování veřejně dostupné služby elektronických komunikací v pevném místě.</u> (3) Poskytovatel strategicky významné služby je povinen testovat schopnost zajištění poskytování strategicky významné služby v rozsahu kritické části stanoveného	

		rozsahu z území České republiky nejméně jednou za dva roky. (4) Poskytovatel strategicky významné služby začne plnit povinnosti uvedené v odst. 1 a 2 pro každou strategicky významnou službu nejpozději do jednoho roku ode dne doručení vyrozumění o zápisu strategicky významné služby do evidence poskytovatelů regulovaných služeb nebo od doručení rozhodnutí o určení strategicky významné služby podle § 27 odst. 2. (5) Stanovený čas a kvalitu služby stanoví poskytovatel regulované služby v závislosti na cílech řízení kontinuity činností podle prováděcího právní předpisu. (6) Pro potřeby tohoto ustanovení je kritická část stanoveného rozsahu vymezena v § 28 odst. 3 písm. a). CELEX 32022L2555	
419. Česká asociace elektronických komunikací	Z	K § 44 odst. (1) návrhu zákona o kyb. bezpečnosti – sdílení informací Původní text § 44 Portál NÚKIB (1) Úřad je správcem a provozovatelem Portálu NÚKIB, který slouží k výkonu pravomocí Úřadu, sdílení informací, provádění digitálních úkonů a poskytování digitálních služeb podle tohoto zákona. Návrh změny Navrhujeme upravit odst. (1) takto:	Vysvětleno - nyní § 47 Portál NÚKIB má sloužit pouze pro poskytovatele regulovaných služeb dle řešeného návrhu zákona a spolupracující organizace, nepůjde o univerzálně přístupnou platformu pro subjekty, které by například spadaly pouze do působnosti ZEK a nikoliv nového ZKB. NÚKIB nadále počítá se vznikem jednotné platformy, která bude umožňovat agregované hlášení dle více předpisů, nicméně tato by měla být spíše komplementárním řešením, které bude "přerozdělovat" příslušné hlášení relevantním subjektům, které je budou zpracovávat ve svých systémech s ohledem na jejich interní procesy. Připomínkové místo s vypořádáním souhlasí.

		<i>(1) Úřad je správcem a provozovatelem Portálu NÚKIB, který slouží k výkonu pravomocí Úřadu, sdílení informací, provádění digitálních úkonů a poskytování digitálních služeb podle tohoto zákona <u>a pro plnění informační povinnosti, pokud tak stanoví jiný zákon.</u></i> a poznámku/odkaz na zákon o ochraně utajovaných informací. Odůvodnění Navrhujeme doplnit funkce Portálu NÚKIB tak, aby jeho prostřednictvím mohly být do budoucna hlášeny bezpečnostní incidenty podle jiných právních předpisů, například podle § 98 odst. 4 zákona o elektronických komunikacích a dalších zákonů upravujících problematiku hlášení bezpečnostních incidentů a byla tak vytvořena jednotná platforma pro hlášení bezpečnostních incidentů již dříve ze strany NÚKIB uvažovaná, která by měla být gestorována NÚKIB a měla sloužit k jednotnému hlášení těchto incidentů. Navrhujeme tak upravit předmětné ustanovení ve smyslu této připomínky. Nový text s vyznačením změn § 44 Portál NÚKIB <i>(1) Úřad je správcem a provozovatelem Portálu NÚKIB, který slouží k výkonu pravomocí Úřadu, sdílení informací, provádění digitálních úkonů a poskytování digitálních služeb podle tohoto zákona <u>a pro plnění informační povinnosti, pokud tak stanoví jiný zákon.</u></i>	

420. Česká asociace elektronických komunikací	Z	K § 40 odst. (1) – Penetrační testy Původní text § 40 Opatření k řešení stavu kybernetického nebezpečí (1) Ředitel Úřadu je v době stavu kybernetického nebezpečí za účelem jeho řešení oprávněn a) poskytnout věcné prostředky v majetku České republiky, které má v užívání Úřad, a které jsou nezbytné k řešení kybernetického bezpečnostního incidentu, nebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem, b) vyžádat si od orgánů a osob informace o věcných prostředcích, o výrobních, provozních a personálních kapacitách a o objemu zásob ve stanovených druzích materiálu, přičemž tyto orgány a osoby mají povinnost poskytnout Úřadu vyžadované informace úplně a pravdivě v Úřadem stanovené lhůtě, c) vyžádat si na základě smlouvy nebo zápisu o sdílení personálních kapacit a věcných prostředků přednostní poskytnutí personálních kapacit nebo věcných prostředků a tyto personální zdroje a věcné prostředky využít, přičemž dožádané orgány a osoby mají povinnost žádosti Úřadu vyhovět, d) nařídit práci v pohotovostním režimu, e) zakázat orgánům a osobám, které k tomu byly Úřadem vyzvány, používání technických aktiv v případě, že jsou taková aktiva bezprostředně ohrožena kybernetickým bezpečnostním incidentem, který je může významně poškodit nebo zničit, nebo jsou takovým incidentem již postižena,	Neakceptováno - nyní § 41 Na tuto povinnost je také navázána povinnost součinnosti vyzvaných orgánů a osob právě za tím účelem toho, aby nebylo zasazeno do funkčnosti technických aktiv, a to provedením zpravidla méně invazivního skenu zranitelností nebo penetračním testováním. Ohledně rozsahu a metodiky je proto nezbytné konzultovat s příslušnými odpovědnými pracovníky orgánů a osob, u nichž se znalost informačního systému předpokládá a skrze jejichž součinnost by tak mělo být zamezeno narušení funkčnosti technických aktiv. Primárně není v zájmu řešení dané situace, aby došlo k narušení fungování dalších organizací a je tak v zájmu Úřadu, aby tyto testy proběhly pokud možno bez dalšího narušení kybernetické bezpečnosti. Připomínkové místo s vypořádáním souhlasí.

		f) uložit orgánům či osobám povinnost provést opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před kybernetickým bezpečnostním incidentem a oznámit provedení opatření a jeho výsledek Úřadu, g) nařídit orgánům a osobám provedení skenu zranitelností nebo penetračního testu, nebo h) nařídit orgánům a osobám zpřístupnění neveřejných komunikačních sítí v jejich správě pro potřeby Úřadu. Návrh změny Navrhujeme doplnit do písmene g) odst. (1) za mezi slova „testu“ a „nebo“ text: <i>„prostředky orgánu a osoby nebo prostředky dodavatele orgánu a osoby“</i> Odůvodnění Toto doplnění upřesňuje povahu provedení penetračních testů povinného orgánu či osoby v součinnosti s Národním úřadem pro kybernetickou a informační bezpečnost, kdy penetrační testy jsou nařízeny provést povinnému orgánu a osobě (vlastními prostředky či prostředky dodavatele), tedy podle stanovené metodiky a dojde i k jejich řádnému vyhodnocení a zohlednění výsledků. Penetrační test provedený NÚKIB bez vědomí povinného orgánu či osoby by byl vždy vyhodnocený jako kybernetický útok a bylo by proti němu podniknuty adekvátní opatření, včetně možného upozornění bezpečnostních orgánů a NÚKIB. Bez potřebné součinnosti a koordinace by tak mohlo docházet k situacím, které by bylo v rozporu se zájmy bezpečnosti ČR a kybernetické bezpečnosti povinných orgánů a osob.	

		Nový text s vyznačením změn § 40 Opatření k řešení stavu kybernetického nebezpečí (1) Ředitel Úřadu je v době stavu kybernetického nebezpečí za účelem jeho řešení oprávněn a) poskytnout věcné prostředky v majetku České republiky, které má v užívání Úřad, a které jsou nezbytné k řešení kybernetického bezpečnostního incidentu, nebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem, b) vyžádat si od orgánů a osob informace o věcných prostředcích, o výrobních, provozních a personálních kapacitách a o objemu zásob ve stanovených druzích materiálu, přičemž tyto orgány a osoby mají povinnost poskytnout Úřadu vyžadované informace úplně a pravdivě v Úřadem stanovené lhůtě, c) vyžádat si na základě smlouvy nebo zápisu o sdílení personálních kapacit a věcných prostředků přednostní poskytnutí personálních kapacit nebo věcných prostředků a tyto personální zdroje a věcné prostředky využít, přičemž dožádané orgány a osoby mají povinnost žádosti Úřadu vyhovět, d) nařídit práci v pohotovostním režimu, e) zakázat orgánům a osobám, které k tomu byly Úřadem vyzvány, používání technických aktiv v případě, že jsou taková aktiva bezprostředně ohrožena kybernetickým bezpečnostním incidentem, který je může významně poškodit nebo zničit, nebo jsou takovým incidentem již postižena, f) uložit orgánům či osobám povinnost provést opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před kybernetickým	

		bezpečnostním incidentem a oznámit provedení opatření a jeho výsledek Úřadu, g) nařídit orgánům a osobám provedení skenu zranitelností nebo penetračního testu <u>prostředky orgánu a osoby nebo prostředky dodavatelů orgánu a osoby</u>, nebo h) nařídit orgánům a osobám zpřístupnění neveřejných komunikačních sítí v jejich správě pro potřeby Úřadu.	
421. Český telekomunikační klastr	D	Český telekomunikační klastr z.s. jako asociace sdružující subjekty především z řad poskytovatelů služeb přístupu k internetu tímto Národnímu úřadu pro kybernetickou bezpečnost předkládá své připomínky k Návrhu zákona o kybernetické bezpečnosti. Předkládané materiály jsou koncipovány pro jejich adresáty nepřehledným a obtížně uchopitelným způsobem, kdy i pro základní orientaci v zákoně a posouzení fundamentálních otázek je třeba pracovat s mnoha dalšími právními předpisy, zejména vyhláškami, které zákon provádějí. Definice základních pojmů jsou často duplicitní či rekurzivní bez vymezení jasného vztahu mezi nimi a základní pojmy zákona jsou popsány přehnaně technickým jazykem. Jak je uvedeno i níže v tomto podání, považujeme širší zmocnění Úřadu v předkládaném návrhu zákona k vydávání podzákonných předpisů za excesivní a problematickou s ohledem na ústavní principy dělby moci. Možnost změn základních kategorií právní úpravy (jako jsou například adresáti jejich jednotlivých povinností) formou pouhých vyhlášek Úřadu pak omezuje dotčené soukromé subjekty v oblastech právní jistoty, legitimního očekávání a stability regulace, což jsou kategorie pro dlouhodobý rozvoj podnikatelského prostředí významné. Máme konečně za to, že předkladatel při zpracování hodnocení dopadů regulace nedostatečně zohlednil enormní počet regulovaných subjektů zejména z řad menších regionálních poskytovatelů přístupu	Vysvětleno K úpravám jednotlivých otázek, jako jsou kritéria rizikovosti dodavatele či nepominutelné funkce na úrovni vyhlášek, je potřeba říct, že tato úprava představuje proporcionální řešení konfliktu mezi širokým správním uvážením NÚKIB, obdobně jako v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, či zákona č. 34/2021 Sb., o prověřování zahraničních investic, a vymezením nepominutelných funkcí či kritérií pro vyhodnocení bezpečnostních hrozeb na úrovni zákona. Obdobný postup navíc již funguje v případě tzv. cloudové vyhlášky NÚKIB (vyhláška č. 316/2021 Sb.). K tomuto je nutno dodat, že vyhláška o kritériích rizikovosti dodavatele se ruší. Nutno poukázat na to, co zaznělo již v průběhu veřejných konzultací, tedy že úprava těchto otázek (kritéria, nepominutelné funkce) formou podzákonného právního předpisu je běžnou legislativní praxí, tak jak tomu bylo mimo jiné například v případě zmíněné vyhlášky o zápisu do katalogu cloudových služeb. V případě, že by mělo dojít ke změně této vyhlášky, tak tato změna bude navíc procházet řádným legislativním procesem, v rámci kterého k ní může kdokoli uplatnit své

		k internetu, kterých v České republice působí přes 1500, a dopady přijímané úpravy na jejich podnikání a účast v hospodářské soutěži. Rozsah regulovaných subjektů – zejména pak subjektů spadajících do působnosti mechanismu prověřování dodavatelského řetězce považujeme za zjevně excesivní a neodůvodněny.	připomínky, které je předkladatel povinen řádně vypořádat. Případné nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu. Co se týče složitosti textu a dopadů na jednotlivé subjekty je nutno dodat, že NÚKIB si kladl, a stále klade za cíl jednotlivé otázky popsat co nejsrozumitelnějším způsobem. Vzhledem k značné komplexitě posuzovaných otázek a připomínek, které bylo a nadále je nutno reflektovat v rámci textu zákona, však mohou některá ustanovení odkazovat na jinou zákonnou či podzákonnou úpravu. K odůvodněnosti postupu popsaného v připomínce je potřeba dodat, že na základě zkušeností z činnosti NÚKIB se jedná o efektivní, avšak proporcionální, prostředek ochrany strategicky významných služeb. V otázkách samotné šíře regulovaných subjektů pak platí, že dané okruhy vychází přímo ze zákona, který stanovuje podmínky pro to, jak se může subjekt stát povinnou osobou. Reakce připomínkového místa S vypořádáním této připomínky nesouhlasíme. Co se týče zahrnutí klíčových definic a kritérií do prováděcích předpisů, na obsahu původně uplatněné připomínky trváme. Vymezení kategorií, jako je zejména okruh adresátů hlavních okruhů povinností dle předkládaného návrhu zákona je zásadním aspektem, bez jehož posouzení v rámci legislativního procesu nelze předložený návrh zákona reálně zhodnotit. Je tomu tak tím spíše, že sám Úřad níže v tomto vypořádání zdůraznil, že samotné vyhlášky nejsou předmětem připomínkového řízení a budou dále přepracovávány. Právní jistota o stabilitě regulatorního prostředí v těchto klíčových aspektech

			musí být dána od počátku a musí trvat i později za účinnosti zákona. Závěr Připomínka vypořádána.
422. Český telekomunikační klastr	Z	K § 2, odst. 1, písm. e) zákona Návrh textových změn: „Pro účely tohoto zákona se rozumí ... regulovanou službou služba, splňující kritéria pro identifikaci regulované služby, a to od okamžiku jejich splnění, nebo služba stanovená jako regulovaná služba u orgánu nebo osoby pravomocným rozhodnutím Úřadu, a to od okamžiku právní moci takového rozhodnutí jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností a k jejímuž poskytování jsou používána aktiva,“ Odůvodnění: Uvedená definice pojmu regulovaná služba je duplicitní k úpravě § 3 až § 5 návrhu zákona a není jasné v jakém vztahu tyto úpravy stojí. Předložená definice pojmu navíc vyvolává otázky ohledně časových aspektů, tj. od kdy se na každou posuzovanou službu mají vztahovat ustanovení zákona vztahující se k regulovaným službám. Navrhujeme proto definici změnit popsáním způsobem a obecnou klauzuli, která regulovanou službu popisovala včlenit do definičních kritérií v § 3 a násl. návrhu zákona.	Akceptováno Dojde k úpravě textu v duchu připomínky. Došlo k doplnění dalších ustanovení v zákoně tak, aby odpovídala požadavku připomínky. Reakce připomínkového místa S vypořádáním této připomínky souhlasíme s dodatečným doporučením. Souhlasíme se změnou definice regulované služby, naše připomínka nicméně nebyla do nového textu zákona přenesena ve všech podstatných ohledech. V novém textu chybí prvek časového určení, od kdy se služba považuje za regulovanou službu. To má význam zejména ve vztahu k určení regulované služby dle § 5 odst. 1 návrhu zákona, kdy z textu není jasné, zda rozhodnutí Úřadu je deklaratorní či konstitutivní – jinak řečeno, zda se daná služba považuje za regulovanou službu až od právní moci příslušného rozhodnutí nebo zda rozhodnutí pouze nalézá, že služba byla regulovanou službou již dříve. Pro právní jistotu navrhujeme plně reflektovat text připomínky v § odst. 1 návrhu zákona, nebo doplnit do § 5 návrhu zákona větu o tom, že služba se za regulovanou službu považuje od právní moci příslušného rozhodnutí. Závěr Připomínka vypořádána.

423. Český telekomunikační klastr	Z	K § 2, odst. 2, písm. d) zákona Návrh textových změn: „Pro účely tohoto zákona se rozumí ... významnou kybernetickou hrozbou kybernetická hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál závažně ovlivnit aktiva poskytovatele regulované služby nebo uživatelů regulovaných služeb natolik, že způsobí značnou majetkovou ~~nebo nemajetkovou~~ újmu,“ Odůvodnění: Pojem značné nemajetkové újmy je natolik otevřený a nejistý (zahrnuje například i zásah do dobré pověsti), co do časových, typových i územních aspektů natolik otevřený, že s dostatečně dlouhým výhledem do budoucna může být za takovou hrozbu označen prakticky jakýkoliv incident ovlivňující aktiva poskytovatele regulované služby. Máme za to, že takto mlhavě vymezený pojem není souladný se záměrem zákonodárce vážícím se k významné kybernetické hrozbě ani s požadavky na právní jistotu a předvídatelnost regulace. Navrhujeme proto vypuštění pojmu nemajetkové újmy z dotčené definice.	Neakceptováno Formulace vychází z čl. 6 bodu 11 směrnice NIS2, podle které se významnou kybernetickou hrozbou rozumí kybernetická hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál vážně ovlivnit síť a informační systémy určitého subjektu nebo uživatelů služeb takového subjektu tím, že způsobí značnou hmotnou nebo nehmotnou újmu. Při posuzování závažnosti újmy budou muset být zohledňovány všechny relevantní skutečnosti, neznamená to však, že by měla povinná osoba předvídat i velmi vzdálené důsledky. Primárně budou posuzovány přímé důsledky (tj. přímá škoda, resp. nemajetková újma) a z nepřímých ty, které jsou v danou chvíli alespoň odhadem ohodnotitelné. Např. citovaný zásah do dobré pověsti může být pro některá odvětví velmi relevantním kritériem, typicky v sektoru bankovníctví nebo poskytování řízených bezpečnostních služeb, nelze jej proto tam, kde je to relevantní, opomíjet. Reakce připomínkového místa S vypořádáním této připomínky nesouhlasíme. Text článku 6, bodu 11 směrnice NIS2 jasně hovoří o způsobení značné hmotné či nehmotné újmy. Pojmy majetková a nemajetková újma obsažené v předloženém návrhu zákona neužívá. Pojmy hmotná/nehmotná újma přitom nelze zaměňovat s pojmy majetková/nemajetková újma. Český právní řád zná kategorie majetku, které jsou z podstaty věci nehmotné (například obchodní podíl). Odchýlení se od textu směrnice a vztahení definice i na újmu

			nemajetkovou je extenzí, která nemá v kontextu návrhu opodstatnění. Závěr Připomínka je vypořádána.
424. Český telekomunikační klastr	Z	K § 2, odst. 2, písm. h) zákona Návrh textových změn: „Pro účely tohoto zákona se rozumí ... významným dodavatelem ten, kdo jako dodavatel s poskytovatelem regulované služby vstupuje do smluvního právního vztahu, který je významný z hlediska bezpečnosti informací ve stanoveném rozsahu řízení kybernetické bezpečnosti,“ Odůvodnění: Původní definice významného dodavatele dopadala na velice široký okruh subjektů, a to – zřejmě nedopatřením i na zákazníky poskytovatele regulované služby, tedy osoby nenesoucí vůči takovému poskytovateli znak dodavatelství. Užití pojmu „právní vztah“ v této definici je taktéž nevhodný, neboť v původním znění definice dopadá například i na škůdce, který způsobí poskytovateli regulované služby významnou újmu – i taková osoba totiž s poskytovatelem vstupuje do právního vztahu.	Akceptováno jinak Nově znění bude následující: "významným dodavatelem ten, kdo jako dodavatel s poskytovatelem regulované služby vstupuje do závazkového vztahu, který je významný z hlediska bezpečnosti informací ve stanoveném rozsahu řízení kybernetické bezpečnosti“. Připomínkové místo s vypořádáním souhlasí.
425. Český telekomunikační klastr	Z	K § 2, odst. 2, písm. i) zákona Návrh textových změn: „Pro účely tohoto zákona se rozumí ... strategicky významnou službou regulovaná služba, splňující kritéria pro identifikaci strategicky významné služby, a to od okamžiku jejich splnění, nebo služba stanovená jako strategicky významná služba u orgánu nebo osoby pravomocným rozhodnutím Úřadu, a to od okamžiku právní moci takového rozhodnutí – jejíž narušení	Akceptováno jinak. Na základě této i dalších připomínek jsme přistoupili k přeformulování definice strategicky významné služby v § 2 odst. 2 písm. i) návrhu zákona, a to tak, že došlo k jejímu sjednocení s definicí strategicky významné služby obsažené v § 28 návrhu zákona. Nově § 2 odst. 2 písm. i) zní: „Strategicky významnou službou regulovaná služba, jejíž narušení by mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek.“ Namítaná

		~~bezpečnosti by mohlo vést k významnému omezení či ohrožení služeb pro občany státu a chodu státu,“~~ Odůvodnění: Uvedená definice pojmu strategicky významná služba je duplicitní k úpravě § 26 a § 27 návrhu zákona a není jasné v jakém vztahu tyto úpravy stojí. Předložená definice pojmu navíc vyvolává otázky ohledně časových aspektů, tj. od kdy se na každou posuzovanou službu mají vztahovat ustanovení zákona vztahující se ke strategicky významným službám. Navrhujeme proto definici změnit popsáním způsobem a obecnou klauzuli, která strategicky významnou službu popisovala, včlenit do definičních kritérií v § 26 a násl. návrhu zákona.	duplicita k definici v § 28 tímto byla odstraněna. Dále uvádíme, že považujeme za vhodné ponechat v § 2 obecnou definici strategicky významné služby a neupravovat ji dle návrhu v připomínce. Máme za to, že je na místě v úvodních částech návrhu zákona vymezit, čím se strategicky významná služba vyčleňuje z množiny regulovaných služeb. Konkrétní kritéria strategicky významné služby jsou řešena v § 27 a § 28. Zvolený způsob práce s pojmem strategicky významná služba v rámci návrhu zákona považujeme za logický a přiléhavý. Současně nespatřujeme problémy stran časových aspektů identifikace, resp. určení strategicky významné služby. Regulovaná služba se stává strategicky významnou službou v momentě, kdy naplní stanovená kritéria pro identifikaci strategicky významné služby (potažmo v návrhu vyhlášky o regulovaných službách, na kterou je v § 28 návrhu zákona odkazováno), nebo od okamžiku, kdy je určena strategicky významnou službou rozhodnutím Úřadu. S vypořádáním této připomínky nesouhlasíme. Navrhované vypořádání neřeší namítané nejasnosti ohledně toho, od kdy je služba považována za strategicky významnou službu a neodstraňuje dvoukolejnost v jejím vymezení. Nebráníme se obecné klauzuli vymezující tento pojem, musí být ale jasné dán její vztah ke kritériím v § 28 návrhu. Lze se inspirovat úpravou nekalé soutěže v občanském zákoníku. Závěr Připomínka je vypořádána.
426. Český telekomunikační klastr	Z	K § 6, odst. 3 zákona	Neakceptováno

	Navrhujeme upravit režim poskytovatele regulované služby přímo v zákoně a nikoliv v prováděcím předpisu. Návrh textových změn: ~~„Režim poskytovatele regulované služby je stanoven prováděcím právním předpisem.~~ Je-li orgán nebo osoba poskytující regulovanou službu určen rozhodnutím Úřadu podle § 5, je vždy poskytovatelem regulované služby v režimu vyšších povinností.“ Odůvodnění: Navrhujeme zakotvení podmínek režimu poskytovatele regulované služby přímo zákonem. Zákonný legislativní proces poskytuje adresátům právní úpravy adekvátní míru stability regulatorního prostředí i právní jistoty, která je nezbytná pro veškeré soukromé hospodářské aktivity. Zákonná úprava nadto ve smyslu Ústavy České republiky představuje projev vůle lidu skrze jeho řádně zvolené zástupce – vykonavatele zákonodárné moci. Tento způsob úpravy je vhodný pro řešení zásadních otázek regulace, mezi které bez jakékoliv pochybnosti patří i okruh regulovaných subjektů. Naproti tomu úprava obsažená v předkládaném návrhu zákona o kybernetické bezpečnosti předpokládá, že otázka okruhu regulovaných subjektů – poskytovatelů regulované služby bude řešena pouhým prováděcím právním předpisem. Předkladatelem navrhovaný postup vnáší do otázky okruhu regulovaných subjektů prvek volatility a nejistoty, která má z podstaty věci negativní dopad na hospodářskou činnost ve státě. Není navíc jasné, čím je odůvodněna potřeba dynamicky a bez užití řádného zákonodárného procesu měnit okruh regulovaných subjektů.	Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech (§ 3 a § 2 písm. d)), tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby (§ 3, ve spojení s § 2 písm. i) a k) a § 22a). Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon (§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)), a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá (§ 3 a § 2 písm. b)). Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. S vypořádáním této připomínky nesouhlasíme. Na obsahu původně uplatněné připomínky trváme. Vymezení klíčových kategorií, jako je zejména okruh adresátů hlavních okruhů povinností dle předkládaného návrhu zákona je zásadním aspektem, bez jehož posouzení v rámci legislativního procesu nelze předložený návrh zákona reálně zhodnotit. Je tomu tak tím spíše, že sám Úřad níže v tomto

			vypořádání zdůraznil, že samotné vyhlášky nejsou předmětem připomínkového řízení a budou dále přepracovávány. Právní jistota o stabilitě regulatorního prostředí v těchto klíčových aspektech musí být dána od počátku a musí trvat i později za účinnosti zákona. Závěr Připomínka je vypořádána.
427. Český telekomunikační klastr	Z	K § 10, odst. 2 zákona Návrh textových změn: „Poskytovatel regulované služby zapsaný v evidenci poskytovatelů regulovaných služeb je povinen plnit všechny povinnosti plynoucí mu ze zákona vůči zapsaným regulovaným službám od uplynutí doby tří měsíců od okamžiku doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb až do okamžiku doručení vyrozumění o výmazu z evidence poskytovatelů regulovaných služeb podle § 11.“ Odůvodnění: Vzhledem ke skutečnosti, že dle ustanovení § 8 odst. 3 návrhu zákona může být dotčený subjekt registrován jako poskytovatel regulované služby bez vlastního přičinění tak, že doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb bude jeho první informace o tom, že spadá do příslušného režimu povinností dle zákona, je naprosto nereálné očekávat, že ihned od okamžiku doručení tohoto vyrozumění bude schopen plnit závazné povinnosti plynoucí mu ze zákona. Pro takto vymezenou skupinu adresátů právní úpravy je dané ustanovení zcela nesplnitelné, což odporuje doktríně racionálního zákonodárce. Navrhujeme proto stanovit nárazníkové období od okamžiku doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb, v němž dotčený subjekt zajistí svou schopnost plnit příslušné zákonné povinnosti. Stejný efekt by	Vysvětleno Den doručení písemného vyrozumění o zápisu do evidence regulovaných služeb je rozhodným datem, se kterým celý zákon pracuje i na jiných místech a počítá se od něj běh některých lhůt. Například jedna z hlavních povinností zavádět bezpečnostní opatření má na zavedení podle § 14 odst. 3 návrhu zákona lhůtu v délce jednoho roku a začíná běžet od tohoto rozhodného data. Neplatí tedy, že by tato povinnost začala platit ihned po doručení vyrozumění o zápisu do evidence. Toto ustanovení pouze říká, že od vyrozumění zápisu do evidence platí, že daná služba je regulovanou službou a poskytovatel regulované služby vůči ní musí plnit své povinnosti. Jednotlivé povinnosti pak vyplývají z dalších ustanovení a mají své samostatné lhůty. S vypořádáním této připomínky nesouhlasíme. Zákon na vícero místech obsahuje povinnosti, které je třeba plnit buď v krátké lhůtě po doručení písemného vyrozumění o zápisu služby do evidence regulovaných služeb nebo ihned, resp. od okamžiku, kdy se dozví o charakteru své služby jako regulované služby, námtkou např. § 12 odst. 3, § 12 odst. 5, § 19 § 20 odst. 2, § 23 odst. 2 nebo § 25 návrhu zákona. Důvody

		mělo i odstranění úpravy registrace poskytovatele regulované služby bez jeho vlastního podnětu.	pro navrhovanou změnu uvedené v odůvodnění naší připomínky tak trvají. Závěr Připomínka je vypořádána.
428. Český telekomunikační klastr	Z	K § 13, odst. 3 zákona Návrh textových změn: „O provedení identifikace a určení organizačních částí a aktiv podle odstavce 1 vede poskytovatel regulované služby dokumentovaný záznam, a to včetně evidence primárních aktiv, která byla ze stanoveného rozsahu vyjmuta, a odůvodnění jejich vyjmutí.“ Odůvodnění: Zákon na žádném místě neupravuje vyjmutí primárních aktiv ze stanoveného rozsahu, není tedy jasné, co se takovým vyjmutím rozumí. Je-li záměrem předkladatele, aby adresát právní úpravy vypracovával negativní seznamy primárních aktiv, která nejsou do stanoveného rozsahu zahrnuta a vypracovával k jejich nezahrnutí individuální odůvodnění, je tato povinnost bez zjevného přínosu neúměrně zatěžující a ve své podstatě duplicitní k povinnosti poskytovatele regulované služby identifikovat aktiva spadající do stanoveného rozsahu dle odst. 1 téhož paragrafu zákona. Odůvodněním nezahrnutí každého primárního aktiva je, že nesplňuje podmínky pro jeho zahrnutí do stanoveného rozsahu dle § 13 odst. 1 zákona.	Neakceptováno Dle směrnice NIS2 měl být rozsah řízení KB stanoven na celou organizaci, aby NÚKIB neúměrně nezatěžoval povinné subjekty, rozhodl se umožnit vyjmout z rozsahu primární aktiva, která s regulovanou službou nesouvisí. Definice řízení KB říká, že je to činnost směřující k zajištění KB regulované služby, tzn. zajištění regulované služby je hlavním cílem, neznamená to však, že by rozsah nemohl být stanoven na celou organizaci, pokud to povinná osoba vyhodnotí jako vhodné, aby mohla KB regulované služby řádně zajistit. Dotčené ustanovení dále stanoví, že je třeba identifikovat primární aktiva organizace a z nich vybrat ta, která souvisí s regulovanou službou. Až nakonec pak identifikovat podpůrná aktiva související s primárními aktivy potřebnými pro regulovanou službu. Tedy organizace nebude evidovat a určovat veškerá aktiva organizace, ale toliko veškerá primární aktiva - tedy informace a služby. Rozsah je pak stanoven pouze na primární aktiva související s regulovanou službou a na ně navázána podpůrná aktiva. Z výše uvedeného vyplývá, že se tak nejedná o identifikaci a evidenci veškerých aktiv organizace, ale pouze veškerých primárních aktiv organizace, což nepovažujeme v kontextu požadavku směrnice NIS2 za administrativně zatěžující, bude se totiž jednat o primární aktiva v množství jednotek a jednoduchého zdůvodnění (např. nesouvisí s regulovanou službou). Je pracováno s

			typovými aktivy, nikoliv s každou službou/informací jako takovou zvlášť. Jde o základní identifikaci služeb, které organizace poskytuje (za jakým účelem je vytvořena a co jsou její nejzákladnější poskytované služby). Evidence pak slouží k tomu, aby bylo možné ověřit, zda byl rozsah stanoven správně. Ze zkušeností z kontrol vyplývá, že povinné osoby mají rozsah často stanoven nesprávně již na úrovni primárních aktiv, proto bylo ustanovení zpřesněno, aby bylo pro povinné osoby návodnější. Následné hodnocení aktiv a rizik se vždy provádí ve stanoveném rozsahu, tedy až na omezeném okruhu, jak primárních, tak podpůrných aktiv. S vypořádáním této připomínky nesouhlasíme. Jakkoliv vnímáme, že se – v duchu textu vypořádání připomínky – jedná pouze o primární aktiva a nikoliv veškerá aktiva poskytovatele, je vytváření negativních seznamů neefektivní administrativní zátěží, která zejména v případě provozovatelů sítí elektronických komunikací a poskytovatelů přístupu k internetu není zcela triviální. Kontrolní a návodný aspekt této povinnosti popsany ve vypořádání dle našeho názoru nevyvažuje administrativní úsilí potřebné k vytvoření a aktualizaci negativního seznamu primárních aktiv, která nejsou v kontextu regulace dle návrhu zákona relevantní. Závěr Připomínka je vypořádána.
429. Český telekomunikační klastr	Z	K § 21, odst. 1 zákona Návrh textových změn: „Úřad je po konzultaci s dotčeným poskytovatelem regulované služby z důvodu ochrany vnitřního či veřejného pořádku a bezpečnosti,	Neakceptováno - nyní § 22 Jak je uvedeno i v důvodové zprávě k tomuto ustanovení, výstraha jako institut je vždy spjata s posouzením toho, zda je v dané situaci převažujícím

		ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn veřejnost informovat o kybernetickém bezpečnostním incidentu s významným dopadem na zabezpečení důležitých společenských nebo ekonomických činností či o porušování povinností daných tímto zákonem s významným dopadem na zabezpečení důležitých společenských nebo ekonomických činností, nebo dotčenému poskytovateli regulované služby rozhodnutím uložit, aby tak učinil sám.“ Odůvodnění: S ohledem na potřebu adresátů úpravy vykonávat ekonomické činnosti v konkurenčním prostředí trhu je informování veřejnosti extrémně tvrdým zásahem do fungování poskytovatele regulované služby, který pro něho může být až likvidační. K takovému kroku je tedy třeba přistoupit teprve až v případě, že jsou pro to dány závažné důvody, které musí být v zákoně definovány. Svévolné či necitlivé užívání tohoto oprávnění úřadem může nezvratně poškodit fungování dotčených trhů způsobem, který nebude možné jednoduše napravit.	zájmem kybernetická bezpečnost právě vůči zásahu do pověsti, a tím i svobody podnikání v případě soukromých organizací. Toto lze dovodit i ze samotného návěti tohoto ustanovení, které přímo stanoví, že výstraha je vydávána právě "z důvodu ochrany vnitřního či veřejného pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu", což je odrazem formulace, kterou jako návrhovaatel žádáte do textu doplnit. Tedy funkce Vámi navrhovaného textu je již obsažena v současné formulaci ustanovení o výstraze. S vypořádáním této připomínky nesouhlasíme. Návěti daného odstavce v rozporu s předloženým vypořádáním vůbec nerefléktuje požadavek významnosti dopadu zákonem chráněné zájmy. Z důvodu ochrany vnitřního či veřejného pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu by Úřad byl oprávněn k informování veřejnosti přistoupit i tehdy, když by hrozba vyjmenovaným chráněným zájmům byla zcela zanedbatelná – i před zanedbatelnou hrozbou je možné se chránit. Takový přístup nepovažujeme za vhodný a přiměřený a trváme na požadavku zohlednění kritéria významnosti dopadu na chráněné zájmy v daném ustanovení. Závěr Připomínka je vypořádána.
430. Český telekomunikační klastr	Z	K § 22, odst. 2 zákona Návrh textových změn: ~~„Poskytovatel regulované služby v režimu vyšších povinností zohlední varování v rámci stanoveného rozsahu, pokud Úřad nebo jiný právní předpis nestanoví jinak.“~~	Vysvětleno - nyní § 23 Úřad nikdy neměl v úmyslu rozšiřovat okruh subjektů, kterých se varování týká nad zákonem stanovenou úroveň, tedy ani globálně, ani vůči poskytovatelům regulovaných služeb v režimu nižších povinností.

	Odůvodnění: Navrhovaný text dává NÚKIB možnost prostřednictvím varování ukládat relativně blíže neurčenému okruhu osob povinnosti, které by adresát úpravy – zde poskytovatel regulované služby – byl bez dalšího povinen plnit. Vzhledem k okruhu adresátů, kteří by byli nuceni takto uložené povinnosti plnit, mohou být takové povinnosti ukládány přinejmenším formou opatření obecné povahy na základě zákonného zmocnění. Opatření obecné povahy je přitom ze zákona spojeno s procesními náležitostmi a prostředky procesní obrany, které v případě varování dle předloženého návrhu chybí. Máme za to, že v předložené podobě je návrh co do otázky závazné povahy varování neústavní. Chápeme potřebu NÚKIB rychle a bez nadbytečných procedurálních formalit reagovat na vyvíjející se charakteristiky kybernetického prostředí a vhodným způsobem varovat soukromý sektor, nemůže se tak však dít formou ukládání závazných povinností.	Úřad toto ustanovení zahrnul pouze proto, aby v případech, kdy je zejména hrozba relevantní pouze pro některé odvětví, mohl navázat varování vůči naopak úžeji vymezenému počtu subjektů. Rozšířit varování na subjekty mimo zákon o kybernetické bezpečnosti pouhým rozhodnutím Úřadu by nebylo legální a rozšíření na poskytovatele regulované služby v režimu nižších povinností je neúčelné, jelikož tito neprovádějí povinně analýzu rizik, do které by mohli tuto změnu hodnoty hrozby či zranitelnosti implementovat. Tedy tato varianta není rovněž z pozice Úřadu relevantní. Toto je také příslušně doplněno do důvodové zprávy, aby o úmyslu Úřadu s použitím tohoto ustanovení nebylo pochyb. Co se týká jiného právního předpisu, který může subjekty zavázat k aplikaci varování, to vychází z faktu, že vzrůstá trend sektorové regulace, která zahrnuje mimo regulaci sektorovou i regulaci kybernetické bezpečnosti. Při její implementaci ze strany sektorových regulátorů zaznává, že by těmto regulátorům připadalo účelné ve svých předpisech zavázat některé subjekty, u kterých to systém řízení bezpečnosti umožňuje (jde o řízení prostřednictvím rizik) a jsou zároveň postaveni mimo dosah zákona o kybernetické bezpečnosti k tomu, aby se tyto organizace řídily varováními vydanými Úřadem. Z tohoto důvodu je tu ponechán prostor pro jiný právní předpis stejné právní síly, tedy zákon, k tomu, aby zavázal další povinné osoby k dodržování varování. S vypořádáním této připomínky nesouhlasíme. Pokud by měly varováním být ukládány závazné povinnosti obecně vymezenému okruhu povinných osob – tak jak vyplývá z předloženého návrhu – musí být jasně stanovena jeho forma (zde zřejmě opatření

			obecné povahy) a prostředky procesní obrany proti němu. Považujeme ale za vhodnější, aby varování mělo spíše doporučující, nezávazný charakter tak, jak uvádí naše připomínka. Závěr Připomínka je vypořádána.
431. Český telekomunikační klastr	Z	K § 23, odst. 3 zákona Návrh textových změn: „Rozhodnutí o povinnosti provést reaktivní protiopatření může být prvním úkonem v řízení. ~~Nepodaří-li se rozhodnutí adresátovi doručit do vlastních rukou do 72 hodin od jeho vydání, doručí se mu tak, že se vyvěsí na úřední desce Úřadu a tímto okamžikem je vykonatelné.~~ Rozhodnutí podle věty první může Úřad vydat i v řízení na místě podle správního řádu. Rozklad podaný proti rozhodnutí podle odstavce 1 nemá odkladný účinek.“ Odůvodnění: Doručování Rozhodnutí o povinnosti provést reaktivní protiopatření jeho vyvěšením na úřední desce úřadu je podstatným zásahem do právní jistoty adresátů právní úpravy a prakticky vyžaduje alokaci stálých kapacit na neustálé monitorování úřední desky NÚKIB a potažmo úředních desek prakticky všech státních orgánů (v rozsahu, v jakém by obdobný přístup zvolily také). To lze bez nadsázky považovat za příklad nemístné regulatorní zátěže soukromého podnikání. Takový přístup je obzvláště záležející za situace, kdy jedinou jeho alternativou je doručování do vlastních rukou adresáta v rámci 72 hodin. Za vhodnější považujeme – v případě, že rozhodnutí nebude možné doručit do vlastních rukou – využít některou z možností elektronického doručování dotčeným subjektům.	Vysvětleno - nyní § 24 Ustanovení míří především na situace, kdy by bylo třeba bezprostředně reagovat na obsah reaktivního opatření a soukromoprávní poskytovatel regulované služby (vždy podnikající FO nebo PO) bude oddalovat doručení pomocí datové schránky. Varianta doručení do vlastních rukou listinným dopisem nebyla vůbec zvažována (s ohledem na povinnost podnikajících FO a PO mít datovou schránku a povinnost Úřadu do ní doručovat). Sekundárně bude adresát vyrozuměn v rámci Portálu, nicméně doručení v rámci tohoto systému nesplňuje požadavky správního řádu na doručení rozhodnutí, proto bude reaktivní protiopatření vždy doručováno i do datové schránky. S vypořádáním této připomínky nesouhlasíme. Doručování do datové schránky je i z našeho pohledu preferovaný způsob doručení. Text návrhu zákona ale tomuto způsobu doručování neodpovídá. Dle § 17 odst. 6 zákona 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, má doručení dokumentu do datové schránky stejné právní účinky jako doručení do vlastních rukou, z textace i systematiky zákona se však o doručení do datové schránky doručením do vlastních rukou nestává – oba pojmy jsou odlišné a zachovávají si vlastní význam, zákon pouze upravuje

			jejich právní účinky. Úřadem navrhovaná textace je naší připomínkou napadána právě proto, že cílí jen na doručení do vlastních rukou, nikoliv na jiné způsoby doručení, které jsou mu postaveny na roveň, jako je například doručení do datové schránky. Závěr Připomínka je vypořádána.
432. Český telekomunikační klastr	Z	K § 28, odst. 3, písm. a) zákona Návrh textových změn: „Pro potřeby mechanismu prověřování bezpečnosti dodavatelského řetězce se rozumí kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle ~~prováděcího právního předpisu tohoto zákona~~ ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní vysoká nebo kritická; ~~kritickou částí stanoveného rozsahu jsou vždy alespoň aktiva stanoveného rozsahu strategicky významné služby, která zajišťují nepominutelné funkce stanoveného rozsahu stanovené prováděcím právním předpisem,~~“ Odůvodnění: Zásadní nevhodnost úpravy klíčových aspektů regulace pouhými prováděcími předpisy byla již zdůvodněna v našich předchozích připomínkách, na něž tímto odkazujeme. Nad rámec toho, však navrhuje vypuštění pevných kritérií, za kterých má určité aktivum spadat do definice kritické části stanoveného rozsahu. Takový postup prakticky anuluje schopnost poskytovatele služby, který je nejlépe informován o charakteristikách a bezpečnostních aspektech svých aktiv, ohodnocovat dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby dle věty první. Předložené definice jsou potom natolik obecné, že do nich spadají koncová zařízení jednotlivých účastníků a jiné periferní části sítě, u	Neakceptováno - nyní § 29 Dle názoru NÚKIB vyhláška o nepominutelných funkcích představuje efektivní nástroj cílící na vše, co je v rámci fungování veřejných komunikačních sítí kritické, a to bez ohledu na umístění konkrétních funkcí v rámci architektury sítě. To znamená, že z pohledu kybernetické bezpečnosti je kritická jak funkčnost jádra sítě, tak také vybraných funkcí ostatních částí sítě, jako například funkce v rádiové přístupové síti, bez nichž by jádro sítě nemohlo být propojeno s koncovými zařízeními. Tím by mohlo dojít ke znefunkčnění takové sítě. Z toho důvodu se jedná o ochranu tzv. pevně daných funkcí, přičemž vyhláška chrání ty, které jsou pro fungování sítě kritické. Nutno dodat, že obdobná úprava není v rámci Evropy ojedinělá. Obdobným způsobem stanovuje seznam kritických funkcí také Finsko či Velká Británie. Vzhledem ke komplexitě telekomunikačních sítí, ale také vysoké úrovni zpracování architektur těchto sítí na úrovni mezinárodních standardizačních organizací, má právě toto odvětví vlastní vyhlášku. V případě kompromitace těchto nepominutelných funkcí může být narušeno či porušeno nejen poskytování služeb koncovým uživatelům, ale také dalších strategicky

		nichž lze přísný režim spojený s kritickou částí stanoveného rozsahu považovat za zcela zjevně nepřiměřený. Předkladatel návrhu zákona nezohledňuje, že I u menších poskytovatelů služeb elektronických komunikací představují zařízení na perifériích sítě doslova desítky tisíc prvků, které by případnou regulací byly dotčeny a které přitom nemají zásadní vliv na fungování služby jako celku. Necitlivá regulace v této otázce může vést až k likvidačním následkům pro velkou část poskytovatelů služeb elektronických komunikací na území České republiky, zejména pak regionálních ISP, kteří tvoří většinu subjektů na trhu přístupu v pevném místě, a může fatálně zhoršit fungování hospodářské soutěže na daném trhu. Pokud by této připomínce nebylo vyhověno a aspekt zajišťování nepominutelných funkcí byl v zákoně zachován, navrhuje výslovné zakotvení toho, že kritickou částí stanoveného rozsahu jsou pouze aktiva v jádru sítě a nikoliv v jejích perifériích.	významných služeb, které jsou na telekomunikačních sítích závislé. S vypořádáním této připomínky nesouhlasíme. Důvody pro navrhovanou změnu textu uvedené v odůvodnění naší připomínky trvají. Vztažení režimu kritické části stanoveného rozsahu na veškeré – i okrajové – části sítě je zcela zjevně nepřiměřené významu těchto zařízení pro zájmy chráněné tímto zákonem. Potřebě definice kritické částí stanoveného rozsahu je z pohledu zákona učiněno zadost již částí daného ustanovení před středníkem. Dvoukolejnost zahrnující nejen věcné hodnocení dle významu daných aktiv ale také tvrdá kritéria dle nepominutelných funkcí vede z právního pohledu k nežádoucímu formalismu a kazuistice, z pohledu hospodářského pak hrozí drastickými následky pro celý trh připojení k internetu v pevném místě, v případě, kdy by bylo z důvodu regulace dodavatelského řetězce nutné vyměňovat na celém trhu statisíce (sic!) koncových zařízení. Závěr Připomínka je vypořádána.
433. Český telekomunikační klastr	Z	K § 30, odst. 1 zákona Návrh textových změn: „Úřad vydá opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, zjistí-li na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Při stanovení podmínek dle předchozí věty je Úřad povinen přijmout vždy jen takové podmínky, které budou pro jejich adresáty nejméně	Neakceptováno - nyní § 31 Již nyní je NÚKIB, stejně jako každý jiný správní orgán, povinen řídit se zákonem č. 500/2004 Sb., správní řád, jehož základní zásady činnosti správních orgánů jsou kodifikovány obdobně jako zásady trestního práva v zákoně č. 40/2009 Sb., trestní zákoník. Ust. § 2 zavazují NÚKIB, aby postupoval v souladu s principem proporcionality. Navrhovanou úpravu § 30 odst. 1 tak považujeme za nadbytečnou.

	zatěžující při zachování účelu odvrácení významného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. K zákazu využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu může Úřad přistoupit jen tehdy, nelze-li významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku odvrátit pouhým stanovením podmínek dle věty první tohoto odstavce. Lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy stanoví Úřad tak, aby tato lhůta byla pro poskytovatele strategicky významné služby nejméně zatěžující, při zachování účelu odvrácení významného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby. Opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu lze vydat nejvýše na dobu v délce trvání tří let ode dne konce lhůty pro zohlednění podmínek nebo zákazu obsaženého v daném opatření obecné povahy.“ Odůvodnění: Navrhujeme výslovné zakotvení důsledné povinnosti úřadu užívat povinnosti či zákazy upravené daným ustanovením jen jako ultima ratio a při současném striktním dodržování zásady proporcionality. Takové výslovné zakotvení není v právním řádu ojedinělé – najdeme jej například v § 12 odst. 2 trestního zákoníku. Důvodem pro jeho zahrnutí do daného paragrafu zákona o kybernetické bezpečnosti je pak velmi vysoký potenciál oprávnění svěřovaného takto zákonem úřadu způsobit při necitlivém zásahu podstatné škody celým odvětvím trhu. Zahrnutí takto výslovných obsahových omezení pro vydávání opatření obecné povahy je pak z praktického pohledu nezbytné pro možnost napadat opatření zákonným postupem u soudu, kdy je zpravidla pro procesní úspěch nezbytné ilustrovat jednoznačný rozpor s konkrétním a relevantním ustanovením zákona, nikoliv pouze s obecnými pravidly normotvorby.	Stejně tak není potřebné omezovat dobu trvání opatření obecné povahy. Mimo standardní přezkumné řízení a řízení o zrušení opatření obecné povahy bude NÚKIB provádět vlastní přezkum, jehož cílem bude zhodnocení, zdali má opatření v dané podobě stále smysl. Výsledkem pak může být změna či zrušení opatření. Cílem NÚKIB není omezení trhu, nýbrž zajištění kybernetické bezpečnosti. Proto jakmile se NÚKIB dozví o pomnutí (či jiné změně) hrozby v podobě rizikovost dodavatele, bude bez zbytečného odkladu reagovat. S vypořádáním této připomínky nesouhlasíme. Zásady proporcionality vyjádřené v § 2 s.ř. jsou ve vztahu k přijímané úpravě příliš obecné a prakticky v soudním řízení nevynutitelné. Tato zásada je nadto založena na právních pojmech s neurčitým obsahem, jako je „šetření práv osob“ a „nezbytný rozsah“ jejichž výklad by se musel realizovat vždy ad hoc v každém soudním řízení. Pro posílení právní jistoty a vymahatelnosti práva je vhodnější obsah těchto neurčitých pojmů v zákoně konkretizovat, a to i s ohledem na dodržení ústavního požadavku předvídatelnosti dle čl. 4, odst. 3 LZPS. Omezení trvání opatření obecné povahy je pro ochranu práv adresátů úpravy nezbytné, neboť závazek Úřadu přezkoumávat tato OOP je z pohledu adresáta právní úpravy nevynutitelný a předmětné OOP z tohoto důvodu po uplynutí jednoho roku lhůty nenapadnutelné. Závěr Připomínka je vypořádána.

		S ohledem zákonnou nemožnost procesní obrany proti opatření obecné povahy po uplynutí lhůty jednoho roku od jeho vydání, navrhuje limitovat trvání OOP na tři roky s tím, že v případě trvání důvodů, pro které bylo opatření vydáno, bude jeho obsah vydán ve formě nového opatření, které bude moci být opětovně podle aktuální situace přezkoumáno soudy.	
434. Český telekomunikační klastr	Z	K § 30, odst. 1 zákona Navrhujeme do zákona včlenit vhodný mechanismus náhrady škod a účelně vynaložených nákladů poskytovatelů strategicky významné služby spojených s implementací povinností a zákazů vyplývajících z opatření obecné povahy vydávaného dle § 30, odst. 1 zákona. Odůvodnění: S ohledem na hrozící zásah do legitimního očekávání hospodářských subjektů, které jsou adresáty dotčené regulace, a způsobení škody vinou nemožnosti vyčerpat ekonomickou hodnotu investic provedených v dobré víře a při zachování obezřetnosti řádného hospodáře v důsledku zákazů či omezení vyplývajících z předmětného OOP je třeba do zákona zahrnout kompenzaci, jejímž účelem bude minimalizace přímých škod, které by mohly ohrozit fungování či efektivitu činnosti poskytovatelů strategicky významných služeb. Nedostatek takové úpravy kompenzace v zákoně by mohl znamenat rozpor zákona s ústavně zaručenou svobodu podnikání vyplývající z Listiny základních práv a svobod.	Neakceptováno Navrhovaná právní úprava je ve své současné podobě ústavně konformní, kvůli čemuž není důvod přidávat ustanovení o náhradě škod. Vzhledem k charakteru navrhované právní úpravy, převážně v oblasti mechanismu bezpečnosti dodavatelského řetězce, která se snaží vyjít vstříc povinným osobám například v otázkách životních cyklů technologií nebo zamezení možné závislosti na jedné technologii skrz systém výjimek, není nutné, aby možnost kompenzací byla upravena přímo v zákoně; přirozeně tím však nejsou dotčena např. práva na náhradu škody či kompenzace podle jiných právních předpisů. Zároveň platí, že pro vydání omezení či zákazu formou opatření obecné povahy budou posuzovány veškeré okolnosti a reálné dopady na trh a podnikatelské prostředí. Z toho důvodu by NÚKIB posuzoval jak životnost jednotlivých technologií, tak například možnosti jednotlivých povinných subjektů či postavení dodavatele na českém trhu apod. S vypořádáním této připomínky nesouhlasíme. Důvody pro navrhovanou změnu textu uvedené v odůvodnění naší připomínky trvají. Závěr Připomínka je vypořádána.

435. Český telekomunikační klastr	Z	K § 30, odst. 3 zákona Návrh textových změn: „Po informování členů Bezpečnostní rady státu podle odstavce 2 písmene a) nebo po projednání podle odstavce 2 písm. b) Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu opatření obecné povahy podávali připomínky. Lhůta pro podání připomínek činí 30 dnů, nestanoví-li Úřad jinak. Úřad uplatněným připomínkám vyhoví, bude-li to možné a nebude-li tím ohrožen účel vydávaného opatření obecné povahy. Ustanovení § 172 odst. 1 a 5, § 173 odst. 1 věty první, část věty za středníkem, a § 173 odst. 1 věty druhé správního řádu se pro postup podle tohoto ustanovení nepoužijí.“ Odůvodnění: S ohledem na možný zásadní dopad navrhovaného opatření obecné povahy považujeme za vhodné výslovné zakotvení závazku NÚKIB vyhovět uplatněným připomínkám, bude-li to možné (tj. například nebudou-li připomínky v neřešitelném rozporu) a nebude-li tím ohrožen účel vydávaného OOP.	Neakceptováno - nyní § 31 Není důvodné do připomínkovaného ustanovení tuto větu doplňovat. Navrhovaná změna cílí na samotný účel připomínek, který plyne z podstaty tohoto institutu. Připomínkování opatření obecné povahy je zakotveno v § 172 správního řádu, který stanovuje správnímu orgánu povinnost se s připomínkami zabývat a vypořádat se s nimi v jeho odůvodnění. Úřad je proto povinen se s připomínkami řádně vypořádat, a v případech, kdy to bude možné, a nebude to odporovat účelu opatření obecné povahy, připomínky zohlednit a vyhovět jim. Obdobně o nemožnosti pouze formálního vypořádání připomínek mluví i judikatura NSS (rozsudek NSS ze dne 15. 09. 2010, č. j. 4 Ao 5/2010-48). Není tedy nutné explicitně zakotvit tuto povinnost do právní úpravy, jelikož by ustanovení vytvářelo duplicitu. S vypořádáním této připomínky nesouhlasíme. Duplicita s úpravou ve správním řádu akcentovaná ve vypořádání naší připomínky není reálně dána. Správní řád i odkazovaná judikatura zakotvují povinnost úřadu pouze se s uplatněnými námitkami vypořádat, tj. je posoudit volným uvážením v kontextu právního řádu i řešené situace a následně o nich rozhodnout. Námi uplatněná připomínka navrhuje zakotvení pravidla, kterým by se Úřad měl v rámci výše uvedeného uvážení řídit – jde tedy nad rámec zákonné úpravy námitek dle § 172 s.ř., a to v zájmu ochrany legitimního očekávání a oprávněných zájmů adresátů opatření. Navrhovaná změna napomůže praktické realizaci právní ochrany adresátů opatření. Závěr

			Připomínka je vypořádána.
436. Český telekomunikační klastr	Z	K § 31, odst. 5 zákona Navrhujeme doplnit odstavec následujícího znění: „Úřad zveřejní informace o udělené výjimce způsobem umožňujícím dálkový přístup do jednoho měsíce od právní moci rozhodnutí, kterým byla tato výjimka udělena. Způsobem dle předchozí věty Úřad zveřejní údaje o totožnosti poskytovatele strategicky významné služby, kterému byla výjimka udělena, všech strategicky významných službách, k nimž se tato výjimka vztahuje, rozsahu udělené výjimky a shrnutí hlavních důvodů a skutečností, na nichž je rozhodnutí o udělení výjimky založeno.“ Odůvodnění: Aby byla zachována rovnost adresátů právní úpravy před zákonem a aby nebyla narušována hospodářská soutěž mezi nimi, nesmí být osoba, které byla dle daného ustanovení povolena výjimka, zvýhodněna proti ostatním soutěžitelům na daném trhu. Ostatní adresáti povinností, z nichž může být udělena výjimka dle tohoto odstavce, musí být formou zveřejnění klíčových aspektů rozhodnutí informováni o možnosti povolení dané výjimky a kritériích jejího přiznání a musí jim být umožněno za obdobných podmínek o výjimku požádat také. Takto budou minimalizovány negativní dopady na hospodářskou soutěž na daném trhu a podpořena transparentnost v rozhodování Úřadu.	Neakceptováno - nyní § 32 Návrh není možné akceptovat, neboť výjimky nebudou zveřejňovány, a to především proto, že zveřejnění rozhodnutí o výjimce může potenciálně ohrozit kybernetickou bezpečnost, a tím být přímo v rozporu se zájmy, na jejichž ochranu nZKB směřuje. Některé části nelze zveřejňovat ani zpřístupňovat jiným subjektům než adresátům rozhodnutí, z tohoto důvodu také mohou být utajované informace podle § 67 nZKB vyjmuty ze spisu. Informace o obsahu rozhodnutí o výjimce nebude možné získat ani podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, protože poskytnutí informací tímto způsobem by totiž muselo být, v souladu s předmětnou judikaturou NSS, kvalifikováno jako o nahlížení do spisu, což lze umožnit pouze vyjmenovanému okruhu subjektů. V souvislosti s udělováním výjimek budou zveřejňovány pouze statistické údaje, např. údaje o počtu udělených výjimek; informace o tom, v jaké oblasti byly výjimky uděleny a podobně. S vypořádáním této připomínky nesouhlasíme. Vypořádání připomínky není přiléhavé, odporuje zásadě transparentnosti výkonu státní moci a může závažně poškodit hospodářskou soutěž. Totéž platí o vyloučení možnosti zjišťování informací dle zákona o svobodném přístupu k informacím. Pokud by předmětné rozhodnutí obsahovalo údaje, které nelze sdělit proto, že jejich sdělení by ohrožovalo kybernetickou bezpečnost, je možné

			z něho vyjmout (začernit či jinak znepřístupnit) právě a pouze tyto údaje. Závěr Připomínka je vypořádána.
437. Český telekomunikační klastr	Z	K § 40, odst. 1, písm. b) zákona Návrh textových změn: „vyžádat si od orgánů a osob informace o věcných prostředcích, o výrobních, provozních a personálních kapacitách a o objemu zásob ve stanovených druzích materiálu, přičemž tyto orgány a osoby mají povinnost poskytnout Úřadu vyžadované informace úplně a pravdivě v Úřadem stanovené přiměřené lhůtě,“ Odůvodnění: Navrhujeme zakotvit požadavek přiměřenosti lhůty stanovované úřadem neboť předložené znění návrhu umožňuje NÚKIB závazně stanovovat i lhůty, které budou pro adresáty úpravy zcela nesplnitelné, což je v rozporu s požadavkem racionality normotvorby.	Neakceptováno - nyní § 41 Úřad je vždy povinen dávat pouze takové lhůty, které jsou přiměřeně splnitelné, k tomu jej váží zásady správního práva, které jsou aplikovány vždy i v případech, že by se samotná pravidla správního řádu neuplatňovala. V opačném případě by se jednalo o nezákonný postup daného orgánu státu. Doplnění tohoto slova by tak bylo nadbytečné a bylo by zároveň z hlediska legislativní tvorby nutné jej umístit na všechna místa, kde se tato zásada bude uplatňovat, tedy kdekoliv bude Úřad brát přiměřenost na zřetel, aby tento náhlý výskyt slova přiměřenost ve vztahu k rozhodování Úřadem nemohlo indikovat, že jinde se přiměřenost aplikovat nemíní. S vypořádáním této připomínky nesouhlasíme. Důvody pro navrhovanou změnu textu uvedené v odůvodnění naší připomínky trvají. Závěr Připomínka je vypořádána.
438. Český telekomunikační klastr	Z	K § 40, odst. 1, písm. e) zákona Návrh textových změn: „zakázat orgánům a osobám, které k tomu byly Úřadem vyzvány, používání technických aktiv v případě, že jsou taková aktiva bezprostředně ohrožena kybernetickým bezpečnostním incidentem s významným dopadem na zabezpečení důležitých společenských	Neakceptováno - nyní § 41 Doplnění takové podmínky by dále zatížilo proces řešení stavu kybernetického nebezpečí a zároveň by bylo nekonzistentní s nově navrženou úpravou. Po konzultaci s gestorem problematiky krizového řízení - Ministerstvem vnitra, Generálním ředitelstvím Hasičského záchranného sboru, je nově stav

		nebo ekonomických činností, který je může významně poškodit nebo zničit, nebo jsou takovým incidentem již postižena,“ Odůvodnění: Navrhujeme zakotvit kvalifikační kritérium bezpečnostního incidentu přičemž v případech, kdy toto kritérium nebude naplněno, bude vyhodnocení rizik spojených s užíváním aktiv ponecháno jejich provozovatelům, respektive uživatelům. Důvodem návrhu je snaha o zmírnění tvrdosti předkládané úpravy.	kybernetického nebezpečí koncipován jako nástroj k řešení ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru, které může mít za následek negativní dopady na poskytování regulovaných služeb nebo na zachování základních funkcí státu, hospodářských činností, bezpečnosti, veřejného zdraví, majetku nebo životního prostředí. Úmyslem není omezovat tento zákaz pouze na technická aktiva bezprostředně ohrožena incidentem s významným dopadem na zabezpečení důležitý společenských nebo ekonomických činností. Máme za to, že by mohlo být prakticky obtížné vymezit nějakou hranici, kdy má používání nějakého aktiva významný dopad a kdy ne, případně i rozlišovat do jaké míry se aktiva vzájemně ovlivňují. S vypořádáním této připomínky nesouhlasíme. Důvody pro navrhovanou změnu textu uvedené v odůvodnění naší připomínky trvají. Závěr Připomínka je vypořádána.
439. Český telekomunikační klastr	Z	K § 40, odst. 1, písm. f) zákona Návrh textových změn: „uložit orgánům či osobám povinnost provést přiměřená opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před kybernetickým bezpečnostním incidentem a oznámit provedení opatření a jeho výsledek Úřadu,“ Odůvodnění: Navrhujeme zakotvit požadavek přiměřenosti opatření ukládaných úřadem neboť předložené znění návrhu umožňuje NÚKIB závazně stanovovat i opatření, které budou pro adresáty úpravy zcela	Neakceptováno - nyní § 41 Úřad je vždy povinen vybrat taková opatření, která jsou vzhledem k dané situaci přiměřená, k tomu jej váží zásady správního práva, které jsou aplikovány vždy i v případě, že by se samotná pravidla správního řádu neuplatňovala. V opačném případě by se jednalo o nezákonný postup daného orgánu státu. Doplnění tohoto slova by tak bylo nadbytečné a bylo by zároveň z hlediska legislativní tvorby nutné jej umístit na všechna místa, kde se tato zásada bude uplatňovat, tedy kdekoliv bude Úřad brát přiměřenost na zřetel, aby tento náhlý výskyt slova přiměřenost ve vztahu k

		nesplnitelná, či jejichž dopady budou ve zjevném ekonomickém rozporu s hrozící újmou.	rozhodování Úřadem nemohlo indikovat, že jinde se přiměřenost aplikovat nemíní. S vypořádáním této připomínky nesouhlasíme. Důvody pro navrhovanou změnu textu uvedené v odůvodnění naší připomínky trvají. Závěr Připomínka je vypořádána.
440. Český telekomunikační klastr	Z	K § 41, odst. 5, písm. m) zákona Návrh textových změn: „prioritizuje poskytování svých služeb a výkon svých činností podle přístupu založeného na rizicích a dostupných kapacitách; tím však nejsou dotčena práva účastníků řízení a dalších osob vstupujících s Úřadem do úředního styku plynoucí z tohoto zákona nebo jiných právních předpisů.“ Odůvodnění: Navrhujeme upřesnění textu návrhu zákona tak, aby bylo bez jakýchkoliv pochybností jasné, že prioritizace činností úřadu nebude mít negativní vliv na procesní práva účastníků řízení a dalších osob vstupujících s Úřadem do úředního styku.	Neakceptováno Pro úřední styk je Úřad vázán zákonem č. 500/2004 Sb., správní řád, který v § 2 až § 8 obsahuje základní zásady činnosti správních orgánů. Za účelem řádného výkonu činnosti jsou správní orgány rovněž vázány lhůtami. Není proto namístě doplňovat § 41 odst. 5 písm. m) návrhu zákona uvedeným způsobem, tím spíše, pokud ani jiný zákon takovou formulaci neobsahuje. S vypořádáním této připomínky nesouhlasíme. Argument Úřadu, že je vázán zákonem č. 500/2004 Sb., správní řád a že není na místě doplňovat § 41 odst. 5 písm. m) návrhu zákona uvedeným způsobem, tím spíše, pokud ani jiný zákon takovou formulaci neobsahuje, není v daném kontextu příslušný. Jiný zákon také neobsahuje formulaci o prioritizaci poskytování služeb a výkonu činností správního orgánu podle přístupu založeného na rizicích a dostupných kapacitách. Tato formulace by mohla být ve vztahu k obecným ustanovením správního práva chápána jako lex specialis, nehledě na to, že pro určité typy činností předložený návrh zákona užití správního řádu vylučuje.

			Důvodnost navrhovaného ustanovení § 41 nadto není zřejmá. Závěr Přípomínka je vypořádána.
441. Český telekomunikační klastr	Z	K § 55, odst. 1, zákona Návrh textových změn: „Prováděcí právní předpis stanoví a) ~~kritéria pro identifikaci regulované služby (§ 4),~~ b) ~~způsob stanovení režimu poskytovatele regulované služby (§ 6 odst. 3),~~ c) ~~bezpečnostní opatření odpovídající režimu poskytovatele regulované služby a míru a způsob jejich zavedení a provádění (§14 odst. 2 a 4),~~ d) způsob stanovení významného dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby v režimu nižších povinností (§ 16 odst. 3), e) obsahové náležitosti, formát a způsob oznámení provedení protipatření a jeho výsledku (§ 20 odst. 3), f) ~~kritéria pro identifikaci strategicky významné služby (§ 27 odst. 4),~~ g) ~~nepominutelné funkce stanoveného rozsahu (§ 28 odst. 4),~~ h) kritéria rizikovosti dodavatele a způsob jejich vyhodnocení (§ 28 odst. 4), i) způsob hlášení údajů subjektem poskytujícím služby registrace jmen domén (§ 35 odst. 1) a j) technické a organizační podmínky používání Portálu NÚKIB, obsahové náležitosti, formát, strukturu a způsob provádění úkonů uvedených v § 44 odst. 2 (§ 44 odst. 3).“ Odůvodnění: Navrhujeme zakotvení kritérií pro identifikaci regulované služby (§ 4), způsobu stanovení režimu poskytovatele regulované služby (§ 6 odst. 3), bezpečnostních opatření odpovídajících režimu	Neakceptováno Ust. § 55 bylo z návrhu vypuštěno. K problematice lze však uvést, že návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech (§ 3 a § 2 písm. d)), tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby (§ 3, ve spojení s § 2 písm. i) a k) a § 22a). Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon (§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)), a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá (§ 3 a § 2 písm. b)). Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti.

		poskytovatele regulované služby a míru a způsob jejich zavedení a provádění (§14 odst. 2 a 4), a kritérií pro identifikaci strategicky významné služby (§ 27 odst. 1) přímo zákonem. Zákonný legislativní proces poskytuje adresátům právní úpravy adekvátní míru stability regulatorního prostředí i právní jistoty, která je nezbytná pro veškeré soukromé hospodářské aktivity. Zákonná úprava nadto ve smyslu Ústavy České republiky představuje projev vůle lidu skrze jeho řádně zvolené zástupce – vykonavatele zákonodárné moci. Tento způsob úpravy je vhodný pro řešení zásadních otázek regulace, mezi které bez jakékoliv pochybnosti patří i okruh regulovaných subjektů a stanovení jejich zásadních povinností. Naproti tomu úprava obsažená v předkládaném návrhu zákona o kybernetické bezpečnosti předpokládá, že otázka okruhu regulovaných subjektů – zejména poskytovatelů regulované služby a poskytovatelů strategicky významné služby – bude řešena pouhým prováděcím právním předpisem. Předkladatelem navrhovaný postup vnáší do otázky okruhu regulovaných subjektů a jejich klíčových povinností prvek volatility a nejistoty, která má z podstaty věci negativní dopad na hospodářskou činnost ve státě. Není navíc jasné, čím je odůvodněna zejména potřeba dynamicky a bez užití řádného zákonodárného procesu měnit okruh regulovaných subjektů.	S vypořádáním této připomínky nesouhlasíme. Na obsahu původně uplatněné připomínky trváme, a to bez ohledu na to, kam či jakým způsobem bylo příslušné ustanovení přesunuto. Vymezení klíčových kategorií, jako je zejména okruh adresátů hlavních okruhů povinností dle předkládaného návrhu zákona je zásadním aspektem, bez jehož posouzení v rámci legislativního procesu nelze předložený návrh zákona reálně zhodnotit. Je tomu tak tím spíše, že sám Úřad níže v tomto vypořádání zdůraznil, že samotné vyhlášky nejsou předmětem připomínkového řízení a budou dále přepracovávány. Právní jistota o stabilitě regulatorního prostředí v těchto klíčových aspektech pak musí trvat i později za účinnosti zákona. Závěr Připomínka je vypořádána.
442. Český telekomunikační klastr	Z	K § 57, odst. 3, zákona Návrh textových změn: ~~„Rozklad proti rozhodnutí o uložení nápravného opatření nemá odkladný účinek.“~~ Odůvodnění: Povinnost plnit uložená opatření bez možnosti včasného přezkumu zásadním způsobem zasahuje do možností procesní obrany adresátů právní úpravy a potenciálně stojí v rozporu s ústavně zaručeným právem na spravedlivý proces dle Listiny základních práv a povinností. Újmu způsobenou nezákonným rozhodnutím, které bylo později zrušeno, v mnoha případech již nebude možné účinně sanovat.	Neakceptováno - nyní § 59 K uložení nápravného opatření bude standardně přistoupeno na základě provedené kontroly. Povinná osoba tak bude mít možnost se proti zjištěním NÚKIB bránit již v rámci kontroly. Návrh zákona dále umožňuje nápravné opatření uložit ve skutkově jasných případech i bez provedené kontroly. Toto se bude typicky týkat porušení oznamovacích povinností nebo provedení úkonů, které lze zkontrolovat tzv. od stolu (zejm. na základě poskytnuté dokumentace). Ve všech případech bude nápravné opatření ukládáno ve správních řízeních vedených podle zákona č. 500/2004 Sb., povinná osoba tedy bude moci v pozici

			účastníka řízení využít všech obraných prostředků, které ji správní řád poskytuje. Praktické poznatky za posledních 6 let aplikace zákona č. 181/2014 Sb. vedou k závěru, že možnost odkladného účinku nápravného opatření v případě rozkladu proti němu je z logiky věci zcela v rozporu s podstatou tohoto nástroje. Z tohoto důvodu také návrh zákona vylučuje odkladný účinek rozkladu podaného proti rozhodnutí o uložení nápravného opatření. Nápravná opatření jsou ukládána v důsledku porušení zákonných povinností, zejm. porušení povinnosti zabezpečit informační systém zavedením bezpečnostních opatření podle prováděcího předpisu. Takový informační systém je zranitelný a náchylný k incidentům. Nápravným opatřením se z podstaty věci ukládá povinnost identifikovaná porušení napravit, nejde tedy o žádnou nečekanou povinnost, na kterou by povinná osoba potřebovala nějakou speciální přípravu, nebo vůči které by se měla principiálně bránit (protože povinnost ji splnit jí vyplývá přímo ze zákona). Součástí nápravných opatření je lhůta, ve které mají být opatření splněna. Taková lhůta musí být z podstaty věci přiměřená povinnostem, které jsou nápravným opatřením ukládány, a zohledňovat konkrétní skutkové okolnosti (tyto požadavky vychází z obecných principů rozhodování správních orgánů). Předmětem rozhodování o uložení nápravného opatření je tedy náprava nezákonného stavu, pro kterou je poskytnuta přiměřená lhůta. Další odklad splnění povinnosti, která už měla být dávno splněna (v opačné případě by k vydání nápravného opatření vůbec nemohlo dojít), proto není žádoucí. Právo bránit se proti prvostupňovému rozhodnutí NÚKIB rozkladem zůstává zachováno (pro případ, že by např.

			lhůta pro splnění nápravného opatření byla stanovena nepřiměřeně okolnostem), nicméně zákon zde vyloučením odkladného účinku podaného rozkladu upřednostňuje veřejný zájem na rychlém zhojení nezákonného stavu. S vypořádáním této připomínky nesouhlasíme. Trváme na původně uplatněné připomínce. Vypořádání nadto považujeme za vnitřně rozporné, když na jednu stranu uvádí, že nápravné opatření ukládáno ve správních řízeních vedených podle zákona č. 500/2004 Sb., povinná osoba tedy bude moci v pozici účastníka řízení využít všech obraných prostředků, které ji správní řád poskytuje, a na druhou stranu omezuje reálně právo účastníka se nápravnému opatření včas a efektivně bránit – obrana ve chvíli, kdy již případná škoda zapříčiněná nezákonným rozhodnutím vznikla, je z podstaty věci neefektivní. Úvaha o zvláštní povaze nápravného opatření jako prostředku k odstranění nezákonného stavu je navíc značně nepřiléhavá, neboť totéž v právním řádu platí pro velkou část prvostupňových rozhodnutí, u nichž rozklad probíhá v běžném režimu. Pokud by navíc bylo mezi Úřadem a účastníkem řízení nesporné, v čem pochybení spočívá a jak jej napravit, nemělo by smysl o rozkladu vůbec uvažovat – rozklad zde má naopak účastníka chránit před situacemi, kdy je povaha problému a způsob jeho nápravy Úřadem vyhodnocena nesprávně a nezákonně. Závěr Připomínka je vypořádána.
443. Český telekomunikační klastr	Z	K § 58, odst. 15, písm. a) zákona	Neakceptováno - nyní § 60

		Návrh textových změn: „a) 250 000 000 Kč nebo do výše 2 % čistého celosvětového ročního obratu dosaženého právníkem osobou nebo, pokud je obviněný součástí konsolidačního celku, dosaženého konsolidačním celkem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 1 písm. a), písm. ~~d)~~ g) až k) a písm. m) až p), odstavce 3 písm. a), ~~e)~~ a f), odstavce 6 písm. b) a odstavce 8 písm. a) a b).“ Odůvodnění: Navrhujeme vypuštění skutků potenciálně spočívajících v pouhých chybách v identifikaci primárních aktiv z dosahu takto vysoké sankce a případnou úpravu sankce výrazně nižší. I s ohledem na navrhovanou presumpci společenské škodlivosti, která znemožňuje filtraci excesů ve správním trestání dle tohoto zákona považujeme výši sankce za pouhý ohrožovací delikt, který může být způsoben i neúmyslně, za nepřiměřenou.	Povinnost identifikace aktiv je základní povinností pro aplikaci dalších požadavků v rámci řízení bezpečnosti informací. Tato povinnost rovněž vyplývá z článku 21 odst. 2 směrnice NIS 2. Z tohoto důvodu je za porušení povinnosti identifikovat aktiva v rámci systému řízení bezpečnosti informací stanovena možnost uložit pokutu v maximální výši. Zároveň je potřeba dodat, že vyvratitelná právní domněnka o společenské škodlivosti přestupků byla z návrhu zákona vypuštěna. S vypořádáním této připomínky nesouhlasíme. Důvody pro navrhovanou změnu textu uvedené v odůvodnění naší připomínky trvají. Závěr Připomínka je vypořádána.
444. Český telekomunikační klastr	Z	K § 59, odst. 2 zákona Návrh textových změn: ~~„Má se za to, že čin, který vykazuje formální znaky přestupku podle tohoto zákona, je společensky škodlivý.“~~ Odůvodnění: Materiálně-formální pojetí přestupků je projevem ústavní zásady, že stanovuje-li zákon meze základních práv a svobod, musí vždy dbát jejich podstaty a smyslu – v právní úpravě přestupků pak tento ústavní regulativ nachází odraz v zásadě správního trestání jako ultima ratio. Plošné zavedení presumpce společenské škodlivosti pro všechny přestupky v zákoně uvedené – včetně přestupků z podstaty nedbalostních, k jejichž spáchání může dojít v důsledku omluvitelného omylu či přehlédnutí – uvedené zásady narušuje. Navrhujeme proto úplné vypuštění dotčeného ustanovení, nebo jeho	Akceptováno - nyní § 61 Ustanovení bylo z návrhu zákona vypuštěno. Připomínkové místo s vypořádáním souhlasí.

		výrazné omezení jen na některé skutkové podstaty přestupků uvedených v zákoně. Zavedení daného ustanovení v předkládaném návrhu zákona o kybernetické bezpečnosti je kvalitativně odlišné od podobného institutu v zákoně o zadávání veřejných zakázek, neboť dopadá na mnohem širší rozsah potenciálních subjektů v typově odlišných situacích – je značný rozdíl mezi subjekty, které se aktivně zapojují do procesů souvisejících s veřejnou zakázkou, a lze tak po nich požadovat jistou zvýšenou míru obezřetnosti, a zákonem o kybernetické bezpečnosti nově označenými subjekty, jichž budou nepochybně vyšší tisíce, na něž povinnosti dle tohoto zákona mají dopadat bez jejich vlastního přičinění a navíc, nad rámec jejich běžné činnosti, jen pro jejich příslušnost do některé z širokých kategorií vyplývajících ze zákona. Uvedené porušení zásad je obzvláště flagrantní za situace, kdy zákon vylučuje užití některých mitigačních ustanovení zákona o přestupcích, které umožňují v odůvodněných případech neukládat tresty za bagatelní přestupky. Takový postup lze považovat za neústavní.	
445. Český telekomunikační klastr	Z	K § 59, odst. 3 zákona Návrh textových změn: „(3) Na postup Úřadu podle tohoto zákona se ustanovení ~~§ 43~~, § 68 písm. b), § 70, § 71, § 80 odst. 3, § 88 odst. 2, § 89, ~~§ 90 odst. 3~~, § 95 odst. 3 a § 96 odst. 1 písm. b) zákona o odpovědnosti za přestupky a řízení o nich) nepoužijí.“ Odůvodnění: Vypuštění ustanovení o upuštění od uložení správního trestu při více přestupcích a zákazu reformationis in peius v případě příkazu není v daných podmínkách odůvodněné. Mitigační ustanovení § 43 ZoOP je významným prostředkem zmírňování nepřiměřené tvrdosti práva a jeho odstranění budí dojem snahy zákon o kybernetické bezpečnosti do pozice jakéhosi super-zákona, který je ostatní zákonné úpravě nadřazen a nemusí respektovat zásady její tvorby. Příkaz je pak	Neakceptováno - nyní § 61 Úprava vypuštění ustanovení o zákazu reformationis in peius v případě příkazu vychází z obdobné úpravy v rámci „velkého“ trestního práva. Zásada zákazu reformationis in peius neplatí v trestním řízení při zrušení trestního příkazu, přičemž tato úprava nikdy nebyla judikována jako neústavní. Zásada zákazu reformationis in peius v případě příkazu není součástí práva na spravedlivý proces a je tudíž v dispozici zákonodárce, zda ji s ohledem k regulované oblasti zavede. V oblasti kybernetické bezpečnosti se nejeví vhodné, aby nebylo po zrušení příkazu možné reflektovat případné nové skutečnosti v uložení vyšší pokuty, a to například za situace, kdy je primárním

		mimořádný prostředek správního řízení, v němž je zásadně prolomena zásada audiatur et altera pars a je vydán správní akt zasahující do právní sféry obviněného z přestupku bez toho, aby se k němu takový obviněný mohl jakkoliv vyjádřit či se proti němu bránit. Za dané situace nesmí být obviněný z přestupku nikterak odrazován či zastrašován od požadavku na řádné projednání dotčeného skutku, zejména ne hrozbou možného zvýšení trestu. I takový postup lze považovat za neústavní.	cílem ukládané pokuty donutit obviněného ke splnění porušované povinnosti. Ustanovení § 90 odst. 3 zákona o odpovědnosti za přestupky přitom výslovně neumožňuje uložit vyšší výměru správního trestu, tj. i vyšší pokutu, pokud byl proti příkazu podán odpor. Zásada zákazu reformationis in peius v případě odvolání podle § 90 odst. 3 správního řádu zůstává zachována. Obviněný tak není nikterak odrazován od podání řádného opravného prostředku. Formulace v důvodově zprávě týkající se rozšíření předmětu přestupkového řízení o nové skutky v případě podaného odporu bude upravena. Využití institutu upuštění od uložení správního trestu se s ohledem na specifickou povahu a charakter regulovaných subjektů a závažnost upravovaných přestupků nejeví vhodné. V mimořádných případech přestupků s minimální škodlivostí jsou zachovány možnosti uložit napomenutí či pokutu v symbolické výši. S vypořádáním této připomínky nesouhlasíme. Důvody pro navrhovanou změnu textu uvedené v odůvodnění naší připomínky trvají. Závěr Připomínka je vypořádána.
446. Český telekomunikační klastr	Z	K § 62, odst. 1 zákona Návrh textových změn: „Úřad může uložit pořádkovou pokutu až do výše 100 000 Kč. Pořádkovou pokutu lze uložit i opakovaně. Celková výše opakovaně ukládaných pokut nesmí přesáhnout 10 000 000 Kč nebo 1 % z čistého	Neakceptováno - nyní § 64 Ukládání sankcí se nad rámec speciální úpravy obsažené v návrhu zákona řídí obecně platnými základními zásadami správního trestání, tedy mj. i zásadou rovného přístupu a nediskriminace. Pokuta (a

		obratu dosaženého právníčkou nebo podnikající fyzickou osobou za poslední ukončené účetní období podle toho, která z daných částek je nižší vyšší.“ Odůvodnění: Navrhujeme zmírnění sazeb pokut, které s ohledem na jinak velmi vysoké pokuty v případě v zákoně vyjmenovaných přestupků za konkrétní skutkové podstaty, lze označit vzhledem k jejich zbytkovému zaměření za nepřiměřené,	je lhostejno, zda jde o pokutu za přestupek, nebo např. donucovací pokutu podle správního řádu) musí být stanovena tak, aby byla zejm. přiměřená, nediskriminační, odpovídající pochybení a přístupu orgánu, který ji ukládá, k trestání obdobných prohřešků u jiných osob, a nelikvidační pro osobu, které je ukládána (jde jen o příkladný výčet pravidel, kterými jsou správní orgány, tedy nejen NÚKIB, při ukládání pokut vázány, a které vycházejí primárně z judikatury správních soudů). Donucovací pokuta podle § 129 správního řádu není trestem ve smyslu trestání nesplnění povinnosti stanovené návrhem zákona, ale donucovacím prostředkem používaným pouze v rámci exekuce správního rozhodnutí. Ustanovení § 64 odst. 2 návrhu zákona nestanoví specifické podmínky pro ukládání donucovacích pokut, naopak se v tomto případě bude Úřad řídit obecnou úpravou obsaženou ve správním řádu. Návrh zákona však speciálně upravuje výši donucovací pokuty, kterou lze v rámci exekuce rozhodnutí Úřadu uložit. Důvodem (uvedeným v důvodové zprávě k návrhu) je zjevná zastaralost částek stanovených správním řádem a jejich naprostá disproporčnost ve vztahu k pokutám, kterým subjekty čelí za porušení povinností stanovených návrhem zákona. Upravená výše donucovací pokuty tak reflektuje maxima pokut, které je možné uložit za neplnění povinností podle návrhu zákona, a má za cíl skutečně motivovat pokutované subjekty ke splnění povinnosti, která jim byla rozhodnutím uložena, což částky stanovené správním řádem postrádají. Výsledná výše pak bude vždy odrážet základní zásady správního trestání uvedené výše. S vypořádáním této připomínky nesouhlasíme.

			Důvody pro navrhovanou změnu textu uvedené v odůvodnění naší připomínky trvají. Nebráníme se zvláštní úpravě výše pořádkových pokut v předloženém návrhu zákona odlišné od úpravy správního řádu, namítáme však, že zvolená výše je pro typické adresáty právní úpravy, kterými jsou například i regionální poskytovatelé připojení k internetu, nepřiměřeně vysoká. Přiměřenost výše pokut k velikosti či ekonomické situaci modelových typických adresátů právní úpravy není uspokojivě zdůvodněna. Závěr Připomínka je vypořádána.
447. Český telekomunikační klastr	Z	K § 62, odst. 2 zákona Návrh textových změn: „Úřad může za účelem vymáhání splnění povinnosti uložené rozhodnutím Úřadu ukládat donucovací pokuty až do výše 10 000 000 Kč nebo 1 % z čistého obrátu dosaženého právnickou nebo podnikající fyzickou osobou za poslední ukončené účetní období podle toho, která z daných částek je nižší vyšší.“ Odůvodnění: Navrhujeme zmírnění sazeb pokut, které s ohledem na jinak velmi vysoké pokuty v případě v zákoně vyjmenovaných přestupků za konkrétní skutkové podstaty, lze označit vzhledem k jejich zbytkovému zaměření za nepřiměřené.	Neakceptováno - nyní § 64 Ukládání sankcí se nad rámec speciální úpravy obsažené v návrhu zákona řídí obecně platnými základními zásadami správního trestání, tedy mj. i zásadou rovného přístupu a nediskriminace. Pokuta (a je lhostejno, zda jde o pokutu za přestupek, nebo např. donucovací pokutu podle správního řádu) musí být stanovena tak, aby byla zejm. přiměřená, nediskriminační, odpovídající pochybení a přístupu orgánu, který ji ukládá, k trestání obdobných prohřešků u jiných osob, a nelikvidační pro osobu, které je ukládána (jde jen o příkladný výčet pravidel, kterými jsou správní orgány, tedy nejen NÚKIB, při ukládání pokut vázány a které vycházejí primárně z judikatury správních soudů). Donucovací pokuta podle § 129 správního řádu není trestem ve smyslu trestání nesplnění povinnosti stanovené návrhem zákona, ale donucovacím prostředkem používaným pouze v rámci exekuce

		správního rozhodnutí. Ustanovení § 62 odst. 2 návrhu zákona nestanoví specifické podmínky pro ukládání donucovacích pokut, naopak se v tomto případě bude Úřad řídit obecnou úpravou obsaženou ve správním řádu. Návrh zákona však speciálně upravuje výši donucovací pokuty, kterou lze v rámci exekuce rozhodnutí Úřadu uložit. Důvodem (uvedeným v důvodové zprávě k návrhu) je zjevná zastaralost částek stanovených správním řádem a jejich naprostá disproporčnost ve vztahu k pokutám, kterým subjekty čelí za porušení povinností stanovených návrhem zákona. Upravená výše donucovací pokuty tak reflektuje maxima pokut, které je možné uložit za neplnění povinností podle návrhu zákona, a má za cíl skutečně motivovat pokutované subjekty ke splnění povinností, která jim byla rozhodnutím uložena, což částky stanovené správním řádem postrádají. Výsledná výše pak bude vždy odrážet základní zásady správního trestání uvedené výše. S vypořádáním této připomínky nesouhlasíme. Důvody pro navrhovanou změnu textu uvedené v odůvodnění naší připomínky trvají. Nebráníme se zvláštní úpravě výše donucovacích pokut v předloženém návrhu zákona odlišné od úpravy správního řádu, namítáme však, že zvolená výše je pro typické adresáty právní úpravy, kterými jsou například i regionální poskytovatelé připojení k internetu, nepřiměřeně vysoká. Přiměřenost výše pokut k velikosti či ekonomické situaci modelových typických adresátů právní úpravy není uspokojivě zdůvodněna. Závěr

			Připomínka je vypořádána.
448. Český telekomunikační klastr	Z	K § 62, odst. 3 zákona Návrh textových změn: „Za přestupek, kterého se poskytovatel regulované služby dopustí tím, že jako kontrolovaná osoba nesplní některou z povinností podle kontrolního řádu, lze uložit pokutu do 10 000 000 Kč.“ Odůvodnění: Navrhujeme zmírnění sazeb pokut, které s ohledem na jinak velmi vysoké pokuty v případě v zákoně vyjmenovaných přestupků za konkrétní skutkové podstaty, lze označit vzhledem k jejich zbytkovému zaměření za nepřiměřené,	Neakceptováno - nyní § 64 Zde lze plně odkázat na odůvodnění obsažené v důvodové zprávě k návrhu zákona: Odstavec 3 stanoví maximální výši pokuty za přestupek proti kontrole podle kontrolního řádu na 10 000 000 Kč. Jde o zlomek maximální výše pokuty za nejzávažnější přestupky proti zákonu, kterým se regulovaný orgán nebo osoba neposkytnutím součinnosti podle kontrolního řádu může vyhnout. Nejde tedy o žádnou zbytkovou kategorii, ale o přestupky, kterými se kontrolovaná osoba může vyhýbat odpovědnosti za splnění stěžejních povinností obsažených v návrhu zákona. Zároveň jde o částku, která by i pro ekonomicky silné orgány a osoby měla být motivační. Cílem sankčních ustanovení kontrolního řádu je přinutit kontrolovaný subjekt ke spolupráci při kontrole, odmítá-li ji dobrovolně. Aktuální výše sazeb obsažených v kontrolním řádu je pro účely návrhu zákona nedostatečná, neboť vůbec nereflektuje závažnost pochybení a maximální výši pokut, kterým se lze neposkytnutím součinnosti podle kontrolního řádu vyhnout. S vypořádáním této připomínky nesouhlasíme. Důvody pro navrhovanou změnu textu uvedené v odůvodnění naší připomínky trvají. Textace daného ustanovení umožňuje ukládat pokuty ve zjevně nepřiměřené výši i za nesplnění drobných procesních povinností dle kontrolního řádu, které jsou navíc v zákoně vymezeny jen velice obecně – viz např. § 10 odst. 2 kontrolního řádu.

			Nebráníme se zvláštní úpravě výše pokut za nesplnění povinností dle kontrolního řádu v předloženém návrhu zákon, namítáme však, že zvolená výše je pro typické adresáty právní úpravy, kterými jsou například i regionální poskytovatelé připojení k internetu, nepřiměřeně vysoká. Přiměřenost výše pokut k velikosti či ekonomické situaci modelových typických adresátů právní úpravy není uspokojivě zdůvodněna. Závěr Připomínka je vypořádána.
449. Český telekomunikační klastr	Z	K § 65, odst. 1 zákona Návrh textových změn: „Na postupy Úřadu podle ~~§ 8, § 9, § 10 a~~ § 11 odst. 1 a 3 se ustanovení správního řádu upravující vedení správního řízení nepoužijí.“ Odůvodnění: Registrace poskytovatele regulované služby a stanovení jeho režimu povinností jsou klíčové momenty, od nichž se odvíjí široká obálka povinností adresátů právní úpravy, včetně možností ukládání drastických správních sankcí. Jedná se o prakticky nejzávažnější změnu právního statusu dotčeného subjektu ve vztahu k zákonu o kybernetické bezpečnosti, která je v tomto zákoně upravena. Jelikož zákon umožňuje provádění a změny registrace i z vlastní iniciativy Úřadu bez toho, aby k takové změně dal podnět dotčený subjekt, je absolutně nezbytné respektovat instituty správního práva upravující zásahy do práv osob, jejich limity a zejména jejich přezkum. Zákon sám plnohodnotný procesní aparát zajišťující zároveň možnost procesní obrany a přezkumu rozhodnutí neobsahuje, není tedy důvodné ani vhodné vylučovat úpravu obsaženou ve správním řádu. Předkládaný návrh z výše uvedeného důvodu může zasahovat do práv adresátů regulace na spravedlivý proces vyplývajících z Listiny základních práv a svobod.	Neakceptováno Ust. § 65 bylo z návrhu vypuštěno. K problematice lze uvést, že Úřad je při své činnosti standardně vázán ustanoveními správního řádu, některá specifická jednání však vyžadují úpravu obecných pravidel. Jde zejména o úkony jako je registrace regulované služby, změna registrace a zápis do evidence regulovaných služeb, u nichž je dán zájem na rychlém a efektivním vyřízení bez zbytečného prodlení. Zjednodušení procesu je dáno veřejným zájmem na zvýšení úrovně kybernetické bezpečnosti subjektů provozujících služby, jež stát definoval jako nezbytné pro zabezpečení důležitých společenských nebo ekonomických činností, kdy narušení jejich poskytování může vést až k významnému omezení chodu státu. Ve veřejném zájmu je tak provedení zařazení subjektu do regulace co nejvíce v souladu se zásadou rychlosti a hospodárnosti, neboť neúměrným a nijak účelným prodlužováním celého procesu může být výše zmíněný zájem představující účel tohoto zákona ohrožen. Do doby registrace a zápisu do evidence regulovaných služeb tyto subjekty nejsou

			odpovědné za zabezpečování svých systémů a hlášení incidentů. S vypořádáním této připomínky nesouhlasíme. Ačkoliv byl napadaný text § 65 odst. 1 z návrhu odstraněn, totéž pravidlo je nyní obsaženo v § 8, odst. 5, § 9 odst. 3 a § 10 odst. 3 návrhu. Úřad ve svém vypořádání odhlíží od skutečnosti, že sice na jedné straně vylučuje užití procesních ustanovení správního řádu, nenahrazuje je však jinými procesními ustanoveními, nýbrž na jejich místě ponechává právní vakuum. Dochází tak ke dvojímu narušení právního postavení účastníka řízení, kdy jednak nemá možnost seznámit se s pravidly průběhu řízení dle daných ustanovení a v druhé řadě (zřejmě) nemůže využívat ochranných procesních ustanovení a institutů ve správním řádě upravených. Pokud má Úřad za to, že je vhodné vyloučit užití ustanovení správního řádu o vedení řízení, nechť se inspirovat například daňovým řádem, který taktéž užití správního řádu vylučuje, na jeho místě však upravuje vlastní procesní aparát. Závěr Připomínka je vypořádána.
450. Český telekomunikační klastr	Z	K § 65, odst. 3 zákona Návrh textových změn: „Proti rozhodnutí o ~~určení regulované služby podle § 5 a rozhodnutí o~~ výmazu z evidence poskytovatelů regulovaných služeb podle § 11 odst. 2 není rozklad přípustný.“ Odůvodnění:	Neakceptováno Ust. § 65 bylo z návrhu vypuštěno. K problematice lze uvést, že důvody pro vyloučení možnosti podat rozklad proti rozhodnutí o určení podle § 5 návrhu zákona jsou vedeny veřejným zájmem na rychlém a efektivním zařazení poskytovatele regulované služby do regulace. Jde o obdobnou situaci jako při určování

		Registrace poskytovatele regulované služby a stanovení jeho režimu povinností jsou klíčové momenty, od nichž se odvíjí široká obálka povinností adresátů právní úpravy, včetně možností ukládání drastických správních sankcí. Jedná se o prakticky nejzávažnější změnu právního statusu dotčeného subjektu ve vztahu k zákonu o kybernetické bezpečnosti, která je v tomto zákoně upravena. Jelikož zákon umožňuje provádění a změny registrace i z vlastní iniciativy Úřadu bez toho, aby k takové změně dal podnět dotčený subjekt, je absolutně nezbytné respektovat instituty správního práva upravující zásahy do práv osob, jejich limity a zejména jejich přezkum. Předkládaný návrh z výše uvedeného důvodu může zasahovat do práv adresátů regulace na spravedlivý proces vyplývajících z Listiny základních práv a svobod.	provozovatelů základní služby podle současného zákona o kybernetické bezpečnosti, u něhož je také vyloučena možnost podat rozklad. Za dobu účinnosti současného zákona a určování provozovatelů základní služby se přitom nestalo, že by subjekt se svým určením nesouhlasil a podal proti rozhodnutí Úřadu žalobu. Vzhledem k zájmům, jejichž ochrana byla určováním provozovatelů základních služeb sledována (zejména národní bezpečnosti a ochrana obyvatelstva), bylo nutné, aby proces určování podle zákona o kybernetické bezpečnosti probíhal, pokud možno, bez výraznějšího zpoždění. Tyto důvody lze v plném rozsahu aplikovat i na určování subjektů podle § 5 návrhu zákona, a to tím spíše, že kritéria § 5 zákona míří na strategické a vysoce důležité subjekty (u nichž by narušením bezpečnosti jejich informačních systémů mohlo dojít k významnému ohrožení veřejné bezpečnosti, zdraví osob nebo majetku nebo jiných chráněných zájmů státu). Ve veřejném zájmu je tak provedení zařazení orgánu nebo osoby do regulace co nejvíce v souladu se zásadou rychlosti a hospodárnosti, neboť neúměrným a nijak účelným prodlužováním celého procesu může být výše zmíněný zájem představující účel tohoto návrhu zákona ohrožen. Do doby registrace a zápisu do evidence regulovaných služeb tyto orgány nebo osoby nejsou odpovědné za zabezpečování svých systémů a hlášení incidentů. Jakékoli prodlužování procesu zařazení orgánů nebo osob do regulace návrhu zákona oddaluje okamžik, od kterého jsou tyto orgány a osoby odpovědné za zajišťování kybernetické bezpečnosti své organizace a ochranu poskytované služby.

			Určení subjektu podle § 5 probíhá ve standardním správním řízení podle zákona č. 500/2004 Sb., přičemž v rámci správního řízení je jednak subjektu dána možnost se vyjadřovat k podkladům rozhodnutí a namítat nejruznější skutečnosti zpochybňující závěry Úřadu, jednak je Úřadu dána povinnost se všemi argumenty subjektu a důvody pro jeho určení vypořádat v rámci odůvodnění rozhodnutí. Stejně tak není vyloučena možnost podat proti rozhodnutí Úřadu správní žalobu. Možnosti obrany jsou tedy i přes zvýšený zájem státu na rychlém a efektivním rozhodování zachovány. S vypořádáním této připomínky nesouhlasíme. Důvody pro navrhovanou změnu textu uvedené v odůvodnění naší připomínky trvají. Závěr Připomínka je vypořádána.
451. Český telekomunikační klastr	Z	K § bodu 16.1 Přílohy k návrhu tezí vyhlášky o regulovaných službách Návrh textových změn: „Podnikatel poskytující veřejně dostupnou službu elektronických komunikací podle zákona o elektronických komunikacích je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, b) je středním podnikem, c) je poskytovatelem veřejně dostupné služby elektronických komunikací skrze nejméně 350 000 aktivních mobilních SIM karet na maloobchodním trhu na území České republiky, nebo d) je poskytovatelem nejméně ~~100 000~~ 350 000 aktivních pevných internetových přípojek na území České republiky,“	Neakceptováno Teze prováděcích právních předpisů jsou sice již teď součástí předkládaného materiálu, ale budou následně předmětem samostatného připomínkového řízení při procesu jejich vydávání. Nelze předpokládat, že jedna pevná přípojka (typicky jedna domácnost) odpovídá jedné osobě (tj. jedné SIM kartě), z pohledu účelu právní úpravy tedy není vhodné uvedená kritéria sjednocovat. Pokud jde o konkrétní počty SIM karet a pevných přípojek, uvedený minimální počet aktivních přípojek byl stanoven tak, aby pokryl subjekty poskytující společně podle posledních dostupných dat Českého telekomunikačního úřadu (za rok 2021) většinu všech aktivních přípojek (cca 60 %). Minimální počet SIM karet pokrývá subjekty, které

	Odůvodnění: Česká republika je charakteristická velmi vysokým počtem poskytovatelů přístupu k internetu v pevném místě. Tato skutečnost vede k pozitivním jevům v oblastech hospodářské soutěže a různorodosti použitých řešení. Subjekty působící na trhu přístupu k internetu v pevném místě jsou ale vlivem silného konkurenčního boje a – z podstaty věci – jejich omezené hospodářské síly více zranitelné vlivy nadměrné regulatorní zátěže. Stanovení hranice 100.000 přípojek v pevném místě jako kritéria pro identifikaci poskytovatele strategicky významné služby je z tohoto důvodu nevhodné, neboť bez zjevného důvodu vystaví i nižší kategorii (co do rozsahu) poskytovatelů dramatickému nárůstu jejich regulatorních povinností – a to i v případě, že záležitosti související s bezpečností svých sítí spravují odpovědně. Umístění dané hranice v předkládaném návrhu je navíc drasticky nesystémové s ohledem na skutečnost, že na trhu mobilním, který je dominován velkými nadnárodními poskytovateli, je hranice nastavena na 3,5 násobek.	společně poskytují veřejně dostupné služby elektronických komunikací uživatelům většiny všech aktivních mobilních SIM karet na maloobchodním trhu (cca 92 %). V případě SIM karet je současně zohledněna skutečnost, že uvedené výrazně nadpoloviční většině poskytují veřejně dostupné služby elektronických komunikací pouze tři subjekty. S vypořádáním této připomínky nesouhlasíme. Na obsahu původně uplatněné připomínky trváme. Má-li být dle obsahu vypořádání text této vyhlášky ještě dopracováván, považujeme to jen za další důvod pro to, aby předmětná klíčová materie byla upravena přímo zákonem. Vymezení klíčových kategorií, jako je zejména okruh adresátů hlavních okruhů povinností dle předkládaného návrhu zákona je zásadním aspektem, bez jehož posouzení v rámci legislativního procesu nelze předložený návrh zákona reálně zhodnotit. Právní jistota o stabilitě regulatorního prostředí v těchto klíčových aspektech pak musí trvat i později za účinnosti zákona. Úřad při stanovení hranice kategorie poskytovatele regulované služby v režimu vyšších povinností nezohlednil počet a obvyklou velikost subjektů poskytujících služby připojení v pevném místě ve srovnání s obvyklou velikostí subjektů působících na mobilním trhu. S ohledem na značnou fragmentovanost trhu fixního připojení k internetu by pro obvyklého poskytovatele fixních služeb přístupu k internetu byl režim poskytovatele regulované služby v režimu vyšších povinností nepřiměřeně zatěžující. Závěr Připomínka je vypořádána.

452. Český telekomunikační klastr	Z	K § bodu 16.2 Přílohy k návrhu tezí vyhlášky o regulovaných službách Návrh textových změn: „Podnikatel zajišťující veřejnou komunikační síť podle zákona o elektronických komunikacích je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, b) je středním podnikem, c) je poskytovatelem veřejně dostupné služby elektronických komunikací skrze nejméně 350 000 aktivních mobilních SIM karet na maloobchodním trhu na území České republiky, nebo d) je poskytovatelem nejméně ~~100 000~~ 350 000 aktivních pevných internetových přípojek na území České republiky,“ Odůvodnění: Česká republika je charakteristická velmi vysokým počtem poskytovatelů přístupu k internetu v pevném místě. Tato skutečnost vede k pozitivním jevům v oblastech hospodářské soutěže a různorodosti použitých řešení. Subjekty působící na trhu přístupu k internetu v pevném místě jsou ale vlivem silného konkurenčního boje a – z podstaty věci – jejich omezené hospodářské síly více zranitelné vlivy nadměrné regulatorní zátěže. Stanovení hranice 100.000 přípojek v pevném místě jako kritéria pro identifikaci poskytovatele strategicky významné služby je z tohoto důvodu nevhodné, neboť bez zjevného důvodu vystaví i nižší kategorii (co do rozsahu) poskytovatelů dramatickému nárůstu jejich regulatorních povinností – a to i v případě, že záležitosti související s bezpečností svých sítí spravují odpovědně. Umístění dané hranice v předkládaném návrhu je navíc drasticky nesystémové s ohledem na skutečnost, že na trhu mobilním, který je dominován velkými nadnárodními poskytovateli, je hranice nastavena na 3,5 násobek.	Neakceptováno Teze prováděcích právních předpisů jsou sice již teď součástí předkládaného materiálu, ale budou následně předmětem samostatného připomínkového řízení při procesu jejich vydávání. Nelze předpokládat, že jedna pevná přípojka (typicky jedna domácnost) odpovídá jedné osobě (tj. jedné SIM kartě), z pohledu účelu právní úpravy tedy není vhodné uvedená kritéria sjednocovat. Pokud jde o konkrétní počty SIM karet a pevných přípojek, uvedený minimální počet aktivních přípojek byl stanoven tak, aby pokryl subjekty poskytující společně podle posledních dostupných dat Českého telekomunikačního úřadu (za rok 2021) většinu všech aktivních přípojek (cca 60 %). Minimální počet SIM karet pokrývá subjekty, které společně poskytují veřejně dostupné služby elektronických komunikací uživatelům většiny všech aktivních mobilních SIM karet na maloobchodním trhu (cca 92 %). V případě SIM karet je současně zohledněna skutečnost, že uvedené výrazně nadpoloviční většině poskytují veřejně dostupné služby elektronických komunikací pouze tři subjekty. S vypořádáním této připomínky nesouhlasíme. Na obsahu původně uplatněné připomínky trváme. Má-li být dle obsahu vypořádání text této vyhlášky ještě dopracováván, považujeme to jen za další důvod pro to, aby předmětná klíčová materie byla upravena přímo zákonem. Vymezení klíčových kategorií, jako je zejména okruh adresátů hlavních okruhů povinností dle předkládaného návrhu zákona je zásadním aspektem, bez jehož posouzení v rámci legislativního procesu nelze předložený návrh zákona reálně zhodnotit. Právní jistota o stabilitě regulatorního

			prostředí v těchto klíčových aspektech pak musí trvat i později za účinnosti zákona. Úřad při stanovení hranice kategorie poskytovatele regulované služby v režimu vyšších povinností nezohlednil počet a obvyklou velikost subjektů poskytujících služby připojení v pevném místě ve srovnání s obvyklou velikostí subjektů působících na mobilním trhu. Pro obvyklého poskytovatele fixních služeb přístupu k internetu by režim poskytovatele regulované služby v režimu vyšších povinností byl nepřiměřeně zatěžující. Závěr Připomínka je vypořádána.
453. Český telekomunikační klastr	Z	K § 10, odst. 1, písm. b) návrhu tezí vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Návrh textových změn: „Povinná osoba seznamuje své dodavatele s pravidly podle písmena a) ~~a vyžaduje plnění těchto pravidel,~~“ Odůvodnění: Navrhovaná úprava stanovuje svým adresátům povinnost vynucovat určitý obsah smlouvy vůči třetím osobám, s nimiž vstupuje do obchodního styku. Z podstaty věci jsou tyto třetí osoby zahraničními subjekty s často mezinárodním dosahem. Typický adresát úpravy – například poskytovatel služeb elektronických komunikací v pevném místě v České republice – přitom jako zpravidla regionální subjekt menšího rozsahu nemá vyjednávací pozici, která by mu umožňovala vynucovat si libovolné smluvní podmínky vůči jeho dodavatelům. Navrhovaná úprava pro typické adresáty prakticky nesplnitelná. Přijetí navrhované úpravy by mělo potenciálně katastrofické důsledky	Vysvětleno Samotné vyhlášky nyní nejsou předmětem připomínkové řízení, tím je v současné chvíli jenom zákon. Samotné vyhlášky jsou stále rozpracovány a probíhají v nich dílčí úpravy. Povinnost zohledňovat požadavky plynoucí ze zákona při řízení dodavatele, tedy při jeho výběru a uzavření smlouvy, platí vždy. Pokud má již subjekt něco zaslavně a začnou mu ze zákona plynout nové povinnosti, měl by své smlouvy revidovat. Následně může uzavřít dodatek, případně původní smlouvu vypovědět a vybrat si dodavatele nového. Obdobně by měl subjekt postupovat ať už se jedná o kybernetickou bezpečnost nebo o jakékoli jiné povinnosti, které mu ukládají zákony. Z tohoto důvodu rovněž existuje lhůta, ve které se mohou povinné subjekty na změny po účinnosti zákona připravit. Stav, ve kterém by subjekty měly uzavřeny smlouvy nesplňující požadavky plynoucí z bezpečnostních opatření, je

		pro tyto poskytovatele připojení, neboť by hrozilo znepřístupněním prakticky všech dodavatelských vektorů více než 1500 ISP působícím v České republice a omezením hospodářské soutěže na tomto trhu jen na velké nadnárodní společnosti.	jednoznačně nežádoucí. Povinnost řídit dodavatele je dána zákonem a jedná se o požadavky směrnice NIS1 a NIS2. Pokud si je povinná osoba schopna uvědomit, jakým způsobem se pracuje s jednotlivými bezpečnostními opatřeními zaváděnými na základě hodnocení rizik u aktiv relevantních pro určený rozsah systému řízení kybernetické bezpečnosti, není toto ustanovení ultimativní, a na něj navazující příloha obsahuje výčet možných relevantních ustanovení do dodavatelských smluv – jejichž obsah a jasné vymezení vzájemných práv a povinností, předchází možným nedorozuměním, které mohou mít zásadní vliv na bezpečné poskytování regulované služby. Každá povinná osoba přihlédne ke svým potřebám/možnostem/specifikám, stejně tak k tomu, na jaké dodavatele budou pravidla dopadat a co od dodavatele nakupují (co je předmětem smlouvy). V případě, že něco povinná osoba není schopna dát do smlouvy s dodavatelem, je nutné tento postup odůvodnit v PoA a průběžně tento stav vyhodnocovat a monitorovat, v PoA by mělo být řádně zdůvodněno, proč není bezpečnostní opatření aplikovatelné a kdy se předpokládá jeho provedení, tak aby se nejednalo o inherentní riziko v případě že může být ošetřeno realizovatelným opatřením. S vypořádáním této připomínky nesouhlasíme. Na obsahu původně uplatněné připomínky trváme. Má-li navíc být dle obsahu vypořádání text této vyhlášky ještě dopracováván, považujeme to jen za další důvod pro to, aby předmětná materie byla upravena přímo zákonem.

			Úřad opomíná zohlednit počet a obvyklou velikost typických adresátů dané právní úpravy, kteří jsou často regionálními poskytovateli připojení k internetu, a jako takoví často nemají vyjednávací sílu dosáhnout změn smluv uzavíraných s jejich dodavateli, kteří jsou mnohdy velkými nadnárodními korporacemi. Odstřížení těchto ISP od možnosti odebírat dodávky zboží a služeb od takových zahraničních společností jen proto, že se jim nepodaří do smlouvy včlenit příslušná ustanovení či je zpravidla v zahraničním právu (!) vynucovat, by bylo závažnou hrozbou pro podnikání adresátů úpravy i pro kybernetickou bezpečnost ve státě. Závěr Připomínka je vypořádána.
454. Český telekomunikační klastr	Z	K § 10, odst. 1, písm. f) návrhu tezí vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Návrh textových změn: „Povinná osoba ~~v souvislosti s řízením rizik spojených s významnými dodavateli zajistí, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní oblasti uvedené v příloze č. 7 k této vyhlášce a“~~ Odůvodnění: Navrhovaná úprava stanovuje svým adresátům povinnost vynucovat určitý obsah smlouvy vůči třetím osobám, s nimiž vstupuje do obchodního styku. Z podstaty věci jsou tyto třetí osoby zahraničními subjekty s často mezinárodním dosahem. Typický adresát úpravy – například poskytovatel služeb elektronických komunikací v pevném místě v České republice – přitom jako zpravidla regionální subjekt menšího rozsahu nemá vyjednávací pozici, která by mu umožňovala vynucovat si libovolné smluvní podmínky vůči jeho dodavatelům.	Vysvětleno Samotné vyhlášky nyní nejsou předmětem připomínkové řízení, tím je v současné chvíli jenom zákon. Samotné vyhlášky jsou stále rozpracovány a probíhají v nich dílčí úpravy. Povinnost zohledňovat požadavky plynoucí ze zákona při řízení dodavatele, tedy při jeho výběru a uzavření smlouvy, platí vždy. Pokud má již subjekt něco zasmulvněno a začnou mu ze zákona plynout nové povinnosti, měl by své smlouvy revidovat. Následně může uzavřít dodatek, případně původní smlouvu vypovědět a vybrat si dodavatele nového. Obdobně by měl subjekt postupovat ať už se jedná o kybernetickou bezpečnost nebo o jakékoliv jiné povinnosti, které mu ukládají zákony. Z tohoto důvodu rovněž existuje lhůta, ve které se mohou povinné subjekty na změny po účinnosti zákona připravit. Stav, ve kterém by subjekty měly uzavřeny smlouvy nesplňující

		Navrhovaná úprava pro typické adresáty prakticky nesplnitelná. Přijetí navrhované úpravy by mělo potenciálně katastrofické důsledky pro tyto poskytovatele připojení, neboť by hrozilo znepřístupněním prakticky všech dodavatelských vektorů více než 1500 ISP působícím v České republice a omezením hospodářské soutěže na tomto trhu jen na velké nadnárodní společnosti.	požadavky plynoucí z bezpečnostních opatření je jednoznačně nežádoucí. Ano povinnost řídit dodavatele je dána zákonem a jedná se o požadavky směrnice NIS1 a NIS2. Pokud si je povinná osoba schopna uvědomit, jakým způsobem se pracuje s jednotlivými bezpečnostními opatřeními zaváděnými na základě hodnocení rizik u aktiv relevantních pro určený rozsah systému řízení kybernetické bezpečnosti, není toto ustanovení ultimativní a na něj navazující příloha obsahuje výčet možných relevantních ustanovení do dodavatelských smluv – jejichž obsah a jasné vymezení vzájemných práv a povinností, předchází možným nedorozuměním, které mohou mít zásadní vliv na bezpečné poskytování regulované služby. Každá povinná osoba přihlédně ke svým potřebám/možnostem/specifikám, stejně tak k tomu, na jaké dodavatele budou pravidla dopadat a co od dodavatele nakupují (co je předmětem smlouvy). V případě, že něco povinná osoba není schopna dát do smlouvy s dodavatelem, je nutné tento postup odůvodnit v PoA a průběžně tento stav vyhodnocovat a monitorovat, v PoA by mělo být řádně zdůvodněno, proč není bezpečnostní opatření aplikovatelné a kdy se předpokládá jeho provedení, tak aby se nejednalo o inherentní riziko v případě že může být ošetřeno realizovatelným opatřením. S vypořádáním této připomínky nesouhlasíme. Na obsahu původně uplatněné připomínky trváme. Má-li navíc být dle obsahu vypořádání text této vyhlášky ještě dopracováván, považujeme to jen za další důvod pro to, aby předmětná materie byla upravena přímo zákonem.

			Úřad opomíná zohlednit počet a obvyklou velikost typických adresátů dané právní úpravy, kteří jsou často regionálními poskytovateli připojení k internetu, a jako takoví často nemají vyjednávací sílu dosáhnout změn smluv uzavíraných s jejich dodavateli, kteří jsou mnohdy velkými nadnárodními korporacemi. Odstřižení těchto ISP od možnosti odebírat dodávky zboží a služeb od takových zahraničních společností jen proto, že se jim nepodaří do smlouvy včlenit příslušná ustanovení či je zpravidla v zahraničním právu (!) vynucovat, by bylo závažnou hrozbou pro podnikání adresátů úpravy i pro kybernetickou bezpečnost ve státě. Závěr Připomínka je vypořádána.
455. Ministerstvo dopravy	Z	Byť vnímáme jako velmi podstatný mechanismus prověřování bezpečnosti dodavatelského řetězce, považujeme jej za mimořádně závažný, pokud jde o hledání zodpovědné míry přijatelné rovnováhy v tom smyslu, k jakým částem strategické infrastruktury se tento mechanismus vztahuje či má vztahovat. Není sporu o tom, že jednou ze stěžejních markant ve veřejné správě je mít bezpečný dodavatelský řetězec. Stejně tak ovšem je neméně podstatné to, aby vyloučením dodavatelů, s jejichž zapojením jsou spojena rizika (o rozličné intenzitě), nastala taková situace (u konkrétního veřejného zadavatele např.) že dostupní „zbylí“ dodavatelé jsou schopni dodat buď zařízení či služby za pro zadavatele rozpočtově neúnosných ekonomických podmínek, či nejsou schopni takové zařízení či služby dodat, a to zčásti či zcela. Za takové situace by nejenže mohl být podstatně ztížen či znemožněn chod významných či kritických informačních systémů státu (registru silničních vozidel, registru řidičů apod.), zásadní narušení provozu by mohla zažít i strategická dopravní infrastruktura státu, pokud jde např. o zajištění provozu řídicích systémů celostátní a regionální dráhy, popř. telematických aplikací na dálnicích, např. systémů pro řízení dopravy, mýtného systému atd.	Neakceptováno NÚKIB v rámci zkoumání ekonomických dopadů oslovil mnoho subjektů v rámci dotazníkového šetření a využil maximální množství informací pro to, aby posoudil možné dopady v rámci návrhu zákona o kybernetické bezpečnosti, včetně mechanismu bezpečnosti dodavatelského řetězce. Zde bylo nutno operovat s danými údaji v určitém stupně obecnosti, jelikož není možno předjímat veškeré dopady navrhované úpravy. Samozřejmě však rádi uvítáme debatu na téma dopadů. Reakce připomínkového místa: Navržené vypořádání neakceptujeme a na připomínce trváme. Od pana ministra nemáme mandát z této připomínky ustoupit.

		V této souvislosti uplatňujeme zásadní připomínku v tom smyslu, že požadujeme, aby byla otázka, v jakém rozsahu a ke kterým částem strategické infrastruktury se předmětný mechanismus bude uplatňovat, podrobena před postoupením do další fáze legislativního procesu důkladnému veřejnému projednání, za účasti správců informačních systémů veřejné správy (rozhodně nejméně orgánů a právnických osob náležejících do rezortu dopravy), odborné veřejnosti, přičemž zvláštní pozornost má být při těchto konzultacích věnována otázce, jak nákladná se pro veřejný rozpočet může ukázat ta či ona varianta řešení na úrovni zákona. Bez uskutečnění této diskuse a zodpovědného zhodnocení ekonomických dopadů nemůže rezort dopravy v žádném případě souhlasit s tím, aby byl návrh předložen k projednání vládě.	Reakce NÚKIB Připomínkovému místu zaslán návrh zákona, který byl po vypořádání připomínek upraven. Závěr Připomínka byla na úrovni vedení vypořádána.
456. Ministerstvo dopravy	Z	Požadujeme do návrhu zákona zapracovat nařízení Evropského parlamentu a Rady (EU) 2023/588 ze dne 15. března 2023, kterým se zavádí Program Unie pro bezpečnou konektivitu na období 2023–2027. Dané nařízení Evropského parlamentu a Rady (EU) 2023/588 ze dne 15. března 2023 v předloženém návrhu zcela absentuje. Program Unie pro bezpečnou konektivitu (neformálně nazývaný též IRIS²) je novou součástí kosmických aktivit Evropské unie a tematicky navazuje na složku Govsatcom a také na řídicí strukturu Kosmického programu Evropské unie ve smyslu nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zavádí Kosmický program Unie a zřizuje Agentura Evropské unie pro Kosmický program a zrušují nařízení (EU) č. 912/2010, (EU) č. 1285/2013 a (EU) č. 377/2014 a rozhodnutí č. 541/2014/EU. Jedná se o ambiciózní evropský program na stavbu a provoz zabezpečené družicové telekomunikační megakonstelace a přímo souvisí s již aktuální agendou Národního úřadu pro kybernetickou a informační bezpečnost. Program Unie pro bezpečnou konektivitu se postupně stává integrální součástí aktivit výborů a pracovních skupin Komise (např.	Akceptováno Do poznámky pod čarou č. 1 byl příslušný předpis Evropské unie doplněn, dále bylo vloženo nové písmeno k), které zní „vykonává působnost ve vybraných oblastech souvisejících s informační a kybernetickou bezpečností, bezpečnostní akreditací a bezpečností systémů a zavedených služeb v rámci Programu Unie pro bezpečnou konektivitu podle nařízení Evropského parlamentu a Rady č. 2023/588, zejména plní funkce příslušného orgánu pro bezpečnou konektivitu podle čl.11 tohoto nařízení. CELEX 32023R0588. Pro úplnost byla do § 41 odst. 4 písm. f) doplněna Agentura Evropské unie pro Kosmický program. Připomínkové místo s vypořádáním souhlasí.

		Bezpečnostní konfigurace Výboru pro kosmický program Evropské unie) a agentury EUSPA včetně bezpečnostní akreditace zajišťované Výborem pro bezpečnostní akreditaci (SAB), kde Českou republiku zastupuje Národní úřad pro kybernetickou a informační bezpečnost. Domníváme se, že by se nařízení Evropského parlamentu a Rady (EU) 2023/588 ze dne 15. března 2023 mělo minimálně promítnout do - poznámky pod čarou č. 1 uvádějící výčet právních předpisů Evropské unie a - § 41 odst. 4 návrhu zákona jako nová působnost Národního úřadu pro kybernetickou a informační bezpečnost (navrhujeme například tuto podobu nového písmene „vykonává působnost v dílčích oblastech souvisejících s informační a kybernetickou bezpečností v rámci Programu Unie pro bezpečnou konektivitu podle nařízení Evropského parlamentu a Rady č. 2023/588“).	
457. Ministerstvo dopravy	Z	V § 41 odst. 4 písm. j) návrhu zákona požadujeme před slovo „bezpečností“ vložit slova „informační a kybernetickou“. Navržená podoba § 41 odst. 4 písm. j) je velice široká a zahrnuje celou škálu činností, které však všechny do působnosti Národního úřadu pro kybernetickou a informační bezpečnost nespádají. Doplnění ustanovení tak povede k jednoznačnému vymezení kompetencí týkajících se zajišťování bezpečnosti v rámci Kosmického programu Unie podle nařízení Evropského parlamentu a Rady č. 2021/696 v kontextu zastupování České republiky ve Výboru pro bezpečnostní akreditaci (SAB), resp. k jednoznačnému určení toho, že Národní úřad pro kybernetickou a informační bezpečnost má vzhledem ke své odbornosti zajišťovat jen informační a kybernetickou bezpečnost. Ostatní aspekty s tímto spojené zajišťují jiné subjekty (Ministerstvo dopravy, Ministerstvo obrany atd.).	Akceptováno jinak - nyní § 44 Text, navrhovaný v připomínce byl akceptován a doplněn působností, kterou Národní úřad pro kybernetickou a informační bezpečnost vykonává v rámci Kosmického programu: "vykonává působnost ve vybraných oblastech souvisejících s informační a kybernetickou bezpečností, bezpečnostní akreditací a bezpečností systémů a zavedených služeb v rámci Kosmického programu Unie podle nařízení Evropského parlamentu a Rady č. 2021/696, zejména plní funkce příslušného orgánu pro GOVSATCOM podle čl. 68 tohoto nařízení" Připomínkové místo s vypořádáním souhlasí.
458. Ministerstvo dopravy	Z	Požadujeme, aby návrh zákona stanovil, že záměrné či nezáměrné rušení signálu globálních družicových navigačních systémů (GNSS)	Neakceptováno.

	spadá mezi kybernetické hrozby, dále aby pro specificky vybrané provozovatele regulovaných služeb, kteří jsou často i provozovateli kritické infrastruktury státu, vznikla povinnost se tímto rizikem zabývat, a rovněž aby Národní úřad pro kybernetickou a informační bezpečnost přijal úlohu centra pro monitorování hrozeb GNSS interference v České republice. Ministerstvo dopravy na základě několikaletého zastupování České republiky ve výboru European GNSS Interference TaskForce a na základě výsledků studie a provedených měření v rámci programu ESA NAVISP s názvem „GNSS Vulnerability & Mitigation in Czech Republic“ zpracované GNSS Centrem Excellence (https://gnss-centre.cz/), je přesvědčeno, že je třeba provést aktivní kroky k ochraně důležité infrastruktury České republiky před záměrným i nezáměrným rušením signálu GNSS, který se využívá k určování polohy a navigaci dopravních prostředků, ale i jako vysoce přesný zdroj času (atomové hodiny), což pak slouží k časové synchronizaci telekomunikačních, datových, bankovních a elektrorozvodných sítí. Rušení signálu GNSS tak může v závislosti na rozsahu a délce působení potenciálně způsobit velmi rozsáhlé výpadky těchto služeb, od zastavení provozu letiště (již se stalo), dopravního kolapsu autonomních vozidel přítomných v místě rušení (otázka budoucnosti), výpadku telekomunikačních (stalo se na Slovensku) či bankovních sítí až po rozpad synchronizace elektrorozvodné sítě vedoucí až k tzv. „blackoutu“ (hrozí v případě několikadenního trvání plošného rušení, které neumožní včasnou synchronizaci synchrofázorové soustavy). Studie „The economic impact on the UK of a disruption to GNSS“, kterou zpracovala v roce 2017 London Economics pro vládu Spojeného království, odhaduje výši ztrát při pětidenním výpadku GNSS pro britské hospodářství na 5,2 miliardy liber. Při zohlednění podmínek v České republice lze ekonomické ztráty v hospodářství odhadovat na 181 milionů Euro. V kontextu probíhající války na Ukrajině rovněž není zcela neopodstatněné se domnívat, že riziko obdobných událostí je oproti minulým letům v České republice	Hrozbou je dle zákona „jakákoliv potenciální okolnost, událost nebo jednání, která mohou být příčinou kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, a která mohou poškodit, narušit nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo další osoby“, což GNSS rušení může naplňovat. Doplnění seznamu hrozeb budeme řešit až v rámci finalizace textů prováděcích předpisů k návrhu zákona. Vyhlášky k zákonu budou mít samostatné připomínkové řízení, ve kterém bude předložena aktualizovaná verze. Satelitní komunikační infrastruktury a služby jsou součástí obecného pojmu sítí a služeb elektronických komunikací, které svůj odraz v seznamu hrozeb již mají (a povinné osoby by je tedy měly reflektovat v procesu řízení rizik), budeme proto zvažovat, zda je vhodné seznam rozšiřovat o jednu specifickou službu, či zvolíme jiné komplexnější řešení. Koncepce zákona o kybernetické bezpečnosti spočívá a vždy spočívala v ukládání povinností orgánům a osobám, které zajišťují fungování státu, společnosti atp. Co se týče dozoru nad rušením signálu ze strany ČTÚ, NÚKIB s ČTÚ na toto téma vedl diskusi a naznal, že současné rozdělení zákonných pravomocí je v tomto smyslu dostatečné. Druhou otázkou jsou samozřejmě zdroje vynakládané na dozor nad rušením signálů a schopnosti ČTÚ účinně dozorovat všechna problematická místa, nicméně toto není věc, kterou by šlo vyřešit prostou změnou zákona o kybernetické bezpečnosti nebo převedením pravomocí na NÚKIB. Tuto problematiku je potřeba řešit komplexně, za součinnosti všech relevantních celků, a to nejen ČTÚ a NÚKIB, ale i všech zainteresovaných ministerstev. Reakce připomínkového místa:

	zvýšené (detailní výsledky studie a měření GNSS interference jsou k dispozici u zpracovatele studie - kontaktní osoba je ředitel GNSS Centra Excellence, Ing. Tomáš Duša Ph.D. a na Ministerstvu dopravy). Záměrem je proto vytvořit právní rámec pro povinnost vybraných provozovatelů regulovaných služeb zabývat se riziky rušení GNSS přijímačů používaných ve svém provozu, jelikož v současnosti nastavený systém vypořádávání se s ohlášenými případy rušení elektromagnetického spektra, které má v gesci Český telekomunikační úřad, není pro potřeby rychlého zásahu proti původci rušení a zejména prevenci, účinný. Proti lokálním, nečekaným a relativně krátce trvajícím incidentům rušení GNSS dnes neexistuje mechanismus obrany. Český telekomunikační úřad měření interference GNSS samo neprovádí, k ohlašování lokálních interferencí GNSS téměř nedochází, Český telekomunikační úřad je proto prakticky neregistruje a nic proti nim nepodniká. K uvedeným incidentům však, podle měření provedených GNSS Centrem Excellence, dochází v okolí dálniční sítě, v okolí letišť atp.. I kdyby však Český telekomunikační úřad události registroval, podle stávajících postupů bude trvat velmi dlouho, než bude Český telekomunikační úřad schopen zareagovat výjezdem měřicího vozu na místo incidentu a následně případně řešit incident s Policií České republiky. Český telekomunikační úřad dnes ani nedisponuje dostatkem měřících vozů, vlastní jich nízké jednotky na celou Českou republiku. Proto je v České republice třeba vytvořit zcela nový systém, který povede k účinné a rychlé obraně proti těmto hrozbám. Zákon o kybernetické bezpečnosti představuje dobrý nástroj umožňující začít prevencí na úrovni samotných provozovatelů regulovaných služeb, kteří jsou napadením potenciálně nejvíce ohroženi, a zároveň nabízí možnost vytvořit rámec pro nové kompetence Národního úřadu pro kybernetickou a informační bezpečnost jako monitorovacího centra hrozeb GNSS interference v České republice. Možnou cestou jak dosáhnout výše uvedeného, by bylo	Navržené vypořádání akceptujeme a souhlasíme i s doplněním seznamu hrozeb do příslušného prováděcího právního předpisu. Nicméně požadujeme být zapojeni do procesu přípravy příslušného prováděcího právního předpisu, v níž bude GNSS interference jako hrozba explicitně řešena. Nad rámec ještě dodáváme, že GNSS služby do obecného pojmu sítí a služeb elektronických komunikací ve smyslu zákona o elektronických komunikacích nespádají. Jednak se nejedná o služby telekomunikační, ale služby primárně navigační, jednak jako radionavigační služby je GNSS definované pouze Radiokomunikačním řádem, nikoliv zákonem o elektronických komunikacích. To však nebrání definici GNSS upravit v rámci prováděcího právního předpisu k zákonu o kybernetické bezpečnosti. Připomínkové místo s vypořádáním souhlasí.

		- rozšířit definici technických aktiv o přijímače signálu GNSS, které jsou již dnes využívány řadou provozovatelů regulovaných služeb (elektrická rozvodná síť, telekomunikační sítě, letiště, banky, burzy atp.), kteří často bývají i provozovateli kritické infrastruktury státu. Díky tomuto by se z nepříznivého ovlivnění uživatelů přijímačů GNSS nasazených v provozu regulovaných služeb stala kybernetická hrozba. Současně by bylo vhodné stanovit v prováděcím právním předpise výčet vybraných regulovaných služeb, které jsou rušením GNSS signálu potenciálně nejvíce ohroženy, - stanovit definici globálního navigačního družicového systému, - rozšířit působnost Národního úřadu pro kybernetickou a informační bezpečnost tak, aby se stal centrem pro monitoring hrozeb rušení GNSS signálu. Takové centrum dosud v České republice chybí, jelikož fenomén rušení GNSS dosud nebyl dostatečně reflektován. Riziko GNSS interference však bude v nadcházejících letech nabývat na důležitosti mimo jiné z důvodu rozvoje autonomní dopravy, která bude na signálu GNSS zcela závislá. Je proto třeba, aby se na celostátní úrovni shromažďováním informací o rušení GNSS někdo zabýval a Národní úřad pro kybernetickou a informační bezpečnost se jeví jako nejvhodnější subjekt, jelikož je již dnes pověřen plněním funkce Národního kontaktního centra pro službu Galileo PRS, jejíž rušení bude rovněž třeba v budoucnu sledovat a řešit s tím spojená bezpečnostní rizika pro silové složky státu. Současně požadujeme v návaznosti na tuto připomínku provést i související změny v návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti, který je nyní projednáván v rámci mezirezortního připomínkového řízení (č. j. předkladatele 4489/2023-NÚKIB-E/110).	

459. Ministerstvo práce a sociálních věcí	Z	K § 1 odst. 3 Větu „<i>Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.</i>“ navrhujeme změnit takto: „<i>Tento zákon se nevztahuje na informační systémy, které nakládají s utajovanými informacemi.</i>“. Dle informací předaných NÚKIB při aktualizaci KII je cílem Úřadu slovní spojení „<i>komunikační systém</i>“ dále nepoužívat.	Neakceptováno Připomínkové místo správně uvádí, že NÚKIB sousloví "komunikační systém" v rámci aplikace současného zákona o kybernetické bezpečnosti již nepoužívá a využití tohoto pojmu je v současném zákoně o kybernetické bezpečnosti obsolentní. Připomínkové ustanovení však odkazuje na zákon č. 412/2005 Sb., upravující bezpečnost systémů nakládajících s utajovanými informacemi. Tento zákon stále používá slovní spojení „informační nebo komunikační systémy“ a na tom tento návrh nic nemění - jedná se o jinou právní úpravu. Uvedení sousloví "komunikační systém" je tedy v tomto případě správné. Připomínkové místo s vypořádáním souhlasí.
460. Ministerstvo práce a sociálních věcí	Z	K § 2 odst. 2 písm. c) Navrhujeme upravit definici tak, aby bylo zřejmé, v jakých případech má být splněna informační povinnost poskytovatele regulované služby. Aktuální definice významné hrozby „<i>Potenciální okolnost na základě technických charakteristik, která má potenciál</i>“ je nejednoznačná a je spojena s informační povinností.	Neakceptováno Definice obou pojmů (jak kybernetické hrozby, tak významné kybernetické hrozby – po úpravě již jen „hrozba“ či „významná hrozba“, stejně jako povinnost informování uživatelů regulované služby) vycházejí ze směrnice NIS2 a Úřad se s v zájmu zajištění co nejvyšší úrovně harmonizace regulace kybernetické bezpečnosti napříč Evropskou unií rozhodl tam, kde to neodporuje cílům národní regulace, zachovat definice pojmů tak, jak jsou formulovány ve směrnici. Nadto je vhodné upozornit, že s potencialitou pracuje v definici hrozby i norma ČSN EN ISO/IEC 27000, která je ostatně (spolu s dalšími normami řady 27000) předlohou návrhů vyhlášek o bezpečnostních opatřeních. Použité definice tedy reflektují praxi v oboru.

			Co se týče plnění povinnosti podle § 20 odst. 2 návrhu zákona, toto informování se bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. Potenciál narušení nebo vážného ovlivnění budou v různých situacích a v kontextu různých poskytovatelů regulovaných služeb vykládány různě. Nebo také v situaci, kdy uživatel nemůže být hrozbou ovlivněn a kdy tedy není možné ani potřebné přijímat žádná opatření ke snížení dopadů realizace hrozby, samozřejmě k žádnému informování docházet nemusí. Je tedy zřejmé, že poměrně volné vymezení situací, ve kterých bude docházet k informování o významných hrozbách, je záměrem zákonodárce, neboť bude potřeba jej aplikovat v charakterem velmi odlišných situacích. Připomínkové místo s vypořádáním souhlasí.
461. Ministerstvo práce a sociálních věcí	D	K § 2 odst. 2 písm. g) Navrhujeme upravit definici tak, aby bylo zřejmé, že zákon upravuje pouze úmyslné chování. (Např.: „...<i>kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v rámci aktiv, v případě že nelze vyloučit úmyslné zavinění.</i>“) Cílem zákona by nemělo být hlášení veškerých kybernetických incidentů. To by mohlo vytvářet neúměrnou zátěž jak pro regulované subjekty, tak pro NÚKIB. Podle navrhované definice budou muset být hlášeny i neúmyslné chyby, například při plánovaných pracích. Britské Národní centrum kybernetické bezpečnosti (National Cyber Security Centre – NCSC) definuje kybernetický incident jako porušení bezpečnosti aktiva (systému) s cílem ovlivnit jeho integritu nebo dostupnost nebo neoprávněný přístup nebo pokus o neoprávněný přístup k aktivu (systému) s cílem porušit jeho důvěrnost.	Akceptováno jinak Definice kybernetického bezpečnostního incidentu zůstala v návrhu zachována, došlo nicméně k úpravě formulace § 16 odst. 1 na „Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a nejsou způsobeny vlastní provozní činností.“ Povinnost poskytovatele regulované služby v režimu vyšších povinností se proto nově nevztahuje na kybernetické bezpečnosti incidenty, které mají původ v kybernetickém prostoru, a zároveň jsou způsobeny vlastní provozní činností. Zahrnutí úmyslu mezi proměnné určující, zda incident bude hlášen či nikoli, bylo zvažováno a bylo zavrženo z důvodu, že zjišťování úmyslu by kladlo na povinné subjekty neúměrnou zátěž (nadto ve chvíli, kdy je

		Doporučujeme využít Metodiku k hlášení kybernetického bezpečnostního incidentu NÚKIB – viz https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni-incidentu_1.1.pdf, v jehož čl. 4.1. se uvádí: „<i>Kybernetický bezpečnostní incident není potřeba Úřadu hlásit v případě, kdy došlo v důsledku technického selhání k nedostupnosti části aktiv, lze s jistotou vyloučit úmyslné zavinění (zejména útočníkem) ...</i>“. Zároveň doporučujeme ze současné Metodiky vyloučit podmínku řádného fungování záložních systémů.	jejich primárním zájmem zvládnutí probíhajícího incidentu a nikoli zjištění, zda incident mohl být zaviněn úmyslně). Pokud jde o doporučení ohledně uvedené metodiky, k obsahu doporučení bude přihlédnuto při tvorbě nové metodiky, která bude založena na návrhu zákona, bude-li přijat. Připomínkové místo s vypořádáním souhlasí.
462. Ministerstvo práce a sociálních věcí	Z	K § 16 odst. 1 Navrhujeme omezit povinnost hlášení kybernetických incidentů pouze na významné incidenty, tedy na incidenty spojené se závažnými hrozbami, nebo zakotvit pravomoc NÚKIB stanovit a uznat výjimky z hlášení kybernetického bezpečnostního incidentu v obdobném rozsahu, jako je rozsah uvedený v kapitole 4 „Úřadem stanovené a uznané výjimky z hlášení kybernetického bezpečnostního incidentu“ Metodiky k hlášení kybernetického bezpečnostního incidentu NÚKIB – viz https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni-incidentu_1.1.pdf. Povinnost daná v tomto ustanovení je nastavena nad rámec implementace směrnice a bez dostatečného odůvodnění v důvodové zprávě. Z té naopak vyplývá, že pro NÚKIB jsou preferované pouze informace o závažných incidentech. I hlášení závažných incidentů by nemělo subjekt zaměstnat natolik, aby jeho pracovníci byli odváděni od řešení samotného incidentu k plněním administrativních povinností daných ZKB.	Akceptováno jinak Definice kybernetického bezpečnostního incidentu zůstala v návrhu zachována, došlo nicméně k úpravě formulace § 16 odst. 1 na „Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a nejsou způsobeny vlastní provozní činností.“ Povinnost poskytovatele regulované služby v režimu vyšších povinností se proto nově nevztahuje na kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a zároveň jsou způsobeny vlastní provozní činností. Reakce připomínkového místa: Není vypořádáno v kontextu připomínky. Není vysvětleno proč by se neměly hlásit jen významné incidenty. Pokud budeme muset hlásit všechny incidenty, tak potřebujeme 1 FTE navíc. NIS2 vyžaduje v článku 20 hlášení pouze významných incidentů: Member States shall ensure that essential and important entities notify, without undue delay, the

		CSIRT or, where relevant, the competent authority in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. 3. An incident shall be considered significant if: (a) the incident has caused or is capable of causing severe operational disruption of the service or financial losses for the entity concerned; (b) the incident has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material losses. Reakce NÚKIB: Povinnost hlášení incidentů se bude vztahovat na kybernetické bezpečnostní incidenty, u kterých lze dovodit úmyslné zavinění. Navrhovaná úprava je přísnější, protože reflektuje snahu EU o zvýšení bezpečnosti a odolnosti napříč celou EU. Z toho důvodu také došlo k vydání předmětné směrnice, v jejímž rámci došlo k podstatnému rozšíření rozsahu regulovaných odvětví v rámci hospodářského prostoru EU. Česká právní úprava si v zájmu zachování kontinuity přístupu zachovala požadavek na hlášení všech kybernetických bezpečnostních incidentů bez ohledu na jejich významnost, který je rozšířen i na ostatní subjekty odpovídající vyšším nárokům na zajištění kybernetické bezpečnosti podle NIS2 (těmto subjektům odpovídá množina "essentials"). Ačkoliv jsou požadavky na hlášení incidentů podle NIS2 méně přísné, NÚKIB si zachovává snahu o detailní povědomí o stavu kybernetické bezpečnosti v rámci České republiky zejména z důvodů analytických a preventivních, tedy např. možnosti detekovat rozsáhlejší kybernetický útok začínající jako incident

		s nízkou významností pro konkrétní subjekt, nicméně v důsledku zásahu více subjektů ve stejném odvětví vyúsťující v rozsáhlou škodlivou kampaň mající za následek narušení dostupnosti základních služeb. Hlášení všech incidentů bez ohledu na jejich významnost je povinnost, která vyplývá povinným subjektům již nyní z aktuálního znění ZKB. Mezi těmito povinnými subjekty je i MPSV. Reakce připomínkového místa: Není pravda, že dnes hlásíme všechny incidenty. To bychom NUKIB zavalili zhruba tisícovkou hlášení ročně. Hlásíme skutečně jen významné incidenty (jednotky za rok) a na ně stejně nedostáváme žádnou reakci. Postupujeme v souladu s metodikou (Národní úřad pro kybernetickou a informační bezpečnost - Metodika k hlášení kybernetického bezpečnostního incidentu (nukib.cz). Nevidím žádný důvod, proč tento status měnit. V rámci prezentace nového zákona a procesu vypořádávání připomínek však ze strany NUKIB několikrát zaznělo, že tato metodika nebude platná. Možná vznikne nová, možná nikoli. Tu jistotu nemáme. A navrhovaná textace zákona pro nás znamená extrémní administrativní zátěž, na kterou musíme zajistit min. 1x FTE. A pro NUKIB to může znamenat faktický DDOS útok z naší strany, protože budeme zasílat několik hlášení denně. A nejen my. Slovo „significant“ je v textu zákona skutečně významné a MPSV na něm trvá. Po schůzce: Připomínkové místo bylo ve vztahu k hlášení incidentů ujistěno, že bude stále fungovat metodická podpora a budou vydány metodické pomůcky týkající

			se hlášení incidentů, jak je tomu nyní. Tímto je připomínka vypořádána. Připomínkové místo s vypořádáním souhlasí.
463. Ministerstvo práce a sociálních věcí	D	K § 16 odst. 2 Navrhujeme zavést zkratku CERT. Zkratka CERT se v tomto ustanovení v rámci návrhu zákona vyskytuje poprvé, aniž by byla zavedena. Navíc z návrhu zákona jednoznačně nevyplývá, že se tímto národním CERT nemyslí právě Úřad. Zkratka je pravděpodobně převzatá z anglického <i>Computer Emergency Response Team</i>, což adresát normy nemusí vědět.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
464. Ministerstvo práce a sociálních věcí	D	K § 17 odst. 1 Navrhujeme vypustit část věty za slovy „prvotní hlášení“ a větu za slovy „prvotní hlášení“ ukončit tečkou. Odůvodnění tohoto našeho návrhu vyplývá z našich návrhů k § 2. Máme zato, že z důvodu požadavku na dodatečný report do 72 hodin po zjištění incidentu je v první fázi vhodné věnovat prioritu řešení incidentu a analýze možných dopadů. Dodatečné informace lze doplnit v následujících reportech, kdy bude navíc zřejmé, zdali se jedná o významný incident, jak požaduje i směrnice NIS2.	Neakceptováno Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnicí NIS2, tzn. pokud bychom do zákona tuto úpravu nezahrnuli, návrh by byl v rozporu se směrnicí a ČR by mohla čelit sankcím za nesprávnou transpozici EU předpisu. Obsahem prvotního hlášení podle čl. 23 odst. 4 písm. a) směrnice NIS2 (ve směrnici označen jako včasné varování) je uvedení toho, "zda se [subjekty] domnívají, že byl významný incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad". Z výše uvedeného důvodu národní právní úprava tento požadavek kopíruje. Připomínkové místo s vypořádáním souhlasí.
465. Ministerstvo práce a sociálních věcí	Z	K § 18 odst. 3 Povinnost upravenou v první větě tohoto ustanovení navrhujeme zúžit pouze na případy významných incidentů, a to takto: „Každý je povinen poskytnout na výzvu Úřadu nezbytné informace a další	Neakceptováno Rozumíme tomu, že povinnost poskytnout součinnost CERT při zvládání všech incidentů představuje pro

		nezbytnou součinnost při zvládnání významného kybernetického bezpečnostního incidentu, pokud nelze sledovaného účelu dosáhnout jinak nebo by bylo jinak jeho dosažení podstatně ztíženo. “. <i>Za druhou větu navrhuje doplnit třetí větu tohoto znění: „V případě, že osoba nebyla incidentem zasažena, náleží ji úhrada nákladů dle zvláštního předpisu. “.</i> Pokud by se měla povinnost uvedená v první větě tohoto ustanovení týkat jakéhokoliv kybernetického incidentu, znamenalo by to velkou administrativní zátěž zejména pro subjekty s velkým počtem zákazníků. Zvláštním předpisem je třeba upravit úplatu v případě, že povinná osoba není incidentem sama zasažena, a to zejména v případě osob uvedených v § 63 odst. 2.	dotčené osoby přinejmenším zvýšenou administrativní zátěží či potřebu alokovat na tuto součinnost personální zdroje, byť dočasně. Na druhou stranu platí, že právní úpravou zakotvená možnost CERT podílet se na zvládnání incidentů představuje pro CERT příležitost analyzovat četnost a povahu jednotlivých incidentů. Tímto způsobem budou průběžně posilovány jak schopnost CERT účinně na konkrétní incidenty reagovat, tak také schopnost podílet se na přípravě preventivních opatření. V konečném důsledku tak dojde k celkovému posílení bezpečnosti v kybernetickém prostoru na území České republiky a prostřednictvím sdílení zjištěných poznatků také na mezinárodní úrovni. Součinnost bude vyžadována pouze v nezbytných a důvodných případech tak, aby byl zásah do práv dožádaných osob proporční k míře nebezpečnosti a rizikovosti daného incidentu a důležitosti poskytované regulované služby, která je tímto incidentem ohrožena. S plněním povinnosti součinnosti podle tohoto ustanovení návrhu zákona se nepředpokládá zvýšená finanční zátěž povinných orgánů a osob, proto není řešena ani případná úhrada nákladů. Připomínkové místo s vypořádáním souhlasí.
466. Ministerstvo práce a sociálních věcí	Z	K § 19 odst. 1 Za dosavadní poslední větu tohoto ustanovení navrhuje vložit novou poslední větu tohoto znění: „Zveřejnění informace nesmí ohrozit bezpečnost nebo provoz regulované služby a povinné osoby.“. Rozsah informační povinnosti není nijak upřesněn, respektive omezen. Úřad tak může vyzvat ke zveřejnění informací bez znalosti celkového kontextu incidentu. Přílišná transparentnost může v některých případech ohrozit bezpečnost regulovaných služeb a kritické infrastruktury.	Neakceptováno - nyní § 20 Uložení a rozsah informační povinnosti je náležitě zvážen ze strany Úřadu. Úřad při rozhodování o zveřejnění informací o kybernetickém bezpečnostním incidentu vezme v rámci správního uvážení do úvahy potřebu zachování rovnováhy mezi zájmem veřejnosti být informovanou o hrozbách a incidentech, a možným poškozením pověsti poskytovatele regulované služby či ohrožením bezpečnosti

			regulované služby zasažené incidentem. Reflektovány budou také skutečnosti, které Úřad zjistil v průběhu konzultace s s tímto poskytovatelem. Reakce připomínkového místa: Zveřejnění informace o bezpečnostním incidentu může vyvolat paniku mezi lidmi a může ohrozit provoz poskytované služby. Pokud NUKIB při vysvětlení souhlasí, že „...vezme v rámci správního uvážení do úvahy potřebu zachování rovnováhy...“, tak proč si tento postup nenapíše do zákona? Reakce NÚKIB: Do předmětného ustanovení byla přidána formulace "po konzultaci s tímto poskytovatelem regulované služby". Případné ohrožení bezpečnosti nebo provozu regulované služby tak bude nejprve konzultováno s dotčeným poskytovatelem. Pokud poskytovatel sám, narozdíl od Úřadu, nedojde k závěru, že by bylo vhodné o incidentu informovat, bude Úřad patrně disponovat větším množstvím informací k dostatečnému posouzení zachování rovnováhy mezi zájmem uživatelů regulované služby na informacích být informování o hrozbách a incidentech, a možným poškozením bezpečnosti, pověsti či obchodních zájmů poskytovatele regulované služby, který incident ohlašuje. Připomínkové místo s vypořádáním souhlasí.
467. Ministerstvo práce a sociálních věcí	Z	K § 19 odst. 2 Část první věty po slovech „bez zbytečného odkladu“ navrhuje nahradit slovy: „hrozbu vyhodnotit a zvážit informování zákazníků tak, aby nedošlo k ohrožení zajišťování kybernetické bezpečnosti nebo provozu regulované služby.“.	Vysvětleno - nyní § 20 Bezodkladně je poskytovatel regulované služby povinen informovat uživatele o krocích, které může uživatel učinit v reakci na hrozbu. K informování o hrozbě samotné poskytovatel regulované služby

		Povinnost informovat o hrozbách za všech okolností může ohrozit bezpečnost regulovaných služeb a kritické infrastruktury.	přistoupí pouze v případech, kdy je to možné a vhodné, tedy po vyhodnocení ze strany tohoto poskytovatele, který může vzít v potaz i v připomínce navrhované skutečnosti. Připomínkové místo s vypořádáním souhlasí.
468. Ministerstvo práce a sociálních věcí	Z	K § 25 odst. 1 jako celku Navrhujeme, aby předkladatel vyjasnil myšlenku týkající se pravomocí Úřadu v případě „hrozícího“ incidentu, anebo aby toto ustanovení upravil tak, aby bylo zřejmé, o jakou situaci se má jednat, a aby vyjasnil, o jaká data a informace se jedná, pokud ještě incident nenastal. Pojem „hrozící kybernetický bezpečnostní incident“ není definován, a není použitý ani v jiných částech návrhu. Není zřejmé, zda neměl předkladatel na mysli „událost“. Především však není zřejmý požadavek na nutnost předávání informací v momentě, kdy ještě nedošlo k incidentu. Není stanoveno, kdo je oprávněn určit, že se jedná o hrozící incident, tedy kdo posoudí oprávněnost podnětu. Bez vyjasnění může docházet ke zneužití a nepřesným interpretacím.	Akceptováno - nyní § 26 Definice hrozícího kybernetického bezpečnostního incidentu byla upřesněna. Úřad bude při zvažování dopadu incidentu brát v rámci správního uvážení v potaz vždy konkrétní okolnosti každého případu. V každém případě se bude jednat o informace a data související s provozem aktiv sloužících k poskytování regulované služby. Připomínkové místo s vypořádáním souhlasí.
469. Ministerstvo práce a sociálních věcí	Z	K § 25 odst. 1, poslední věta Za dosavadní poslední větu tohoto ustanovení navrhujeme doplnit novou poslední větu tohoto znění: „<i>Formát, rozsah, způsob a termín předání informací nesmí jít nad rámec smluvních závazků.</i>“. Je nutné respektovat smluvní ujednání.	Neakceptováno - nyní § 26 Toto ustanovení míří na krajní situace, kdy by hrozící či probíhající kybernetický bezpečnostní incident mohl mít závažný vliv na poskytování regulované služby s dopadem na zachování základních funkcí státu, hospodářských činností, bezpečnosti, veřejného zdraví, majetku nebo životního prostředí. V takovém případě převládá zájem státu na odvrácení incidentu s takto významným dopadem nad soukromoprávní dohodou o předání dat. Povinnost zanést do smlouvy specifikace podmínek pro formát předání dat,

			provozních údajů a informací po vyžádání povinnou osobou je součástí bezpečnostních opatření, která bude poskytovatel regulované služby v režimu vyšších povinností povinen zavádět. Vzhledem k tomu, že příslušná ujednání by měla být součástí smluvního vztahu mezi poskytovatelem regulované služby a významným dodavatelem, měl by institut předání dat sloužit jako ultima ratio až poté, co selžou jednání mezi dotčenými stranami. Do situace, kdy je smlouva jasně ujednána, vyhovuje oběma stranám a významný dodavatel se jejím plnění nebrání, Úřad nikdy zasahovat nebude. Připomínkové místo s vypořádáním souhlasí.
470. Ministerstvo práce a sociálních věcí	Z	K § 28 odst. 1 Navrhujeme doplnit, že Úřad si může vyžádat pouze informace a data, které jsou k tomuto účelu nezbytné. Dále navrhujeme doplnit, že Úřad je oprávněn použít informace a data pouze za účelem hodnocení rizikivosti dodavatelů bezpečnostně významné dodávky a pouze za tímto účelem je oprávněn si je vyžádat. Navrhované znění explicitně neomezuje účel sběru informací, účel žádostí ani charakter sbíraných a vyžadovaných informací. Absence těchto omezení vytváří zjevně nezamýšlený prostor pro zneužití institutu sběru údajů a součinnosti k neodůvodněnému shromažďování údajů o právnických i fyzických osobách. Navrhované znění by bylo možné vykládat např. tak, že zakládá povinnost poskytovatele služeb elektronických komunikací poskytnout NÚKIB na vyžádání shromažďované provozní a lokalizační údaje, ačkoli takové poskytnutí by ve většině případů bylo neproporcionálním zásahem do ústavně chráněného základního práva na soukromí.	Neakceptováno - nyní § 29 NÚKIB shromažďuje a vyhodnocuje informace primárně za účelem zajištění fungování mechanismu bezpečnosti dodavatelského řetězce. Z povahy činnosti správních orgánů však nelze vyloučit, že získané informace budou využity i při dalších činnostech NÚKIB nebo jiných orgánů veřejné moci. Bylo by v rozporu se základními zásadami činnosti správních orgánů, pokud by NÚKIB tyto informace nepředal, respektive nevyužil při výkonu ostatních pravomocí. NÚKIB však garantuje, že v žádostech o součinnost podle § 29 odst. 1 až 3 bude postupovat v souladu s principem proporcionality. Tento soulad bude kontrolován i dotazovanými orgány a osobami, které řádně neodůvodněné žádosti nemusí vyhovět. Je vhodné doplnit, že žádosti o součinnost podle § 29 ods. 1 až 3 se nijak neliší od obdobných institutů zákona. Připomínkové místo s vypořádáním souhlasí.

471. Ministerstvo práce a sociálních věcí	D	K § 28 odst. 3 písm. c) Navrhujeme doplnit úroveň poddodavatelského řetězce, která má být předmětem zjišťování povinné osoby mechanismu prověřování dle § 32 odst. 1 písm. a), nebo způsoby pro její stanovení (např. odkaz na prováděcí právní předpis a zmocnění k jeho vydání). Dále navrhujeme doplnit povinnost podnikatele vyhodnotit takovou informaci přiměřeně k jeho schopnostem. V souladu s cílem a účelem předmětné úpravy je přiměřené, aby povinná osoba mechanismu prověřování zjišťovala informace nejen o primárním dodavateli, kterým bude často pouze distributor, ale také o přímém výrobcí daného produktu nebo poskytovateli služby, vůči nimž je stěžejní prověřit rizikovost. Navrhované znění však lze vykládat i jako povinnost zjišťovat informace i o dodavatelích jednotlivých komponent daného výrobku (polovodičových prvků) nebo dodavatelích dílčích programových prostředků (licencí), pomocí nichž je poskytována služba přímým dodavatelem. Taková povinnost pro povinné osoby mechanismu prověřování by byla nepřiměřená, a není opodstatněna bezpečnostními riziky, která jednotlivé komponenty či programové vybavení představují pro kybernetickou bezpečnost regulované služby.	Neakceptováno NÚKIB je přesvědčen, že současný návrh úpravy umožňuje poskytovateli strategicky významné služby dostatečnou volnost uvážení, zda zjištění a nahlášení určitého poddodavatele je pro něj přiměřené z pohledu vynaloženého úsilí. Je však na poskytovateli, aby si tento krok dokázal obhájit během kontroly ze strany NÚKIB. Nelze však a priori říci, že dodavatel licence nebo jednotlivých komponentů nemá z pohledu kybernetické bezpečnosti význam. Stejně tak není možné pevně stanovit úroveň, do které mají být informace o dodavatelích zjišťovány. Neurčitost a navázání na přiměřené úsilí je kompromisem, který zajistí správné a efektivní fungování mechanismu a zároveň nebude neadekvátně zatěžovat poskytovatele strategicky významné služby. Připomínkové místo s vypořádáním souhlasí.
472. Ministerstvo práce a sociálních věcí	Z	K § 29 odst. 1 a 2 Mezi orgány, které mají poskytovat Úřadu informace a součinnost, navrhujeme doplnit Český telekomunikační úřad (ČTÚ). Návrh zákona o kybernetické bezpečnosti a související předpisy významně dopadají na poskytovatele regulovaných služeb v oblasti služeb elektronických komunikací, přesto původní znění výslovně nezmiňuje mezi orgány poskytujícími součinnost ČTÚ (jakkoli jej lze považovat za „další orgán“ podle části věty za středníkem). ČTÚ má přitom ve vztahu k oblasti služeb elektronických komunikací největší	Neakceptováno - nyní § 30 Dle navrhované úpravy NÚKIB v rámci získávání informací spolupracuje s relevantními orgány státu, přičemž v případě jednotlivých sektorů pak zákon v podobě, jaké je dnes, tuto spolupráci předpokládá s regulátory jednotlivých sektorů, je-li to pro daný případ možné. Toto je zaručeno mimo jiné § 8 odst. 2 zákona č. 500/2004 Sb, správního řádu. Dále je tento postup dán principem dobré správy, kdy NÚKIB pro

		odbornost, dohlíží nad bezpečností a integritou komunikačních sítí a ukládá opatření k řešení hrozeb (§ 98 zákona č. 127/2005 Sb., o elektronických komunikacích), díky čemuž disponuje řadou informací významných z hlediska technologií, které je pro zajištění bezpečnosti dodavatelského řetězce třeba zohlednit (zejména z hlediska nepominutelných funkcí stanoveného rozsahu).	co nejlepší vyhodnocení situace a možných dopadů počítá s dožádáním informací od relevantních orgánů státu v rámci jednotlivých odvětví. Důvodem, proč jsou v navrhovaném zákoně popsány orgány, které jsou obsaženy v § 30, je ten, že tyto fungují napříč jednotlivými sektory a jejich spolupráce je tak pro správné posouzení rizik, včetně vyhodnocení pro případné omezení či zákaz, žádoucí. Připomínkové místo s vypořádáním souhlasí.
473. Ministerstvo práce a sociálních věcí	D	K § 30 odst. 2 Do tohoto ustanovení navrhuje doplnit text: „<i>Opatření obecné povahy nabývá účinnosti 6 měsíců od jeho vydání.</i>“. Navrhované znění v § 30 odst. 3 vylučuje aplikaci vybraných ustanovení správního řádu, včetně ustanovení o účinnosti opatření obecné povahy (dále jen „OOP“), což zakládá právní nejistotu. S ohledem na významné dopady opatření obecné povahy do nákupních procesů povinných osob mechanismu prověřování také není možné realizovat povinnosti plynoucí z OOP okamžitě bez negativního dopadu na poskytování regulované služby. Je proto třeba nastavit účinnost jako odloženou. Námi navržená úprava směřuje k odstranění nejistoty povinných osob mechanismu prověřování a vytváří prostor pro zajištění odpovídajících náhradních bezpečnostně významných dodávek v souladu se zákazy a podmínkami dle OOP. Avšak obecně nevnímáme využití institutu OOP v této podobě jako vhodné. Proto dáváme do úvahy přehodnocení institutu OOP coby prostředku pro omezení dodavatelského řetězce, případně navrhuje doplnění tohoto procesu o konkrétní procesní kroky NÚKIB do ZKB. Doplněno by mělo být zejména zajištění právních jistot subjektům, kteří vstupují do procesu Mechanismu a přezkoumatelnost vydaného OOP.	Neakceptováno - nyní § 31 Lhůta pro plnění podmínek a zákazů plynoucích z opatření obecné povahy bude stanovena Úřadem přímo v OOP, proto není potřeba posunovat jeho účinnost samotnou. Tato lhůta bude přiměřená a bude zohledňovat ekonomickou životnost bezpečnostně významných dodávek tak, aby byla maximálně šetřena práva subjektů, na které OOP dopadne. Účinnost je zachována podle ustanovení správního řádu a opatření obecné povahy tak nabývá účinnosti patnáctým dnem po dni vyvěšení veřejné vyhlášky, pokud by hrozila vážná újma veřejnému zájmu, tak může nabýt účinnosti již dnem vyvěšení. Pro realizaci povinností bude v OOP stanoveno dostatečné přechodné období, zpravidla v řádu let, ve kterém budou mít subjekty prostor své dodávky uvést do souladu s podmínkami nebo zákazy stanovenými v OOP. Institut opatření obecné povahy byl zvolen, jelikož nejlépe odpovídá potřebám mechanismu prověřování dodavatelského řetězce, kdy musí být stanoveny konkrétní povinnosti blíže nespecifikovanému okruhu subjektů. Je na místě uvést, že tento institut je v právním řádu běžně využívaný a subjektům poskytuje dostatečnou právní jistotu. Proti vydanému OOP je pak možné podat

	V důvodové zprávě je uváděno: „Stanovit omezení jiným způsobem, například rozhodnutím Úřadu, by vyžadovalo, aby Úřad disponoval významně větším rozsahem informací o bezpečnostně významných dodávkách, než vyžaduje předkládaná podoba návrhu“. Z uvedeného by však vyplývalo, že NÚKIB si je vědom, že koná bez znalosti předmětu posuzování samotného OOP. Nelze se však domnívat, že by mohlo dojít k posouzení něčeho, o čem posuzující subjekt nemá dostatek informací. Odůvodnitelnost OOP jako prostředku, který je určen neurčitému počtu adresátů nepovažujeme taktéž za adekvátní, a to už z důvodu toho, že NÚKIB je povinen vést databázi poskytovatelů regulovaných služeb. Z takového seznamu je v případě potřeby jistě možné zajistit konkrétní okruh adresátů. Pokud by existoval konkrétní okruh adresátů, nemohlo by se jednat o OOP, které je charakterizováno (vedle konkrétně určeného předmětu) právě obecně vymezeným okruhem adresátů, nýbrž o individuální rozhodnutí, a to bez ohledu na to, že by se týkalo většího množství adresátů. Institut OOP v omezené formě, kterou NÚKIB předkládá v návrhu zákona, mimo jiné neumožňuje subjektům podávat námitky jako účastníkům řízení. Zároveň i s ohledem na znění ostatních připomínek akcentujeme, že OOP vydává NÚKIB sám a nepodléhá schválení např. správním orgánům a institucím, kterým náleží gesce ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu, jak je v zákoně a vyhláškách často zmiňováno. Případně lze navrhnout řešení podle rakouské legislativy spočívající ve vytvoření odborné komise ze zástupců orgánů veřejné správy v daných oblastech a zástupců dotčených osob. Ve znění § 28 Prověřování rizik spojených s dodavatelem ZKB není dostatečným způsobem popsán proces, kterým NÚKIB dojde k	návrh na zahájení přezkumného řízení nebo jej napadnout správní žalobou na jeho zrušení. Opatření obecné povahy bude Úřad vydávat vždy na základě maxima informací, které bude moci získat s ohledem na rozsah své pravomoci a součinnost jiných orgánů. Z pohledu Úřadu by nebylo účelné vést řízení vedoucí k rozhodnutí, jelikož se množina subjektů, které budou případným zákazům nebo podmínkám stanoveným v OOP podléhat, může v průběhu času měnit, a proto je vhodnější využití tohoto prostředku, kterým lze stanovit konkrétní povinnosti blíže neurčenému okruhu osob, kterým jsou v případě mechanismu prověřování bezpečnosti dodavatelského řetězce povinné osoby regulace, splňující specifická kritéria. Na procesu vydávání OOP se budou podílet povinné osoby a relevantní orgány státu prostřednictvím připomínek k jeho návrhu, jejichž vypořádání musí Úřad náležitě odůvodnit a v případech, kdy to nebude odporovat smyslu a účelu opatření, připomínkám vyhoví. Některé orgány státu na procesu vydání OOP také spolupracují prostřednictvím poskytování informací nebo stanovisek, které slouží jako podklad pro vydávání opatření obecné povahy. Je na místě, aby rozhodování připadalo Úřadu, jakožto gestorovi kybernetické bezpečnosti. S ohledem na smysl zákona není vhodné kazuisticky popisovat postup správního orgánu, ale stanovit rozsah jeho zmocnění a prostředky, kterými může působit. Postup vydávání opatření obecné povahy upravuje správní řád a mechanismus prověřování tento postup s jistými modifikacemi využívá. Součástí procesu vydávání OOP bude také zhodnocení rizik a dopadů, které navrhované opatření může mít. Proti opatření obecné povahy lze podat návrh na zahájení přezkumného řízení nebo podat správní žalobu na jeho zrušení. V

		závěrům shrnutým v OOP. Formulace „<i>Úřad shromažďuje a vyhodnocuje informace a data</i>“ není dostatečným popisem procesních kroků, které bude NÚKIB činit, a nezakládá ani předpoklad, že návrh znění OOP bude zpětně konzultováno s orgány, které NÚKIBu předkládaly informace, ani že bude znění OOP zároveň podléhat schválení některých z těchto orgánů. Součástí celého procesu by měla být bezpodmínečně analýza rizik a dopadová analýza nákladů a výnosů takového opatření. Jako příklad obdobného procesu, který je již praxí ověřený, může NÚKIBu sloužit např. proces analýzy relevantních trhů ČTÚ, kdy je povinnost plnění povinností OOP udělena subjektu na základě rozhodnutí ČTÚ. Zásadním nedostatkem OOP je ovšem nemožnost podání opravného prostředku. V případě takto významného omezení tržního prostředí považujeme za zásadní, aby se dotčené subjekty mohly bránit proti vydání takového opatření jinou než pouze soudní cestou. Soudní přezkum vydaného OOP je s ohledem na lhůty výběrového řízení dodavatele a jeho prověřování pro interní účely a celého procesu kontrakce a dodávky nových technologií nedostačující. Aplikuje se zde princip <i>ex nunc</i>, což v tomto případě znamená, že dotčená osoba bude muset po vydání OOP konat okamžitě, aby stihla případnou lhůtu pro výměnu/vyřazení technologií omezeného/zakázaného dodavatele. Proto kontrakty s omezeným/vyřazeným dodavatelem v případě zrušení OOP soudem již nebude možné obnovit.	procesu vydávání OOP mohou oprávněné subjekty také uplatňovat proti jeho návrhu připomínky. Proti tomuto institutu je tedy možné se bránit více způsoby. Závěry uvedené v OOP také musí být řádně a přezkoumatelně odůvodněny. Pokud by plnění opatření obecné povahy mohlo podstatným způsobem ohrožovat poskytování strategicky významné služby, může být také udělena výjimka z podmínek nebo zákazu jím stanovených. Připomínkové místo s vypořádáním souhlasí.
474. Ministerstvo práce a sociálních věcí	Z	K § 31 odst. 1 Navrhujeme před čárkou na konci tohoto odstavce doplnit slova „<i>nebo by vyžadovalo vynaložení nepřiměřeného úsilí nebo nákladů ze strany povinné osoby mechanismu prověřování.</i>“ V rámci udělování výjimek by měly být zohledněny ekonomické dopady opatření obecné povahy na povinné osoby a praktická	Akceptováno jinak - nyní § 32 Již současné znění umožňuje, aby byla výjimka udělena na základě skutečnosti, že by plnění povinností stanovených opatření obecné povahy vyžadovalo od poskytovatele strategicky významné služby natolik zásadní a závažné kroky (např. z

		možnost zajištění náhradních bezpečnostně významných dodávek, jelikož povinnosti a omezení plynoucí z opatření obecné povahy mohou mít za následek nepřiměřené náklady nebo jejich splnění může vyžadovat nepřiměřené úsilí (např. na zajištění náhradního plnění jiného bezpečnostně významného dodavatele).	pohledu nákladů), že by v jejich důsledku došlo k podstatnému ohrožení poskytování strategicky významné služby. Pro vyjasnění jsme však toto doplnili do důvodové zprávy v následujícím znění: "Skutečností odůvodňující povolení výjimky z opatření obecné povahy může být např. vynaložení takového úsilí nebo finančních nákladů, které by přímo ohrozily existenci poskytovatele strategicky významné služby a tím i poskytování samotné strategicky významné služby." Připomínkové místo s vypořádáním souhlasí.
475. Ministerstvo práce a sociálních věcí	D	K § 32 odst. 2 Navrhujeme doplnit, že doba 1 roku od dne doručení písemného vyrozumění o zápisu se vztahuje také na povinnost zjišťovat informace podle § 32 odst. 1 písm. a). Přechodné období by se nemělo uplatnit pouze pro povinnost hlásit NÚKIB informace, ale i pro povinnost je zjišťovat a řídit se opatřením obecné povahy. Požadavek, aby povinné osoby mechanismu prověřování zahájily sběr informací a plnění opatření obecné povahy bezprostředně po účinnosti zákona, bez stanovení přechodného období, je nepřiměřený.	Neakceptováno - nyní § 33 Smyslem roční přechodné lhůty pro hlášení předmětných informací je mimo jiné umožnit poskytovateli strategicky významné služby nastavit do té doby procesy shromažďování a dokumentace požadovaných informací a tyto informace shromáždit v takové kvalitě, aby měl NÚKIB po prvotním hlášení informací co nejpřesnější a nejúplnější informace o významnosti dodavatelů a jejich plnění v celé strategicky významné infrastruktuře a mohl tak bezodkladně zahájit jejich prověřování. Realita pak bude taková, že poskytovatel strategicky významné služby si v prvním roce po písemném vyrozumění o označení regulované služby jako strategicky významné služby v evidenci regulovaných služeb (zde proběhla změna oproti původnímu návrhu, kdy se přechodná lhůta vázala na účinnost zákona) nastaví procesy a začne zjišťovat požadované informace. Tyto pak bude muset nejpozději po roce a deseti dnech nahlásit NÚKIB. Není tedy důvod stanovovat přechodnou lhůtu i pro povinnost informace zjišťovat.

			Poskytovatelé strategicky významné služby budou mít dostatek času i podle stávajícího návrhu. Připomínkové místo s vypořádáním souhlasí.
476. Ministerstvo práce a sociálních věcí	D	K § 38 Navrhujeme toto ustanovení vypustit. Stav kybernetického nebezpečí nemá svým rozsahem a požadovanými prostředky nahrazovat/ duplikovat standardní nouzový stav.	Akceptováno jinak - nyní § 39 Souhlasíme s navrhovatelem, že cílem stavu kybernetického nebezpečí není nahrazovat/duplikovat standardní nouzový stav. Na vhodném znění celé soustavy ustanovení o stavu kybernetického nebezpečí spolupracujeme s Ministerstvem vnitra – Generálním ředitelstvím Hasičského záchranného sboru a návrh bude upraven na základě těchto jednání. Stav kybernetického nebezpečí byl upraven tak, aby opatření, která umožňuje, neodpovídala a tedy neduplikovala opatřením v rámci krizových stavů v krizovém zákoně. Připomínkové místo s vypořádáním souhlasí.
477. Ministerstvo práce a sociálních věcí	D	K § 40 odst. 1 písm. g) a odst. 2 písm. b) Navrhujeme ustanovení § 40 odst. 1 písm. g) a odst. 2 písm. b) vypustit. Zákon nedefinuje rozsah ani metodiku provedení skenu zranitelností a penetračního testu. Sken zranitelností a penetrační test technických aktiv provedený na jejich produkční části může zásadně narušit funkčnost technických aktiv až do míry ekvivalentní reálnému kybernetickému útoku. Může způsobit nestabilitu, dlouhodobé selhání, případně přímo usnadnit budoucí kybernetický útok. Provedení skenu zranitelností a penetračního testu musí být vždy v odpovědnosti vlastníka nebo provozovatele technických aktiv a musí být prováděno v rámci plánovaných výlukových oken, a to v definovaném rozsahu s odhadnutelným dopadem.	Neakceptováno - nyní § 41 Povinnost součinnosti vyzvaných orgánů a osob je v návrhu zákona právě za tím účelem toho, aby nebylo zasaženo do funkčnosti technických aktiv, a to provedením zpravidla méně invazivního skenu zranitelností nebo penetračním testováním. Ohledně rozsahu a metodiky je proto nezbytné konzultovat s příslušnými odpovědnými pracovníky orgánů a osob, u nichž se znalost informačního systému předpokládá, a skrze jejichž součinnost by mělo být zamezeno narušení funkčnosti technických aktiv. Připomínkové místo s vypořádáním souhlasí.

478. Ministerstvo práce a sociálních věcí	D	K § 41 odst. 3 písm. x) Navrhujeme za slovo „státu“ doplnit slova „Evropské unie“.	Akceptováno - nyní § 44 Připomínkové místo s vypořádáním souhlasí.
479. Ministerstvo práce a sociálních věcí	D	K § 41 odst. 4 Navrhujeme zavést zkratku CSIRT. Zkratka CSIRT se v tomto ustanovení v rámci návrhu zákona vyskytuje poprvé, aniž by byla zavedena. Zkratka je pravděpodobně převzatá z anglického <i>Computer Security Incident Response Team</i>, což adresát normy nemusí vědět.	Akceptováno - nyní § 44 Připomínkové místo s vypořádáním souhlasí.
480. Ministerstvo práce a sociálních věcí	D	K návrhu vyhlášky o regulovaných službách <u>K návrhu vyhlášky obecně</u> Navrhujeme změnit formu prováděcího předpisu na nařízení vlády. Znění navrhované předkladatelem umožňuje NÚKIB, aby na základě vlastního uvážení rozhodoval o okruhu jím regulovaných subjektů, přičemž zákon nevylučuje, aby tento okruh byl rozšířen na libovolný subjekt v národním hospodářství. Taková míra koncentrace pravomocí v rukou jednotlivého orgánu veřejné správy je v demokratickém a právním státě nepřijatelná. Navrhovaná změna má za cíl přenést pravomoc určování rozsahu působnosti zákona o kybernetické bezpečnosti na vládu obdobně jako v případě nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které v současnosti určuje prvky infrastruktury, na něž dopadá nejprísnejší režim regulace dle zákona o kybernetické bezpečnosti.	Neakceptováno Právní forma nařízení vlády není pro danou regulaci odpovídající. Stanovení okruhu povinných osob, jejich režimu a dalších ustanovení pro něž je vydáván prováděcí právní předpis je analogicky nejpodobnější současnému nastavení vyhlášky č. 437/2017 Sb., o kritériích pro stanovení provozovatelů základní služby, což je spolu s § 22a současného zákona o kybernetické bezpečnosti způsob stanovení osobní působnosti transpozičních ustanovení předchozí směrnice NIS1. Stejným způsobem je tedy přistupováno k transpozici směrnice NIS2 - podstata věci se i přes rozdílnost směrnic v tomto případě nijak nemění. Stanovení okruhu povinných osob prostřednictvím prováděcího právního předpisu na základě a v mezích zákona (jak vyplývá z čl. 79 odst. 3 Ústavy) je v působnosti Úřadu. Z tohoto důvodu také není využito nařízení vlády, které má být využito jen v situacích, kdy se věc týká působnosti více než dvou orgánů nebo je dán naléhavý obecný zájem, což v tomto případě provedení běžného ustanovení zákona není. Je potřeba také upozornit, že domněnka navrhovatele, že je Úřadu dána pravomoc "rozšířit

			regulaci na jakýkoliv subjekt v národním hospodářství" je mylná, protože jsou zákonem za prvé dány odvětví v rámci kterých je možné takové úvahy vůbec provádět, nehledě na to, že za druhé přijímání každého právního předpisu je podmíněno řádně provedeným legislativním procesem, který umožňuje zapojení široké skupiny připomínkových míst, stejně jako v tomto případě. Připomínkové místo s vypořádáním souhlasí.
481. Ministerstvo práce a sociálních věcí	D	K návrhu vyhlášky o regulovaných službách <u>K § 4 odst. 1</u> V souvislosti s obecnou poznámkou k návrhu vyhlášky navrhujeme znění tohoto ustanovení navrhované předkladatelem nahradit tak, že kritéria pro identifikaci a určení regulovaných služeb stanoví vláda nařízením.	Neakceptováno Vypořádání připomínky viz výše. Připomínkové místo s vypořádáním souhlasí.
482. Ministerstvo životního prostředí	Z	§15 odst. 2; pro poskytovatele regulované služby v režimu nižších povinností chybí položka „řízení aktiv“, i když v §13 je uvedena povinnost určení primárních aktiv. Pokud pro poskytovatele regulované služby nebudou určena primární a podpůrná aktiva, není možné zavést řízení rizik, a tedy i ostatní opatření následujících za bodem c).	Akceptováno Upraveno v nZKB. Děkujeme za věcnou připomínku. Připomínkové místo s vypořádáním souhlasí.
483. Ministerstvo životního prostředí	Z	Výše uvedená připomínka navazuje, resp. je v rozporu s §58; přestupky, kde je v bodu 2) odst. d), e) uvedeno, že poskytovatel regulované služby v režimu nižších povinností se dopustí přestupku, pokud neidentifikuje všechna primární aktiva, resp. podpůrná aktiva.	Akceptováno Děkujeme Vám za věcnou připomínku. Připomínkové místo s vypořádáním souhlasí.
484. Ministerstvo životního prostředí	Z	Nesouhlasíme s tím, jak je v příloze návrhu vyhlášky implementováno to, že podle směrnice je bez další specifikace výzkum dalším kritickým odvětvím, resp. že je bez další specifikace výzkum a vývoj regulovanou službou.	Akceptováno jinak Odvětví 19. Výzkum, vývoj a vzdělávání, resp. služba 19.1. Výzkum a vývoj nejsou regulovány bez další specifikace, ke specifikaci dochází zkombinováním s

			kritérii poskytovatele regulované služby. Není tedy regulována každá služba výzkumu a vývoje, ale pouze taková služba, která je poskytována specifikovanými osobami. Nad rámec Vaší připomínky došlo k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji. Připomínkové místo s vypořádáním souhlasí.
485. Ministerstvo životního prostředí	Z	Nesouhlasíme s tím, jak je v příloze návrhu vyhlášky definováno to, co je ve směrnici uvedeno v čl. 6 bodě 41 směrnice, resp. jak jsou v návrhu vyhlášky implementovány pojmy výzkumné organizace ve smyslu směrnice (čl. 6 bod 41) a vysoké školy (čl. 2 odst. 5 písm. b) směrnice). Z pohledu na subjekty vyskytující se (bez ohledu na jejich velikost) v seznamu výzkumných organizací vedeném na MŠMT je jasné, že zdaleka ne všechny z nich lze charakterizovat jako důležité subjekty ve smyslu čl. 3 odst. 2 směrnice, případně takové, které naplňují myšlenku recitálu 36 směrnice. Naopak například ne na všech vysokých školách, které jsou středním nebo velkým podnikem, musí být vykonávány jakékoli výzkumné činnosti, natož kritické výzkumné činnosti.	Akceptováno jinak Došlo k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji. Připomínkové místo s vypořádáním souhlasí.
486. Ministerstvo životního prostředí	Z	Nesouhlasíme s tím, že v rozporu s důvodovou zprávou k předkládanému návrhu není v tomto případě velikost podniku tím stěžejním kritériem, ale je to právě existence záznamu v seznamu výzkumných institucí, která – v kombinaci s další podmínkou – činí z těchto subjektů poskytovatele regulované služby v režimu vyšších povinností. Pokud jde o implementaci čl. 2 odst. 2 směrnice, rozhodně nelze o všech těchto subjektech prohlásit, že pro ně platí z písm. b) až e).	Akceptováno jinak Došlo k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji.

			Zahrnutí některých osob do odvětví 19. nad rámec požadavků směrnice NIS2 nepředstavuje provedení čl. 2 odst. 2 písm. b) až e) směrnice, nýbrž národní regulaci nad rámec požadavků směrnice NIS2 (odůvodněnou specifickými národními potřebami; je potřeba myslet na to, že směrnice NIS2 je směrnicí, nikoli nařízením, tzn. členské státy mohou jít nad rámec jejích požadavků, pokud tím není mařen její účel). Čl. 2 odst. 2 písm. b) až e) směrnice jsou provedeny v ustanoveních o kritériích pro určení regulované služby. Připomínkové místo s vypořádáním souhlasí.
487. Ministerstvo životního prostředí	Z	Nesouhlasíme se zařazením veřejných výzkumných organizací do režimu poskytovatele regulované služby vyšší úrovně. <u>Odůvodnění:</u> Návrh zákona by měl zpracovat požadavky směrnice NIS 2 do českého právního řádu jako kompromis balancující mezi potřebou regulovat všechna podstatná odvětví a objektivní schopností členských států zajistit reálný výkon pravidel obsažených v transpozičních národních předpisech. Návrh zákona z povahy věci zasahuje do práv adresátů normy, a je proto koncipován na tzv. dvourychlostním modelu kybernetické bezpečnosti. Poskytovatelé regulované služby jsou v rámci návrhu zákona proto rozděleni do dvou režimů – nižších a vyšších povinností. Zahrnutí nekomerčních výzkumných organizací do národní regulace však představuje národní úpravu nad rámec požadavků směrnice NIS2, i dle důvodové zprávy je relevance výzkumných organizací zaměřených na nekomerční užití výsledků z pohledu bezpečnosti vnitřního trhu nižší. Nicméně výzkumná organizace, jejímž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj za účelem využití tohoto výzkumu pro komerční účely, vysoká škola nebo jiná výzkumná organizace je navržena jako poskytovatel	Akceptováno jinak Výběr služeb a subjektů regulovaných v rámci odvětví 19. Výzkum a vývoj nad rámec požadavků směrnice NIS2 proběhl na základě vyhodnocení aktuální úrovně kybernetické bezpečnosti odvětví, posouzení strategičnosti a relevance subjektů, které by do regulace měly být zařazeny, a v neposlední řadě i po konzultaci se subjekty, na které regulace bude dopadat. Odvětví výzkumu a vývoje je strategickým odvětvím, v němž jsou jednak investovány nemalé veřejné prostředky, na jejichž ochraně má stát logický zájem, jednak v něm vzniká a je uchováváno obrovské množství strategicky cenných informací. Výsledky výzkumů jsou v posledních letech častým terčem kybernetických útoků, jež mají za cíl odcizit dosažené poznatky a využít je buďto komerčně (bez nutnosti financovat jejich legální opatření), nebo pro působení proti zájmům České republiky. S ohledem na skutečnost, že výzkumné instituce a vysoké školy soustřeďují v rámci svých kapacit nadkritické množství materiálních, lidských a finančních zdrojů

	regulované služby v režimu vyšších povinností v případě, že provádí citlivou výzkumnou činnost, nebo většina prováděných výzkumných projektů je financována z více než 50 % z veřejných zdrojů. A díky tomu, že drtivá většina prováděných výzkumných projektů resortních v.v.i. je financována z více než 50 % z veřejných zdrojů, měly by tyto v.v.i. spadat automaticky do režimu vyšších povinností. Resortní výzkumné organizace MŽP neprovádí citlivé výzkumné činnosti, neprovozují velké výzkumné infrastruktury, ani nespádají pod Akademii věd. Primárním cílem jejich existence je provádět nezávisle především aplikovaný výzkum a experimentální vývoj v oblasti ochrany životního prostředí a veřejně šířit výsledky těchto činností formou výuky, publikací nebo transferu znalostí. Podstatné v této věci také je, že všechny náklady, které přímo souvisí s výzkumnou činností jsou účtovány přímo k projektům, k nimž patří. Kromě přímých nákladů vznikají v souvislosti s výkonem činností i náklady nepřímé (tzv. režijní). Do režijních nákladů se započítávají náklady spojené se zajištěním provozu objektu instituce (elektrická energie, zemní plyn, vodné, stočné, povinné revize, daň z nemovitosti, ostraha), osobní náklady zaměstnanců zajišťujících řízení a provoz instituce, materiálové náklady zaměstnanců zajišťujících řízení a provoz instituce, odpisy investičního majetku, poštovné, telekomunikační poplatky, pojištění majetku, bankovní poplatky a samozřejmě i náklady na IT infrastrukturu včetně zajištění její bezpečnosti. Přípustná výše nepřímých nákladů se liší dle typu projektu a poskytovatele, většinou je ale ve výši 20 % z celkových či 25 % z přímých nákladů projektu. V posledních letech je ale snahou poskytovatelů účelové podpory tyto režijní náklady snižovat, požadavky na v.v.i. i legislativní povahy ale neustále rostou. Důvodová zpráva uvádí velmi hrubé odhady nákladů na zavedení a následné provádění bezpečnostních opatření pohybující se přibližně mezi 800 tis. Kč a 1,5 mil. Kč vůči jednomu zabezpečovanému systému. Dále uvádí, že podstatnou proměnnou celkových nákladů bude především to, jaký je daný počet jednotlivých systémů u každé	potřebných pro dosahování průlomových poznatků, které přinášejí znalostní řešení socioekonomických výzev, je tak veřejný zájem na zajištění dostatečné úrovně jejich kybernetické bezpečnosti zcela zřejmý a odůvodněný. Zároveň však došlo k přehodnocení rozřazení regulovaných subjektů do jednotlivých režimů a také k redukci regulovaných osob. Došlo tedy k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji. Kritérium financování z veřejných zdrojů však zůstalo zachováno, a to právě za účelem ochrany veřejných prostředků investovaných do výzkumné činnosti. Připomínkové místo s vypořádáním souhlasí.

		konkrétní organizace a také, že takový násobek výše uvedené částky bude potřeba daným organizacím alokovat v rámci veřejných rozpočtů. Tato skutečnost by měla, též v kontextu přijímání úspor státního rozpočtu, významný negativní vliv na rozsah a kvalitu činností resortních výzkumných organizací, kdy se převážně jedná o činnosti pro podporu výkonu státní správy. V konečném důsledku by tedy tato úprava měla negativní dopad na kvalitu výkonu státní správy v resortu MŽP a omezila by plnění prioritních úkolů na ochranu životního prostředí, které vyplývají ze složkových zákonů nebo usnesení vlády (a obdobně i v jiných resortech). Pro představu v rámci běžné v.v.i. může jít hrubě o 20 systémů, tedy náklady dle odhadů NÚKIB někde mezi 16 až 30 mil. Kč ročně. Realitou je však také nižší vyspělost resortních v.v.i. v kybernetické bezpečnosti obecně (dosud jsou v tomto ohledu bez regulace), z čehož se dá odhadnout, že náklady na jejich zabezpečení budou spíše odpovídat vyšším odhadům NÚKIB.	
488. Ministerstvo životního prostředí	D	K §27; žádáme o upřesnění, které regulované služby jsou strategicky významné. Z §27 odst. 1 vyplývá, že je celá veřejná správa zařazena automaticky mezi poskytovatele strategicky významné služby. Odstavec 2 poté sděluje určování případné strategicky významné služby ze strany NÚKIB – odstavec 2 je tedy vztažen pouze na subjekty mimo odstavec 1?	Vysvětleno - nyní § 28 Z § 28 odst. 1 návrhu zákona vyplývá pouze tolik, že veřejná správa je jedním z odvětví, v nichž mohou být identifikovány strategicky významné služby při splnění kritérií pro identifikaci strategicky významné služby. Konkrétní kritéria pro identifikaci strategicky významné služby v odvětvích uvedených v § 28 odst. 1 návrhu zákona jsou definovány v návrhu prováděcího právního předpisu, a to v návrhu vyhlášky o regulovaných službách. Teprve pokud regulovaná služba v odvětví veřejné správy naplní kritéria uvedená v návrhu vyhlášky o regulovaných službách, bude identifikována jako strategicky významná služba. Na základě § 28 odst. 2 návrhu zákona může být regulovaná služba, která nesplňuje kritéria pro identifikaci strategicky významné služby, určena strategicky významnou na základě rozhodnutí

			Úřadu při splnění kritérií uvedených v tomto ustanovení. Tímto způsobem jsou doplněna dopředu stanovená kritéria pro identifikaci strategicky významné služby a je upravena možnost Úřadu vyhodnotit okolnosti konkrétního případu a rozhodnout, že jsou naplněny důvody pro určení strategicky významné služby. Připomínkové místo s vypořádáním souhlasí.
489. Ministerstvo životního prostředí	D	K §32 odst. 3 doporučujeme upřesnit a sjednotit uvedena evidence dodavatelů bezpečnostně významných dodávek. Dodavatel bezpečnostně významných dodávek je synonymum významného dodavatele z §2 odst. 2 písm. h)? Nebo je to jiný dodavatel?	Vysvětleno - nyní § 33 Jedná se o dva odlišné pojmy, kdy každý se vztahuje k jiné problematice návrhu zákona. Významný dodavatel je definován v § 2 odst. 2 písm. h) návrhu zákona. Vztahuje se na něj speciální úprava obsažená v § 26 návrhu zákona a dále se s ním pracuje v návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. Pojem dodavatel bezpečnostně významné dodávky je využíván v rámci mechanismu prověřování bezpečnosti dodavatelského řetězce a je definován v § 29 odst. 3 písm. c) návrhu zákona. Přestože se jedná o dva odlišné pojmy, nelze vyloučit, že významný dodavatel dle § 2 odst. 2 písm. h) nebude současně i dodavatelem bezpečnostně významné dodávky podle § 29 odst. 3 písm. c). Dle § 48 odst. 2 návrhu zákona Úřad povede evidenci dodavatelů bezpečnostně významných dodávek, nikoliv evidenci významných dodavatelů. Připomínkové místo s vypořádáním souhlasí.
490. Ministerstvo životního prostředí	D	K § 40 odst. 1 písm. d) žádáme o vysvětlení nařízení práce v pohotovostním režimu ředitelem Úřadu. Jakých osob by se mohlo dotknout a jak je definován	Vysvětleno - nyní § 41 Obsah ustanovení byl v rámci spolupráce s gestorem problematiky krizového řízení - Ministerstvem vnitra,

		pohotovostní režim?	Generálním ředitelstvím Hasičského záchranného sboru upraven. Ustanovení bylo po konzultaci s gestorem upraveno na nařízení pracovní pohotovosti konkrétním zaměstnancům zaměstnavatele po konzultaci se zaměstnavatelem, přičemž nařízení pracovní pohotovosti je možné pouze v případě, že je to nezbytné k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru. Připomínkové místo s vypořádáním souhlasí.
491. Ministerstvo životního prostředí	D	Jestliže je v §15, odst. 2, bod a) uvedeno „ <i>zajišťování minimální úrovně KB</i> “, měla by být tato minimální úroveň srozumitelně prezentována.	Vysvětleno V současnosti je v praxi ustálené slovní spojení - systém řízení bezpečnosti informací, které je známo i pod anglickou zkratkou ISMS. S tímto pojmem pracuje vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti a nově se bude týkat režimu vyššího. Jedná se o systematický přístup k zavádění bezpečnostních opatření v organizaci. Režim nižší bude mít vyhláškou dány povinnosti, jejichž smyslem je rovněž zavedení bezpečnostních opatření v organizaci, nicméně funguje na odlišném principu od ISMS, a proto byl vytvořen pojem, který bude tento postup zastřešovat a to zajišťování minimální úrovně KB. Nový pojem byl vytvořen především se záměrem zpřehlednění a odlišení obou vyhlášek. Dále je toto popsáno v odůvodnění vyhlášky pro režim nižší. Připomínkové místo s vypořádáním souhlasí.
492. Ministerstvo životního prostředí	D	Na rozdíl od definice citlivé výzkumné činnosti, kterou návrh vyhlášky definuje, není jasné, co to znamená „ <i>většina prováděných výzkumných projektů</i> “. Většinou se rozumí více než 50 % z počtu výzkumných projektů řešených v referenčním roce? Pokud se projektem rozumí to, co je vysoutěženo jako projekt, bez zohlednění jeho dílčích částí (podprojektů, pracovních balíčků), které jsou ale	Akceptováno jinak V návaznosti na připomínku dojde k úpravám kritéria poskytovatele regulované služby, zejm. k časovému ukotvení posuzovaných kritérií a redefinici projektů, které bude potřeba zvažovat. Prováděcí předpisy k

		zohledňovány při vykazování spotřebovaných nákladů poskytovateli, pak počet takto podpořených projektů se mění každý rok. Bylo by vhodné použít exaktnější kritérium, zohledňující např. podíl veřejných prostředků na zdrojích získaných organizací na realizaci činností podle zřizovací listiny (hlavní činnosti, další činnosti, jiné činnosti) za nějaké referenční období. Každopádně fakt, že je subjekt příjemcem jakéhosi množství veřejných prostředků, nepovažujeme za relevantní kritérium, především v porovnání s prováděním citlivé výzkumné činnosti.	návrhu zákona budou mít vlastní připomínkové řízení, ve kterém bude možné upravené znění připomínkovat. Připomínkové místo s vypořádáním souhlasí.
493. Ministerstvo životního prostředí	D	Oproti definici citlivé výzkumné činnosti, kterou návrh vyhlášky definuje, není jasné, co znamená „<i>veřejné zdroje</i>“. Veřejnými zdroji se pro účely tohoto zákona rozumí pouze veřejné zdroje rozdělované podle zákona č. 130/2002 Sb. tj. zdroje, které pocházejí ze státního rozpočtu ČR? Nebo se jimi pro účely navrhovaného zákona rozumějí i zdroje ze zahraničních programů, které však také často pocházejí z veřejných zdrojů, ovšem ne na úrovni státního rozpočtu ČR, ale např. na úrovni EU? Podíl projektů podpořených z veřejných prostředků ČR a z jiných veřejných prostředků se mění každý rok.	Vysvětleno Veřejnými prostředky se rozumí obecně prostředky z veřejných rozpočtů, lhostejno, zda jde o národní rozpočet nebo financování z fondů EU. S ohledem na rozmanitost financování a veřejných zdrojů a jejich proměnlivost v čase nepovažujeme za vhodné je na úrovni zákona blíže specifikovat. Pro přehlednost a posílení právní jistoty adresátů normy bude doplněna důvodová zpráva. Připomínkové místo s vypořádáním souhlasí.
494. Asociace krajů	Z	K vymezení pojmů - § 2 (úprava definici pojmu "dostupnosti, důvěrnosti a integrity informací a dat" na "dostupnosti, důvěrnosti, integrity, authenticity-originalita") Navrhovaná definice obsahující "dostupnost, důvěrnost a integritu dat" nepokrývá identifikaci, autentizaci, autorizaci jako metody zajišťující základní kontroly přístupu, stejně jako některé další služby související s digitálním podpisem. Vysvětlení: Autenticita-originalita - prokazatelnost místa, času nebo zdroje původu informací.	ROZPOR Neakceptováno Nahrazení CIA modelu jiným konceptem je na NÚKIB pravidelně diskutovaná otázka a prozatím jsme vždy došli k závěru, že je stávající pojetí dostatečné. Zákon o kybernetické bezpečnosti má sloužit jako univerzální předpis řešící kybernetickou bezpečnost různých druhů služeb, které reguluje. Navrhované doplnění se v převážné míře váže na oblast digitálních podpisů nebo obecně služeb vytvářejících důvěru a upravuje trochu jinou otázku, než která je předmětem úpravy kybernetické

			bezpečnosti v navrhovaném zákoně. Legislativa, která odvětví služeb vytvářejících důvěru reguluje, však i nadále zůstává v platnosti (pouze část kybernetické bezpečnosti je nově přenesena do zákona o kybernetické bezpečnosti), problematiku jdoucí nad rámec zákona o kybernetické bezpečnosti tedy budou i nadále řešit k tomu příslušné předpisy a příslušní regulátoři.
495. Asociace krajů	Z	K § 14, § 16, - úprava časového rámce pro implementaci opatření nejpozději do 1 roku na nejpozději do 18 měsíců Navrhovaný časový rámec je pro nové subjekty, které budou spadat pod regulaci velice krátký, ať s ohledem na finanční zdroj tak také na zajištění lidských zdrojů.	ROZPOR Neakceptováno Subjekty budou zjišťovat naplnění identifikačních kritérií regulovaných služeb, na základě čehož budou provádět registraci daných služeb. Teprve od doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb začnou subjektům běžet lhůty pro plnění povinností. Pro zavádění bezpečnostních opatření se tak jedná o lhůtu 12 měsíců. Se stejnou délkou přitom rovněž pracuje současná právní úprava. Regulované subjekty pak mají další nástroje, jak s nově nabytými povinnostmi pracovat. Jedná se například o plán zvládání rizik, který subjektům umožňuje postupné zavádění bezpečnostních opatření. Dle našeho názoru je proto lhůta přiměřená.
496. Asociace krajů	Z	K § 2 odst. 1 písm. b) - primárním aktivem jsou data, informace, služby a procesy Srovnání dat a informace nejsou korektní, data mohou a nemusí nést část informace. Současně informace bude vždy složena z dat. Data jsou fakta, která se stávají informacemi tehdy, pokud jsou vnímána či vyjádřena v kontextu a nesou význam, který je pochopitelný pro lidi.	ROZPOR Akceptováno Vracíme se k původní definici primárního aktiva.
497. Asociace krajů	D	K § 2 odst. 1 písm. b) provozní údaje	Akceptováno

		Není pochopitelné jaké provozní údaje jsou myšlena. Provozní údaje mohou mít různý význam, od množství provedených snímků na RTG, datasheety, provozní údaje ze zákona o elektronických komunikacích, apod.	Aktuální znění definice primárních aktiv již nezahrnuje provozní údaje. Její znění po zapracování vícero připomínek bylo upraveno, aktuálně jsou "primárním aktivem informace a služby,". Vysvětlení použití této definice je v důvodové zprávě. Připomínka vypořádána.
498. Asociace krajů	D	K § 2 - definice významný dopad Není jasné co je definováno jako významný dopad. Pojem je uveden ve vyhláškách, ale není v zákoně.	Akceptováno jinak Přístup k výkladu neurčitých právních pojmů použitých v návrhu zákona byl doplněn do důvodové zprávy v tom smyslu, že jejich obecná definice není právě s ohledem na jejich charakteristiku coby neurčitých právních pojmů a současně univerzální aplikovatelnost na skutkově zcela odlišné situace žádoucí (nadto např. pojem významný dopad je v rámci zákona používán pro různé situace a v závislosti na místě jeho použití nabývá v jednotlivých částech zákona odlišných významů). Jakákoli definice, o kterou by se předkladatel návrhu zákona pokusil, by z povahy věci musela poměrně obecná (aby pokryla všechny zamýšlené situace) a nepřinášela by adresátům normy žádnou přidanou hodnotu. Tam, kde je to možné a vhodné, jsou pojmy buďto vysvětleny v prováděcích předpisech, nebo jsou blíže přiblíženy v důvodové zprávě. Blížší výklad těchto pojmů pak bude prováděn v závislosti na konkrétních skutkových okolnostech posuzovaného případu. Obecně však tyto pojmy slouží k vydefinování situací, které dosahují natolik významné intenzity, že stát považuje za nezbytné je podřadit pod zákonnou regulaci. Připomínka vypořádána.

499. Asociace krajů	D	K §2 vymezení pojmů Požadujeme vymezit všechny pojmy, které jsou v návrhu uvedené - například dodavatel bezpečnostně významné dodávky, bezpečnostně významná dodávka, informační a komunikační služby (§ 28 odst 3b) a další.	Neakceptováno Zmíněné pojmy jsou definovány vždy pro potřeby použití v dané části zákona, v tomto případě konkrétně pro potřeby využití v mechanismu prověřování dodavatelského řetězce. Oba zmíněné pojmy jsou v §29 popsány a vysvětleny tak, aby jejich využití v mechanismu prověřování dodavatelského řetězce bylo jasné a bezproblémové. Jejich definování na úrovni §2 (Definice) není účelné, neboť návrh zákona jako takový nemá ambici ani potřebu definovat tyto pojmy mimo specializovaný prostor, kde je tomu potřeba (tj. pro potřeby mechanismu prověřování dodavatelského řetězce). Připomínka vypořádána.
500. Asociace krajů	Z	K § 2 Požadujeme definovat "důležité společenské nebo ekonomické činnosti". Směrnice hovoří v některých částech o "kritické společenské nebo hospodářské činnosti." Dle našeho názoru je "kritické" daleko užší rozsah než "důležité".	ROZPOR Akceptováno jinak Děkujeme za upozornění. Takovéto stanovení poskytovatele regulované služby je odpovídající, neboť národní právní úprava může (i v souladu se směrnicí) stanovit okruh povinných subjektů širěji, než jak stanovuje směrnice. Z tohoto důvodu také není možné využít stejné pojmosloví. Na místo rozvedení definice v § 2 došlo k úpravě kritérií v ustanovení o identifikaci regulované služby, což je de facto rozvedením připomínkovaného ustanovení.
501. Asociace krajů	D	K § 5 Požadujeme definovat "významný dopad".	Akceptováno jinak Přístup k výkladu neurčitých právních pojmů použitých v návrhu zákona byl doplněn do důvodové zprávy v tom smyslu, že jejich obecná definice není právě s ohledem na jejich charakteristiku coby

			neurčitých právních pojmů a současně univerzální aplikovatelnost na skutkově zcela odlišné situace žádoucí (nadto např. pojem významný dopad je v rámci zákona používán pro různé situace a v závislosti na místě jeho použití nabývá v jednotlivých částech zákona odlišných významů). Jakákoli definice, o kterou by se předkladatel návrhu zákona pokusil, by z povahy věci musela poměrně obecná (aby pokryla všechny zamýšlené situace) a nepřinášela by adresátům normy žádnou přidanou hodnotu. Tam, kde je to možné a vhodné, jsou pojmy buďto vysvětleny v prováděcích předpisech, nebo jsou blíže přiblíženy v důvodové zprávě. Bližší výklad těchto pojmů pak bude prováděn v závislosti na konkrétních skutkových okolnostech posuzovaného případu. Obecně však tyto pojmy slouží k vydefinování situací, které dosahují natolik významné intenzity, že stát považuje za nezbytné je podřadit pod zákonnou regulaci. Připomínka vypořádána.
502. Asociace krajů	D	K § 6 odst. 3 Režim poskytovatele regulované služby by měl být stanoven přímo v zákoně a nikoli ve vyhlášce, protože vyplývá přímo z transpozice směrnice.	Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech (§ 3 a § 2 písm. d)), tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby (§ 3, ve spojení s § 2 písm. i) a k) a § 22a). Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon (§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)), a to již od své novelizace v roce 2010, přičemž

			opět současný zákon toho také využívá (§ 3 a § 2 písm. b)). Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Připomínka vypořádána.
503. Asociace krajů	Z	K § 8 Identifikace regulované služby V odstavci 2 se uvádí, že "Registraci podle odstavce 1 je poskytovatel regulované služby povinen provést nejpozději do 30 dnů ode dne, kdy zjistí, že došlo k naplnění kritérií pro identifikaci regulované služby, nejpozději však do 90 dnů ode dne, kdy k naplnění kritérií pro identifikaci regulované služby došlo." Navrhujeme, aby tato lhůta byla "90 dnů ode dne, kdy zjistí, že došlo k naplnění kritérií pro identifikaci regulované služby, nejpozději však do 180 dnů..." Nový ZKB dle tezí vyhlášek dopadne a může dopadnout na celou řadu organizací, které kraje zřizují. Předpokládáme, že velká část těchto organizací bude po krajském úřadě požadovat radu a pomoc, protože nebude schopna se svým rozpočtem rychle dosáhnout souladu se zákonem. Požadujeme proto prodloužit délku registrace.	ROZPOR Neakceptováno Jak je uvedeno v důvodové zprávě návrhu zákona: "Ve veřejném zájmu je tak provedení zařazení orgánu nebo osoby do regulace co nejvíce v souladu se zásadou rychlosti a hospodárnosti, neboť neúměrným a nijak účelným prodlužováním celého procesu může být výše zmíněný zájem představující účel tohoto návrhu zákona ohrožen. Do doby registrace a zápisu do evidence poskytovatelů regulovaných služeb tyto orgány nebo osoby nejsou odpovědné za zabezpečování svých systémů a hlášení incidentů. Jakékoli prodlužování procesu zařazení orgánů nebo osob do regulace návrhu zákona oddaluje okamžik, od kterého jsou tyto orgány a osoby odpovědné za zajišťování kybernetické bezpečnosti své organizace a ochranu poskytované služby." K prodloužení uvedených lhůt tudíž nemůžeme přistoupit. Ostatně

			subjekty se se zněním zákona mohou seznamovat již nyní. Následně po účinnosti předpisu budou mít dostatečně dlouhou lhůtu na to vše řádně vyhodnotit.
504. Asociace krajů	Z	K § 10 odst. 2 Požadujeme prodloužit lhůtu na plnění povinností plynoucích ze zákona vůči zapsaným regulovaným službám na minimálně šest měsíců. Je nutné si uvědomit, že směrnice dopadne na řadu krajských příspěvkových organizací, z nichž řada bude v režimu vyšších povinností, např. nemocnice. Pokud má být zabezpečen soulad se Zákonem, je nutné k tomu dát dotčeným orgánům čas a prostor, zvláště pokud bude nutné přijmout nové zaměstnance nebo vysoutěžit externí dodavatele.	ROZPOR Vysvětleno Den doručení písemného vyrozumění o zápisu do evidence regulovaných služeb je rozhodným datem, se kterým celý zákon pracuje i na jiných místech a počítá se od něj běh některých lhůt. Například jedna z hlavních povinností zavádět bezpečnostní opatření má na zavedení podle § 14 odst. 3 návrhu zákona lhůtu v délce jednoho roku a začíná běžet od tohoto rozhodného data. Neplatí tedy, že by tato povinnost začala platit ihned po doručení vyrozumění o zápisu do evidence. Toto ustanovení pouze říká, že od vyrozumění zápisu do evidence platí, že daná služba je regulovanou službou a poskytovatel regulované služby vůči ní musí plnit své povinnosti. Jednotlivé povinnosti pak vyplývají z dalších ustanovení a mají své samostatné lhůty.
505. Asociace krajů	Z	K § 13 odst. 3 Požadujeme vyjmout nutnost evidovat primární aktiva, která byla vyjmuta ze stanoveného rozsahu. Jde o významně administrativně náročný úkon, navíc z hlediska kybernetické bezpečnosti naprosto nadbytečný.	ROZPOR Neakceptováno Stanovený rozsah se vztahuje na aktiva související s regulovanou službou (nikoliv všechna identifikovaná primární aktiva - pokud tedy všechna nesouvisí s regulovanou službou). Je pracováno s typovými aktivy, nikoliv s každou službou/informací jako takovou zvlášť. Jde o základní identifikaci služeb, které organizace poskytuje (za jakým účelem je vytvořena, a co jsou její core služby).

			Primární aktiva, která nesouvisí s regulovanou službou, není potřeba hodnotit (nZKB to nechce). Nepovažujeme tuto změnu při identifikaci aktiv za nepřiměřenou. Je pravda, že v tomto ustanovení se projevují zkušenosti Úřadu z kontrolní činnosti, kdy správně stanovit rozsah ISMS organizacím způsobuje značné problémy. Oproti platné právní úpravě došlo k otočení způsobu identifikace primárních aktiv, na které se nyní pohlíží z pohledu celé organizace a určují se ty, které souvisejí s regulovanou službou. Nesouhlasíme s tím, že pro zajištění kybernetické bezpečnosti současné znění předmětného ustanovení nebude mít vliv, a že se jedná o nepřiměřený zásah do práv povinných subjektů. Naopak naší snahou je zmírnění požadavku NIS2 zavádět opatření na celou organizaci v tom smyslu, že se „první podívám na celou organizaci, ale opatření zavádím na těch aktivech, které se přímo dotýkají poskytování regulované služby“.
506. Asociace krajů	Z	K § 40 odst. 1 písm. d) Není jasné, komu může Úřad nařídít práci v pohotovostním režimu. Požadujeme doplnit a popsat, jak bude procesně takové nařízení práce v pohotovostním režimu vypadat.	ROZPOR Akceptováno - nyní § 41 Obsah ustanovení byl v rámci spolupráce s gestorem problematiky krizového řízení - Ministerstvem vnitra, Generálním ředitelstvím Hasičského záchranného sboru upraven.
507. Asociace krajů	Z	K § 40 odst. 1 písm. h) Není jasné, co je to "neveřejná komunikační síť" - není definovaná v tomto návrhu ani v Zákoně o elektronických komunikacích. Požadujeme doplnit do definic nebo příslušný odstavec odstranit.	ROZPOR Vysvětleno - nyní § 41 Zpřístupněním veřejné sítě v tomto případě není mířeno na její primární užívání Úřadem, nicméně jen jako užívání podpůrné, které bude zpravidla zahrnovat pouze posílání informací, a to v případě, že takové

			informace nebude možné doručit dostatečně rychlým způsobem jinak. Prakticky se tak nemusí stát, aby Úřad měl do takové sítě přístup, nicméně postačí aby mu byla zpřístupněna zprostředkovaně, případně pokud bude zpřístupněna pouze ta část sítě, která je nezbytná k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru za stavu kybernetického nebezpečí. Bezpečnostní politiky by tuto variantu měly zohledňovat. Tato formulace je převzata ze zákon o IZS a vysvětlena v důvodové zprávě.
508. Asociace krajů	Z	Díl 5 jako celek Prověřování bezpečnosti dodavatelského řetězce není součástí směrnice. Požadujeme proto doplnit do RIA, jaký bude dopad na regionální podnikání, především na malé a střední podniky, a na zájem krajů i státu o co nejrychlejší pokrývání regionů vysokorychlostním internetem, a toto posouzení učinit ideálně na základě objektivních dat (např. jakých regionálních a národních poskytovatelů se nové povinnosti dotknou přímo či nepřímo, jaké nyní využívají dodavatele, jací dodavatelé z nich budou s určitou mírou pravděpodobnosti zasaženi opatřením obecné povahy nůkib a podobně).	ROZPOR Neakceptováno Co se týče podnikatelského prostředí obecně, je namístě uvést, že ekonomický dopad zavedení prověřování bezpečnosti dodavatelského řetězce je (společně se všemi dopady pozitivními) podrobně specifikován v bodě 3.3 závěrečné zprávy RIA. S odkazem na poslední zmíněnou pasáž je nicméně nutno zopakovat, že přesnou výši finančních dopadů (včetně finančních dopadů na malé a střední podniky) není možné předem stanovit a veškeré předchozí požadavky na jejich vyčíslení vedly k vytvoření odhadů s nízkou vypovídací hodnotou. Pokud jde o uvedení konkrétních regionálních a národních poskytovatelů, respektive jejich dodavatelů, jedná se o citlivé informace, které Úřad bez dalšího není oprávněn sdělovat.
509. Asociace krajů	Z	Díl 5 jako celek NÚKIB neuvažuje přímé dopady na spotřebitele, ale zároveň uvádí, že lze očekávat tlak regulovaných orgánů na promítnutí nákladů na	ROZPOR Akceptováno

		zavátění bezpečnostních opatření do cen služeb. To je negativní vliv na spotřebitele. Úřad by měl do RIA doplnit odhad toho, jak bude tento potenciální vliv na ceny vypadat, protože regulované služby jsou v odvětvích, která zasahují velkou část společnosti, která je na ceny velmi citlivá (jde např. o energetiku, ale i telekomunikace).	Do závěrečné zprávy RIA bylo v bodě 3.7 Dopady na spotřebitele doplněno zohlednění případného negativního dopadu v podobě nárůstu ceny za poskytované služby.
510. Asociace krajů	Z	K § 28 odst. 3 písm.a) Text odstavce je velmi komplikovaný a obtížně srozumitelný. Požadujeme jej přeformulovat tak, aby bylo jasné, co je vlastně záměrem předkladatele a co chce regulovat a že "kritická část stanoveného rozsahu" je jen úzce konkrétně vymezená část aktiv regulovaného subjektu. Dáváme na zvážení, zda používat "vyhlášku o nepominutelných funkcích". Poskytovatelé strategicky významné služby jsou z několika různých odvětví (energetika, distribuce atd.), ale "nepominutelné funkce" jsou z neznámého důvodu vyjmenované pouze pro telekomunikace. Domníváme se, že sebeidentifikace aktiv dle příslušné vyhlášky (těch, která ohodnotí poskytovatel na úrovni vysoká nebo kritická) postačuje pro všechny odvětví.	ROZPOR Vysvětleno - nyní § 29 Hlavním důvodem, proč je odstavec natextován daným způsobem, je skutečnost, že je nutno zkombinovat vlastní analýzu rizik poskytovatelů strategicky významných služeb s pevně stanovenými nepominutelnými funkcemi, které cílí na veškeré funkce kritické pro fungování veřejných komunikačních sítí. Důvodů, proč je vyhláška o nepominutelných funkcích zaměřena právě na veřejné komunikační síť, je několik. Je to zejména vysoká úroveň standardizace v rámci mezinárodních organizací a vysoká komplexita topologie telekomunikačních sítí, kdy je nasnadě určit to nejkritičtější v rámci jádra sítě a dalších částí sítě. Telekomunikace mohou navíc způsobit tzv. kaskádový efekt, kde znefunkčnění telekomunikací může způsobit ochromení dalších, na telekomunikace navázaných strategicky významných služeb. Z toho důvodu NÚKIB považuje za nutné vedle analýzy rizik jednotlivých subjektů určit funkce, u nichž nesmí dojít ke kompromitaci, jinak hrozí znefunkčnění sítě. Obdobný přístup zvolilo například Dánsko, Belgie či Finsko. Jedná se o přístup založený na identifikaci všech rizikových funkcí/komponent pro funkčnost sítě, nehledě na jejich umístění v rámci jádra či rádiové přístupové sítě.

511. Asociace krajů	Z	K § 28 odst. 3 písm. c) Obáváme se, že takto široké pojetí pojmu "dodavatel" ve spojení s poměrně širokým pojetím "kritické části stanoveného rozsahu" tak, jak jsme to pochopili z odstavce 3a) (pokud se podíváme na návrh vyhlášky o nepominutelných funkcích, tak nepominutelnou funkcí je např. takřka celá síť telekomunikačního operátora) způsobí, že mechanismus dopadne takřka na každého dodavatele velkých operátorů, kteří jsou subjektem mechanismu dle vyhlášky. Regulovanými subjekty tak budou stovky malých a středních regionálních operátorů, jejichž normální činností je poskytování služeb elektronických komunikací v regoínech. Kromě již tak komplikovaného plnění regulačních povinností ze zákona (protože na odvětví elektronických komunikací se směrnice vztahuje bez ohledu na velikost podnikatele) budou mít další povinnosti, které na ně přenesou jejich zákazníci. Navrhujeme proto lépe definovat, kdo je dodavatel a kdo poddodavatel a ideálně "kritickou část stanoveného rozsahu" omezit tak, aby zahrnovala skutečně jen kritické části sítě operátora s celonárodní působností (např. jádro sítě 5G) a nezahrnovala okrajové části sítě, které nejsou z hlediska kybernetické bezpečnosti tak kritické. Úřad by měl také do důvodové zprávy doplnit mezinárodní srovnání obdobných úprav v ostatních zemích EU.	ROZPOR Neakceptováno – nyní § 29 K uvedenému je nutno dodat, že z hlediska strategické bezpečnosti státu plynou ze strany dodavatele i poddodavatele totožná rizika, jelikož ti mají v rámci bezpečnosti dodavatelského řetězce obdobné možnosti zásahu/vlivu do bezpečnostně významných dodávek. Z tohoto důvodu je zákonná šíře taková, jak je uvedena v § 29. Co se týče rozsahu chráněných aktiv, tak konkrétně nepominutelné funkce chrání vše, co je kritické pro fungování telekomunikačních sítí, a to neohledně na umístění těchto funkcí v rámci topologie sítě. Obdobnou úpravu, kdy je chráněno vše kritické, ať už se jedná o jádro či rádiovou přístupovou síť, má například Belgie, Dánsko, Litva či Finsko. K tomuto je nutno dodat, že kompromitace funkcí, které jsou popsány vyhláškou o nepominutelných funkcích a jsou součástí rádiové přístupové sítě, může způsobit znepřístupnění jádra sítě, a tím pádem znefunkčnění celé sítě.
512. Asociace krajů	Z	Současný návrh §37 navrhujeme dát pod odst. 1 a dále přidat odst.2 ve znění: <i>V případě, že je subjekt regulovaný tímto zákonem požádán jiným subjektem z jiného legislativního důvodu o informaci, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost bezpečnostního opatření podle tohoto zákona, musí žadatel písemně garantovat a případně na žádost Úřadu i prokázat stejnou nebo vyšší míru ochrany obdržených informací, která mu byla poskytovatelem těchto informací předána a jejichž míra ochrany informací byla poskytovatelem viditelně označena.</i> Považujeme rozsah paragrafu §37 za nedostatečný a námi navržený	ROZPOR Neakceptováno - nyní § 38 Děkujeme za podnět - i když velmi souhlasíme s navrhovaným záměrem a zpracování koncepce ochrany neutajovaných informací citlivé povahy (což je v zásadě podstata této připomínky) má NÚKIB také jako úkol v Akčním plánu k aktuální Strategii kybernetické bezpečnosti České republiky, nepovažujeme zrovna toto doplnění jako vhodné. Za prvé není směřováno do vhodného ustanovení, ale co je podstatnější, není dostatečně legislativně

		přidaný text má za úkol ošetřit předávání informací (či dokumentací) při meziresortních komunikacích, např. kontrolách, které probíhají podle jiného zákona a kde musí poskytovatel předat velkou míru informací, které sám považuje za důležité, ale žadatel již dle svého uvážení ne.	zpracováno a nejsou v něm domyšleny všechny potřebné detaily. NÚKIB sám v rámci přípravy tohoto návrhu obdobné ustanovení zamýšlel, nicméně v rámci aktuálně připravované koncepce existuje stále řada nedořešených otázek, pro které není vhodné obdobné ustanovení nyní do návrhu zavádět. Stanovení takového pravidla je potřebné, nicméně v rámci českého právního prostředí se jedná o samostatný velký projekt. Bude tedy potřeba pro tuto chvíli ještě k předávání informací přistupovat jako doposud, tedy nejlépe podmiňovat předání požadavky odpovídajícími nastavení kybernetické bezpečnosti v dané organizaci, tj. využívat systém řízení bezpečnosti informací zavedený v dané organizace podle současného zákona o kybernetické bezpečnosti, resp. vyhlášky o kybernetické bezpečnosti (analogicky platí v tomto návrhu).
513. Asociace krajů	Z	K § 45 odst. 2 Navrhujeme změnu: <i>Úřad poskytuje v odůvodněných případech údaje z evidencí orgánům veřejné moci na jejich žádost, je-li to nezbytné pro výkon jejich působnosti. Poskytnuté údaje je možné využít jen pro potřeby, které byly uvedeny v žádosti. Úřad označí vydávané údaje viditelně doporučenou úroveň ochrany informací a žadatel vynaloží přiměřené úsilí k zajištění bezpečnosti informací takto poskytnutých údajů.</i> Popsané povinnost při předávání informací neveřejného charakteru považujeme v návrhu tohoto zákona obecně za nedostatečný. Uvedenou textaci lze pouze jednou použít i jako rozšíření §66.	ROZPOR Neakceptováno - nyní § 48 Stejně jako u další připomínky týkající se ochrany neutajovaných informací Vám bohužel musíme odpovědět, že byť souhlasíme s navrhovaným záměrem a zpracování koncepce ochrany neutajovaných informací citlivé povahy má NÚKIB jako úkol v Akčním plánu k aktuální Strategii kybernetické bezpečnosti České republiky, nepovažujeme zrovna toto doplnění za vhodné. Připomínka není dostatečně legislativně zpracována a nejsou v ní domyšleny všechny potřebné detaily. NÚKIB sám směřuje k tomu, aby byla koncepce ochrany neutajovaných informací stanovena v zákoně, avšak v rámci aktuálně připravované koncepce existuje stále řada nedořešených otázek, pro které není

			vhodné obdobné ustanovení teď do návrhu zavádět. V rámci českého právního prostředí se jedná o samostatný velký projekt. Bude tedy potřeba pro tuto chvíli ještě k předávání informací přistupovat jako doposud. Samotný NÚKIB má interně nastavenou koncepci, kterou se řídí a využívá systém řízení bezpečnosti informací.
514. Asociace krajů	D	K § 45 odst. 3 Navrhujeme změnu: <i>Úřad může v odůvodněných případech poskytovat údaje z evidencí Národnímu CERT, orgánům nebo osobám vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným orgánům nebo osobám působícím v oblasti kybernetické bezpečnosti v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru. V takovém případě Úřad viditelně označí poskytované informace doporučenou úrovní bezpečnosti informací a v nejvyšší možné míře po žadatelích dodržování této bezpečnosti informací vyžaduje.</i> Popsané povinnost při předávání informací neveřejného charakteru považujeme v návrhu tohoto zákona obecně za nedostatečný. Uvedenou textaci lze pouze jednou použít i jako rozšíření §66.	Neakceptováno - nyní § 48 Stejně jako u připomínky k § 37 (nyní § 38) Vám bohužel musíme odpovědět, že byť souhlasíme s navrhovaným záměrem a zpracování koncepce ochrany neutajovaných informací citlivé povahy má NÚKIB jako úkol v Akčním plánu k aktuální Strategii kybernetické bezpečnosti České republiky, nepovažujeme zrovna toto doplnění za vhodné. Připomínka není dostatečně legislativně zpracována a nejsou v ní domyšleny všechny potřebné detaily. NÚKIB sám směřuje k tomu, aby byla koncepce ochrany neutajovaných informací stanovena v zákoně, avšak v rámci aktuálně připravované koncepce existuje stále řada nedoručených otázek, pro které není vhodné obdobné ustanovení teď do návrhu zavádět. V rámci českého právního prostředí se jedná o samostatný velký projekt. Bude tedy potřeba pro tuto chvíli ještě k předávání informací přistupovat jako doposud. Samotný NÚKIB má interně nastavenou koncepci, kterou se řídí a využívá systém řízení bezpečnosti informací. Připomínka vypořádána.
515. Asociace krajů	Z	K § 43 odst. 2 U §43 odst 2) nekonkretizovat složení kontrolní komise, ale odkázat se na jiný právní předpis.	ROZPOR Vysvětleno - nyní § 46

			Jednací řád Poslanecké sněmovny rozlišuje 3 druhy komisí, které může Poslanecká sněmovna zřizovat. Jedná se za prvé o komise, které jsou zřizovány podle jednacího řádu, za druhé o komise zřizované na základě zvláštních zákonů a za třetí komise vyšetřovací, jejichž postavení upravuje přímo Ústava. V tomto případě se jedná o komisi zřízenou na základě zvláštního zákona - nZoKB (dostupné z https://www.psp.cz/sqw/hp.sqw?k=195).
516. Asociace krajů	Z	Obecně NUKIB vůbec neprovedl dopad na regulované subjekty, toto by se mu mělo vytknout a mělo by se požadovat doplnění důvodové zprávy. Není naprosto jasné jak povinnosti dopadnou na obce, kraje, jimi zřizované organizace atd atd, není tam žádná analýza nákladů, vůbec nic. V podstatě se vysmáli metodice pro RIA. Například: § 15 – Seznam bezpečnostních opatření – pro vyšší i nižší povinnosti je stanoveno, že jsou bezpečnostními opatření „bezpečnost lidských zdrojů“– a contrario ke stanoveným: řízení přístupu, řízení rizik, řízení identit a jejich oprávnění atd. nerozumím, co tím myslí. V důvodovce jsem k tomu nic nenašla. Co to má na obci znamenat? K § 15 - v zákoně je jenom výčet bezpečnostních opatření. Ve vyhláškách je pak specifikované, co je tím konkrétně myšleno (§ 11 vyšších povinností a § 6 nižších povinností). V podstatě každá ORP (= nižší povinnosti) bude muset plnit toto: § 6 Bezpečnost lidských zdrojů Povinná osoba v rámci bezpečnosti lidských zdrojů a) stanoví politiku bezpečného chování uživatelů, v rámci které zohledňuje relevantní témata uvedená v příloze č. 4 této vyhlášky, b) stanoví pravidla rozvoje bezpečnostního povědomí, včetně pravidel pro tvorbu hesel dle § 9,	ROZPOR Vysvětleno Asi nerozumíme přesně tomu, které povinnosti autor postrádá. Z textace připomínky je patrné, že se její autor zorientoval jak v zákoně samotném, tak i ve vyhláškách, které jej zpřesňují. To je tedy onen rozsah povinností. Kategoricky nesouhlasíme s autorovým závěrem v otázce hodnocení dopadů provedených Úřadem, Hodnocení dopadů obsahuje hodnocení nákladů z několika různých zdrojů. Veškeré zdroje, metodiky i důvody pro problematičnost stanovení konkrétního výpočtu, který připomínkové místo požaduje, jsou uvedeny napříč hodnocením dopadů, zejm. v kapitole 3.1, resp. ve všech odkazovaných metodikách, ze kterých je výpočet složen. Nad to bylo úřadem provedeno ještě další šetření. Metodika tohoto šetření nevznikala „na zelené louce“, ale vycházela z metodik dříve prováděných průzkumů NUKIB a Ministerstva vnitra, které zjišťovaly potřebu finančních zdrojů na kybernetickou bezpečnost pro státní úřady, ministerstva a Úřad vlády ČR. V přípravné fázi byla podoba celého výzkumu včetně teoretických východisek konzultována na jednáních se Svazem

	c) v souladu s pravidly rozvoje bezpečnostního povědomí provádí vstupní školení v oblasti kybernetické bezpečnosti, d) v souladu s pravidly rozvoje bezpečnostního povědomí provádí pravidelná školení v oblasti kybernetické bezpečnosti, e) v rámci školení podle písm. c) a d) zohledňuje relevantní témata uvedená v příloze č. 4 této vyhlášky, f) vede přehledy o školeních podle písm. c) a d), g) zajistí potřebná odborná teoretická i praktická školení administrátorů a osoby odpovědné za kybernetickou bezpečnost v souladu s jejich pracovní náplní, h) zajistí kontrolu dodržování bezpečnostní politiky a i) určí pravidla a postupy pro řešení případů porušení stanovených pravidel. Zároveň ale podle § 4 musí povinná osoba vést dokumentaci zahrnující oblasti uvedené v příloze 2, a tam je zároveň další bezpečnost lidských zdrojů: 1. Politika bezpečnosti lidských zdrojů a) Pravidla rozvoje bezpečnostního povědomí a evidence přehledů o školeních. b) Bezpečnostní školení nových zaměstnanců. c) Stanovení periody pro pravidelná školení. d) Pravidla pro řešení případů porušení bezpečnostní politiky.	průmyslu a dopravy, Svazem měst a obcí a Ministerstvem vnitra ČR. Členové výše zmíněných organizací a státní úřady měli možnost se k celému výzkumu s předstihem dostatečně vyjádřit, což v několika případech rovněž udělali. Četné připomínky byly do podoby dotazníkového šetření implementovány. Nicméně ve fázi provádění samotného průzkumu, zaslalo výsledky jen velmi malé procento subjektů oslovených prostřednictvím výše zmíněných organizací. Použitá metodika byla maximálně zaměřena na novou podobu připravované regulace, zohledňovala jak náklady na jednotlivá bezpečnostní opatření, tak otázku personálií a ve všech podstatných rysech se shoduje s metodikou Ministerstva průmyslu a obchodu, na kterou připomínka odkazuje. Uvedené hodnocení dopadů je dostatečné. Závěrem bychom rádi doplnil, že pokud má autor další dotazy nebo potřebuje s výkladem, ať už současného zákona, nebo obsahu tohoto návrhu pomoci, vždy se může na Úřad obracet.

		e) Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice I. vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu, II. změna přístupových oprávnění při změně pracovní pozice, III. předání odpovědností při změně pracovní pozice nebo ukončení pracovního vztahu s administrátory nebo osobou odpovědnou za kybernetickou bezpečnost. Pravidla bezpečného chování uživatelů včetně pravidel pro tvorbu hesel. Takže je to poměrně hodně compliance / byrokracie pro všechny povinné subjekty. Přitom podle směrnice ORP / obce nemusí být povinným subjektem podle NIS 2 vůbec - je to jen na národním státu, zda si řekne, že ano. NÚKIB v důvodové zprávě uvádí tuším něco takového, že obce mají s kyberbezpečnostními incidenty "neblahé zkušenosti" bez dalších detailů, o co jde, takže všechny ORP chce mít regulované. Jedná se o naprostou nepřiměřenost požadované regulace, kvůli "neblahým" zkušenostem někollika ORP zatížit vysokou měrou povinností ty, které na KB dbají a podstatně jim navýšit provozní náklady. Pak ještě zkoumáme k § 4, např. vodní hospodářství, odpadové hospodářství, věda, výzkum, vzdělávání, jestli to bude mít dopad i na municipality, resp. i na DSO. Bude to mít dopad, pokud jsou zřizovateli podniků, které jsou ve vyhlášce specifikované jako že budou mít nižší nebo vyšší povinnosti.	

		Respektive dopadne to na tyto podniky, takže jejich zřizovatel bude muset zajistit, že na to tyto podniky / organizace dostanou finance.	
517. Asociace krajů	Z	K návrhu vyhlášky o kybernetické bezpečnosti, §5 Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností přidat text: 8) Zodpovědnost vrcholného vedení za dodržování povinností dle tohoto textu nelze delegovat ani pracovní-právním vztahem. Jedná se o nejčastější způsob zbavení se zodpovědnosti. Po předání povinností pak zase klesá znalost vrcholového vedení o kybernetické bezpečnosti.	ROZPOR Neakceptováno Smysl této povinnosti není ultimativní. Plnění této povinnosti je myšleno obecně. Jedná se o závazek, aby vedení usilovalo o získání/zajištění potřebných zdrojů, jako v jakékoliv jiné oblasti, např. provoz, platy, investice atd. Nikdy nenastane situace, kdy budou prostředky na všechno, proto vedení určuje priority. Zároveň je mířeno na lidské kapacity, aby byly zajištěny role, které se budou kybernetickou bezpečností zabývat, a aby měli na problematiku odpovídající čas (např. 1/5 úvazek manažera kybernetické bezpečnosti pro velkou organizaci nemusí být dostatečný). Nejedná se o absolutní zajištění všech zdrojů, ale maximální snahu a postupné zlepšování. Nejenom v soukromoprávních organizacích, ale i veřejnoprávních, toto ustanovení zakotvuje požadavky na to, aby si vedení uvědomilo závazek a svou vůdčí roli určující směřování systému řízení informační bezpečnosti s ohledem na strategické směřování organizace. Dále je nutné podotknout, že individuální odpovědnost vrcholného vedení, která může v extrémním případě skončit pozastavením výkonu řídicí funkce (§ 63 nZKB), nelze podat vůči osobě vykonávající veřejnou funkci vymezenou funkčním nebo časovým obdobím a obsazovanou na základě přímé nebo nepřímé volby nebo jmenováním podle zvláštních právních předpisů.
518. Asociace krajů	Z	K příloze vyhlášky o regulovaných službách, č. 18	ROZPOR

		Takto vymezený rozsah poskytovatelů regulované služby může dopadnout (převážně zřejmě v podobě nižších povinností) i na celou řadu domovů seniorů, které také poskytují zdravotní péči (a jsou z hlediska počtu zaměstnanců středním podnikem). Bylo to skutečně záměrem navrhovatele?	Vysvětleno. Zařazení podniků ve vybraných odvětvích do režimu nižších, či vyšších povinností se odvíjí zejména od požadavků směrnice NIS2. Směrnice zakotvuje minimální harmonizaci, její požadavky na regulaci středních a velkých poskytovatelů zdravotní péče ve smyslu čl. 3, písm. g) směrnice Evropského parlamentu a Rady 2011/24/EU ze dne 9. března 2011 o uplatňování práv pacientů v přeshraniční zdravotní péči, bez zohlednění dalších charakteristik, proto nelze podkročit. Pokud je domov seniorů poskytovatelem zdravotní péče a počtem zaměstnanců odpovídá střednímu podniku, bude poskytovatele regulované služby v režimu nižších povinností.
519. Asociace krajů	Z	K příloze vyhlášky o regulovaných službách, č. 19 Věda, výzkum a vzdělávání Kraje jsou zřizovateli výzkumných institucí, které jsou vedeny v seznamu výzkumných organizací vedený MŠMT podle §33a zákona č. 130/2002 Sb., o podpoře výzkumu a vývoje. Tyto mají být zařazeny mezi poskytovatele regulované služby v režimu vyšších povinností. Toto je zcela mimo rámec principu proporcionality, protože do takového režimu se dostane např. Hvězdárna Valašské Meziříčí nebo Archeologické centrum Olomouc, které jsou zřizované krajem. Směrnice přitom "Výzkumné organizace" bez dalšího uvádí jako "další kritická odvětví", která mohou být subjektem regulace v režimu nižších povinností. Zároveň z kontextu směrnice (recitál 36) vyplývá, že výzkumné organizace jsou takové, které "by měly být chápány tak, že zahrnují subjekty, které se v podstatné části svých činností zaměřují na provádění aplikovaného výzkumu nebo experimentálního vývoje ve smyslu manuálu Frascati z roku 2015 OECD." Požadujeme tak redefinovat v návrhu vyhlášky identifikaci výzkumných organizací, protože jinak NÚKIB přistupuje např. k historickému výzkumu v	ROZPOR Akceptováno Došlo k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji.

		regionálním muzeu stejně jako k vojenskému výzkumu, což jistě předkladatel nezamýšlel.	
520. Asociace krajů	Z	K návrhu vyhlášky o kybernetické bezpečnosti, § 2 odst. 2 písm. e) Změna textu na: <i>událostí již zrealizovanou nebo právě realizovanou událostí</i> Předkládaný návrh více rozlišuje hrozbu a událost.	ROZPOR Akceptováno jinak Definice kybernetické bezpečnosti události byla změněna na událost, která může nebo mohla vyústit v kybernetický bezpečnostní incident. Za použití této definice jednak není potřeba rozlišovat právě realizovanou událost od zrealizované události, což se může jevit jako složité, a jednak zahrnuje jak zafungování bezpečnostních opatření, které zabránily události vyústit v incident, tak i možnost, že událost v incident vyúští. Rozlišení mezi hrozbou a událostí je pak takový, že hrozba existuje kontinuálně a v incident vyúští využitím zranitelnosti. Okamžik, kdy se tak stane, se nazývá kybernetickou bezpečnostní událostí.
521. Česká národní banka	Z	V § 59 požadujeme odstavec 2 vypustit. Odůvodnění: Právní úprava přestupků obecně vychází z materiálně-formálního pojetí přestupku a případné odchylky od tohoto pojetí, které jsou obecně považovány za nevhodné, musí být dostatečně odůvodněny. Jak vyplývá ze zásad tvorby právní úpravy přestupků zpracovaných Ministerstvem vnitra, přestupkem nemá být jakékoliv porušení právní povinnosti, ale porušení určitým způsobem kvalifikované, resp. dosahující dostatečné intenzity (typové závažnosti). Má jít o jednání, které je podle představy předkladatele v obvyklých (typických) případech natolik závažné, že vyžaduje uplatnění odpovědnosti za přestupek. Z hlediska tvorby práva je však podstatné, že za přestupek by mělo být označeno pouze takové protiprávní jednání, které v typických případech materiálního znaku (společenské škodlivosti) dosahuje. Pokud důvodová zpráva uvádí, že společenská škodlivost je u přestupků podle zákona o kybernetické bezpečnosti dána již	Akceptováno Ustanovení bude vypuštěno. Připomínkové místo s vypořádáním souhlasí.

		samotným naplněním skutkové podstaty přestupku, není žádný důvod se od materiálně-formální pojetí přestupku odchylovat. Důvodová zpráva k § 59 odst. 2 zákona o kybernetické bezpečnosti je identická, jako důvodová zpráva k § 270 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, která byla provedena zákonem č. 183/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích. Vyvratitelná právní domněnka, že čin, který vykazuje formální znaky přestupku podle zákona o zadávání veřejných zakázek, je společensky škodlivý, však byla zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, k 15.7.2023 vypuštěna. Důvodem byla skutečnost, že právní úprava nebyla nezbytná. Pokud považuje předkladatel navrhovanou právní úpravu za nezbytnou, musí takovou nezbytnost dostatečným způsobem odůvodnit.	
522. Česká národní banka	D	Doporučujeme upravit § 18 takto: <i>§ 18 Zvládání kybernetických bezpečnostních incidentů</i> <i>(1) Úřad nebo Národní CERT poskytne bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení podle § 17, nebo podle ustanovení přímo použitelného právního předpisu Evropské unie se srovnatelným účinkem podle § 70, poskytovateli regulované služby své vyjádření ke kybernetickému bezpečnostnímu incidentu.</i> <i>(2) Na žádost dotčeného poskytovatele regulované služby poskytne Úřad nebo Národní CERT metodickou podporu k provádění možných zmírňujících opatření, a případnou další technickou podporu ke zvládání hlášeného kybernetického bezpečnostního incidentu s významným dopadem na poskytovatele regulované služby nebo na kybernetický prostor státu.</i> <i>(3) Každý je povinen poskytnout na výzvu Úřadu nezbytné informace a další nezbytnou součinnost při zvládání kybernetického bezpečnostního incidentu, pokud nelze sledovaného účelu dosáhnout jinak nebo by bylo jinak jeho dosažení podstatně ztížené. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem</i>	Akceptováno jinak Odst. 5 ustanovení § 18 byl upraven následovně: "Odstavce 1 až 4 se při zvládání kybernetických bezpečnostních incidentů nahlášených dobrovolně podle § 16 odst. 5 a incidentů oznámených jiným dozorovým orgánem v souvislosti s plněním povinností podle zvláštního odvětvového předpisu ve smyslu § 71 použijí obdobně." Připomínkové místo s vypořádáním souhlasí.

		<i>uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti.</i> <i>(4) Údaje o kybernetických bezpečnostních incidentech, událostech, kybernetických hrozbách a zranitelnostech jsou vedeny v evidenci podle § 45.</i> <i><u>(5) Odstavce 1 až 4 se při zvládání kybernetických bezpečnostních incidentů nahlášených dobrovolně podle § 16 odst. 5 použijí obdobně.</u></i> Odůvodnění: Dáváme na zvážení doplnění, které zajistí, že se režim § 18 bude vztahovat i na incidenty oznámené poskytovateli regulované služby podle DORA (a případné i jiných obdobných sektorových nařízení podle § 70). Z navrženého znění ZKB se to nezdá vyplývat, když podle § 70 se § 17 neuplatní, tj. neuplatní se ani režim § 18, ledaže by šlo o dobrovolně nahlášený incident.	
523. Česká národní banka	D	V dokumentu „Teze prováděcích právních předpisů k navrhované právní úpravě“ v části „Příloha č. 7 k vyhlášce č. XXXX Sb.“ na straně 67 v písm. n) doporučujeme za slova „<i>odstoupit od smlouvy</i>“ vložit slova „<i>nebo smlouvu vypovědět bez výpovědní doby</i>“. Odůvodnění: S ohledem na účinky odstoupení podle § 2004 odst. 1 občanského zákoníku, ve znění pozdějších předpisů, není odstoupení od smlouvy vždy praktickým řešením (např. u smluv o zavedení informačního systému a jeho následné podpoře) a, s přihlédnutím k dalším ustanovením občanského zákoníku, nemusí být ani řešením možným (např. omezení daná § 2005 občanského zákoníku, ve znění pozdějších předpisů). Je-li účelem vytvoření možnosti okamžitého rozvázání smluvního vztahu s nevyhovujícím dodavatelem, nevidíme důvod, proč by vyhláška nemohla dovolovat i další možné prostředky k dosažení takového účelu. Nad uvedené, protože dané prostředky svým použitím ani nehrozí vytvořit stav nejistoty o právech a povinnostech smluvních stran, je poměrně velká šance, že s jejich použitím nebude oprávněná strana váhat.	Akceptováno Připomínkové místo s vypořádáním souhlasí.

524. Český telekomunikační úřad	Z	K § 28 odst. 3 písm. a) Návrhu Připomínka ČTÚ: ČTÚ navrhuje v § 28 odst. 3 písm. a) Návrhu zrušit slova „vysoká nebo“. Připomínkou navrhovaná úprava promítnutá do úplného znění Návrhu zní: „(3) Pro potřeby mechanismu prověřování bezpečnosti dodavatelského řetězce se rozumí a) kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní ~~vysoká nebo~~ kritická; kritickou částí stanoveného rozsahu jsou vždy alespoň aktiva stanoveného rozsahu strategicky významné služby, která zajišťují nepominutelné funkce stanoveného rozsahu stanovené prováděcím právním předpisem,“. Odůvodnění: ČTÚ se domnívá, že navrhovaná úprava v § 28 odst. 3 písm. a) Návrhu, která zavádí mechanismus prověřování bezpečnosti dodavatelského řetězce s povinností pro poskytovatele strategicky významné služby postupem podle prováděcího právního předpisu, kdy tento má ohodnotit dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní vysoká nebo kritická, je příliš široká, když by navržená právní úprava měla být primárně zaměřena pouze na významné služby s úrovní kritická. Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je vhodné, aby byla možnost státu zakázat vybraného dodavatele, u kterého identifikuje významné hrozby (v případě sítí elektronických komunikací se bude jednat zejména o jádro sítě, nikoli o přístupové části sítě včetně části přípojně).	ROZPOR Neakceptováno - nyní § 29 Co se týče zmíněných aktiv stanoveného rozsahu, která poskytovatel ohodnotil úrovní vysoká (tedy části textu "vysoká nebo"), tak zde, na základě předešlých zkušeností a vlastního sledování, NÚKIB konstatuje, že tato aktiva jsou rovněž kritická pro fungování strategicky významných služeb. Co se týče navýšení hlášení incidentů, tak k tomu dle názoru NÚKIB s nejvyšší pravděpodobností nedojde. Co do ochrany aktiv stanoveného rozsahu, která poskytovatel ohodnotil úrovní vysoká (v rámci připomínky se jedná o část "vysoká nebo"), tak zde, na základě předešlých zkušeností a zkoumání, NÚKIB konstatuje, že tato aktiva jsou kritická pro fungování strategicky významných služeb. Byť by se striktně jazykovým výkladem dalo dovodit, že je možné do kritického rozsahu sítě zahrnout pouze aktiva s dopadem "kritická", nelze tak učinit. Co se týče ochrany aktiv stanoveného rozsahu, u kterých poskytovatel tyto ohodnotil úrovní vysoká (v rámci připomínky se jedná o část "vysoká nebo"), tak zde, na základě předešlých zkušeností a poznání (vyplývajících zejména z kontrolní činnosti NÚKIB), NÚKIB konstatuje, že tato aktiva jsou velmi důležitá až kritická pro fungování strategicky významných služeb. Aktiva ohodnocena jako vysoká mají podstatné dopady na primární aktiva, a tím pádem na chod celé strategicky významné služby. Ochrana pouze kritických aktiv by nebyla v plném rozsahu schopna pokrýt bezpečnost strategicky významné služby v doménách dostupnost, důvěrnost i integrity.

		Při souběhu obou povinností, tj. posuzovat jak strategicky významné služby s vysokou úrovní, tak i s úrovní kritickou může rovněž docházet k významnému navýšení hlášení incidentů. Konkrétně z hlediska bezpečnosti veřejných sítí elektronických komunikací za dostatečné považuje ČTÚ uložení povinnosti poskytovateli strategicky významné služby spočívající v ohodnocení dopadu narušení bezpečnosti informací na stanovený rozsah strategicky významné služby pouze s úrovní, která naplňuje podmínku, že je kritická. Tím bude z pohledu ČTÚ naplněn požadavek přiměřenosti regulace v oblasti kybernetické bezpečnosti a poskytovatelům regulované služby umožní zaměřit se na ochranu jejich aktiv, která jsou nejdůležitější pro bezpečné a spolehlivé poskytování služeb ve veřejné síti elektronických komunikací.	
525. Český telekomunikační úřad	Z	K § 28 odst. 3 písm. a) Návrhu Připomínka ČTÚ: ČTÚ navrhuje doplnit § 28 odst. 3 písm. písm. a) Návrhu, ve znění zásadní připomínky ČTÚ č. 1 k Návrhu tak, že zní: „(3) Pro potřeby mechanismu prověřování bezpečnosti dodavatelského řetězce se rozumí a) kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní ~~vysoká nebo~~ kritická; kritickou částí stanoveného rozsahu jsou vždy alespoň aktiva stanoveného rozsahu strategicky významné služby, která zajišťují nepominutelné funkce stanoveného rozsahu stanovené prováděcím právním předpisem, v případě regulované služby zajišťování veřejné komunikační sítě se nepominutelné funkce stanoveného rozsahu nevztahují k přístupové síti veřejné komunikační sítě a její přípojně části, včetně funkce jejich řízení“. Odůvodnění: V návaznosti na první připomínku ČTÚ, ze které	ROZPOR Neakceptováno – nyní § 29 NÚKIB považuje za nutné chránit veškeré funkce, které jsou považovány za kritické, jelikož kompromitace takových funkcí může způsobit znefunkčnění sítě. K tomuto je nutno dodat, že kritické funkce nemusí být nutně vztaženy pouze na jádro sítě, jelikož další funkce, jako jsou vybrané funkce rádiové přístupové sítě, mnohdy zabezpečují a udržují chod poskytování služeb koncovým uživatelům. Například řízení rádiových stanic představuje prostředek, pomocí kterého se koncoví uživatelé připojují ke službám poskytovaným jádrem sítě. V případě jejich kompromitace tak může být narušeno či zcela porušeno poskytování služeb koncovým uživatelům, včetně strategicky významných služeb. Je pravdou, že jádro sítě je nejzásadnější z hlediska bezpečnosti a integrity sítě a dostupnosti poskytovaných služeb, ale bez zabezpečené rádiové přístupové sítě pozbývá funkční jádro smysl, jelikož nemůže dojít k propojení koncových zařízení s jádrem, což souvisí s nemožností

		vyplývá, že by navržená právní úprava regulace dodavatelského řetězce (§ 28 a násl. Návrhu) měla směřovat v případě regulované služby zajišťování veřejné komunikační sítě do jádra sítě, které je nejzásadnější z hlediska bezpečnosti a integrity sítě a dostupnosti poskytovaných služeb, navrhuje ČTÚ nevztahovat regulaci dodavatelského řetězce, včetně možnosti uložení podmínky nebo zákazu využití plnění dodavatele bezpečnostně významné dodávky opatřením obecné povahy vydaným NÚKIB postupem podle § 30 Návrhu, k přístupové části sítě, včetně části přípojné a funkce řízení těchto částí. Tato technická aktiva mají z hlediska cílů regulace Návrhu nižší význam než kritický. V návaznosti na tuto připomínku bude potřeba touto připomínkou navrženou limitaci zmocnění k vydání prováděcího předpisu promítnout do navazující vyhlášky o nepominutelných funkcích stanoveného rozsahu, jejíž teze jsou připojeny k Návrhu.	zajistit dostupnost. Obdobný způsob ochrany kritických částí funkce, nehledě na jejich umístění v rámci architektury sítě, lze nalézt například v Dánsku, Belgii, Litvě, Rumunsku či Finsku.
526. Český telekomunikační úřad	Z	K § 30 odst. 3 Návrhu Připomínka ČTÚ: ČTÚ navrhuje do § 30 odst. 3 Návrhu za větu první vložit větu, která zní: „Dotýká-li se návrh opatření obecné povahy podle věty první poskytovatelů regulované služby zajišťování veřejné komunikační sítě nebo regulované služby poskytování veřejně dostupné služby elektronických komunikací, Úřad vyzve k vyjádření k návrhu opatření obecné povahy Český telekomunikační úřad.“. Odůvodnění: S ohledem na možný značný zásah podmínek nebo zákazů obsažených v navrhovaném opatření obecné povahy, kterým Úřad (NÚKIB) stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, do plnění povinností podnikatelů v elektronických komunikacích (poskytovatelů regulované služby zajišťování veřejné komunikační sítě nebo regulované služby poskytování veřejně dostupné služby elektronických komunikací) stanovených zákonem o elektronických komunikacích nebo uložených ČTÚ na jeho základě, například plnění povinností a závazků	Neakceptováno - nyní § 31 Nejprve je nutno uvést, že NÚKIB v rámci získávání informací a jiné součinnosti dle navrhovaného zákona spolupracuje s relevantními orgány státu, v případě jednotlivých sektorů pak zákon v podobě, v jaké je dnes, tuto spolupráci předpokládá s regulátory jednotlivých sektorů (např. telekomunikace, doprava, energetika), je-li to v daném případě možné. Toto je zaručeno mimo jiné § 8 odst. 2 zákona č. 500/2004 Sb, správního řádu. Dále je tento postup dán principem dobré správy, kdy NÚKIB pro co nejlepší vyhodnocení situace a možných dopadů počítá s dožádáním informací od relevantních orgánů státu v rámci jednotlivých odvětví. Po schůzce Do ustanovení § 31 byla doplněna součinnost ČTÚ a připomínka byla vypořádána.

		obsažených v přidělu rádiových kmitočtů podle § 22 zákona o elektronických komunikacích, považuje ČTÚ za žádoucí, aby byla dána povinnost Úřadu (NÚKIB) konzultovat navržené opatření obecné povahy s ČTÚ jako regulátorem v oblasti uvedených regulovaných služeb.	Připomínkové místo s vypořádáním souhlasí.
527. Český telekomunikační úřad	Z	K § 37 Návrhu Připomínka ČTÚ: ČTÚ navrhuje upravit § 37 Návrhu tak, že zní: „Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost protipatření vydaného podle tohoto zákona, nebo informace, které jsou vedené v evidencích vedených Úřadem podle § 45, se podle právních předpisů upravujících svobodný přístup k informacím nebo vytváření, správu, provoz, užívání a rozvoj informačních systémů veřejné správy neposkytují.“ Odůvodnění: ČTÚ navrhuje doplnit § 37 Návrhu ve smyslu této připomínky tak, aby komplexněji řešil otázku výjimek z poskytování, resp. uveřejňování informací. Konkrétně navržené doplnění směřuje formou normativního odkazu (obdobně jako v případě zákona č. 106/1999 Sb.) k zákonu č. 365/2021 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a jeho prováděcímu předpisu, které počítají s uveřejňováním dokumentů, které obsahují informace o informačních systémech veřejné správy. Uveřejnění těchto informací (včetně například informací o stavu (nastavení a fungování) systému a budoucího rozvoje informačního systému), by mohlo znamenat riziko, resp. mohlo ohrozit zajišťování kybernetické bezpečnosti u těchto systémů. ČTÚ tak navrhuje z obecného režimu uveřejňování podle předpisů upravujících informační systémy veřejné správy učinit výjimku z důvodů kybernetické bezpečnosti ve smyslu touto připomínkou navržené úpravy, resp. doplnění Návrhu.	Neakceptováno - nyní § 38 Máme za to, že takto kauzální úprava neposkytování informací není v tomto případě vhodná. Přestože chápeme problémy navrhovatele, není výjimka v § 38 podle původního návrhu postavena takovýmto způsobem - vedle zákona o ISVS je pak celá řada dalších předpisů, které by takto výslovně mohly být uvedeny, pokud by se připomínka přijala. V zásadě jde také o to, že pokud je potřeba dokumentaci vedenou podle zákona o ISVS neposkytovat, je možné použít výjimku v § 10a ZKB již nyní (a to i s využitím podpůrného materiálu vydaného NÚKIB zde: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podperne-materialy/#:~:text=Doporu%C4%8Den%C3%AD%20N%C3%9AKIB%20k%20(ne)poskytov%C3%A1n%C3%AD%20informac%C3%AD%20v%20oblasti%20kybernetick%C3%A9%20bezpe%C4%8Dnosti%20a%20bezpe%C4%8Dnosti%20syst%C3%A9m%C5%AF%20nakl%C3%A1daj%C3%ADc%C3%ADch%20s%20utajovan%C3%BDmi%20informacemi). Okrajovým faktorem je také to, že gestorem zákona o ISVS je Ministerstvo vnitra, nikoliv NÚKIB. Reakce připomínkového místa Připomínkové místo na připomínce trvá a tato je předmětem rozporu. V průběhu vypořádání připomínkové místo navrhlo několik úprav § 38.

			Reakce NÚKIB V rámci finálního návrhu vypořádání byl připomínkovému místu zaslán návrh na úpravu odůvodnění k § 38. Úprava § 38 v návrhu zákona, kterou Úřad obdržel od připomínkového místa, nebyla akceptována Reakce připomínkového místa Připomínkové místo má stále za to, že navržená úprava § 38 návrhu zákona o kybernetické bezpečnosti ani ve spojení s příslušným ustanovením návrhu vyhlášky o dlouhodobém řízení informačních systémů veřejné správy obsahujícím výjimku ze zveřejňování informací o informačních systémech veřejné správy, není z právního ani legislativního hlediska v pořádku a nezajišťuje naplnění identifikované potřeby ochrany ISVS, když tyto dvě právní úpravy na sebe neváží z námi opakovaně uvedených důvodů. Tento nesoulad daných navržených právních předpisů podtrhuje i věta, na které je postaven výklad obsažený v metodickém pokynu připravovaném ze strany DIA: „<i>Samotný zákon o kybernetické bezpečnosti tedy vylučuje zveřejňování informací pouze pro předpisy, které upravují svobodný přístup k informacím, čímž se může myslet např. zákon č. 106/1999 Sb. o svobodném přístupu k informacím, ale v obecné rovině jakákoliv zveřejňování povinnost umožňující svobodný přístup daná právními předpisy, tedy i Vyhláškou</i>“. Tento výklad k tomu, co lze rozumět právními předpisy upravujícími svobodný přístup k informacím, kterými jsou čl. 17 Listiny, zákon č. 106/1999 Sb., zákon č. 123/1998 Sb., o právu na informace o životním prostředí apod., ale zřejmě nikoli předmětná vyhláška o dlouhodobém řízení informačních systémů veřejné

		správy, je minimálně velmi extenzivní a tedy problematický. Tyto a další námi upozorňované složitosti výkladu by právě ČTÚ navrhovaná úprava § 38 návrhu zákona o kybernetické bezpečnosti vyřešila. Odpovědnost za funkčnost právní úpravy však leží na straně gestorů daných předpisů. Pokud však bude jak v rámci odůvodnění k návrhu zákona o kybernetické bezpečnosti a dále příslušným pokynem kompetentními orgány deklarováno, obdobně jako je navrhováno v závěru připravovaného návrhu metodického pokynu, že na základě dané právní úpravy je založena výjimka z povinnosti zveřejňovat ty informace o systémech veřejné správy podle předmětné vyhlášky o dlouhodobém řízení informačních systémů veřejné správy, které by mohly ohrozit zajišťování kybernetické bezpečnosti, pak se bude ČTÚ jako adresát předmětných povinností stanovených vyhláškou takovou výjimkou ze zveřejňování informací o systémech veřejné správy řídit [jestliže se bude moci o jednoznačnou metodiku a závěry (pokyny) v ní uvedené opřít]. Vzhledem k tomu, že další diskuze nad danou problematikou je zjevně nadbytečná a konsenzu v řešení není možno dosáhnout, dovoluujeme si tedy za Český telekomunikační úřad (ČTÚ) k jeho připomínce č. 527 vypořádání uzavřít tak, že ČTÚ nezbývá než na dané připomínce trvat a ponechat se svůj názor na věc. Avšak při zohlednění výše uvedeného (tj. doplnění odůvodnění k návrhu zákona o kybernetické bezpečnosti k § 38 a dále vydání metodického pokynu DIA k vyhlášce o dlouhodobém řízení ISVS) sdělujeme, že <u>bereme neakceptování připomínky č. 527 ze strany NÚKIB</u>

			<u>na vědomí a tuto připomínku považujeme za vypořádanou „bez rozporu“.</u> Připomínka je vypořádána.
528. Český telekomunikační úřad	Z	K § 44 odst. 1 Návrhu Připomínka ČTÚ: ČTÚ navrhuje rozšířit možnost použití Portálu NÚKIB jako společné platformy pro hlášení bezpečnostních incidentů. ČTÚ tak navrhuje upravit odstavec 1 v tomto smyslu: „(1) Úřad je správcem a provozovatelem Portálu NÚKIB, který slouží k výkonu pravomocí Úřadu, sdílení informací, provádění digitálních úkonů a poskytování digitálních služeb podle tohoto zákona a pro plnění informační povinnosti, pokud tak stanoví jiný zákon.“. Odůvodnění: ČTÚ navrhuje doplnit funkce Portálu NÚKIB tak, aby jeho prostřednictvím mohly být do budoucna hlášeny bezpečnostní incidenty podle jiných právních předpisů, například podle § 98 odst. 4 zákona o elektronických a dalších zákonů upravujících problematiku hlášení bezpečnostních incidentů a byla tak vytvořena jednotná platforma pro hlášení bezpečnostních incidentů již dříve ze strany NÚKIB uvažovaná, která by měla být gestorována NÚKIB a měla sloužit, což ČTÚ podporuje, k jednotnému hlášení těchto incidentů. ČTÚ tak navrhuje upravit předmětné ustanovení ve smyslu této připomínky.	Vysvětleno - nyní § 47 Portál NÚKIB má sloužit pouze pro poskytovatele regulovaných služeb dle řešeného návrhu zákona a spolupracující organizace, nepůjde o univerzálně přístupnou platformu pro subjekty, které by například spadaly pouze do působnosti ZEK a nikoliv nového ZKB. NÚKIB nadále počítá se vznikem jednotné platformy, která bude umožňovat agregované hlášení dle více předpisů, nicméně tato by měla být spíše komplementárním řešením, které bude "přerozdělovat" příslušné hlášení relevantním subjektům, které je budou zpracovávat ve svých systémech s ohledem na jejich interní procesy. Závěr Po doplnění odůvodnění připomínkové místo s vypořádáním souhlasí.
529. Český telekomunikační úřad	Z	K § 63 Návrhu Připomínka ČTÚ: ČTÚ navrhuje do § 63 odst. 1 Návrhu doplnit větu, která včetně poznámky pod čarou zní: „Pokud se Úřadem připravované rozhodnutí nebo opatření obecné povahy může dotknout plnění existující povinnosti uložené	Neakceptováno - nyní § 65 Dle navrhované úpravy NÚKIB v rámci získávání informací spolupracuje s relevantními orgány státu, a to i s regulátory jednotlivých sektorů, je-li to pro daný případ vhodné a potřebné. Takový postup předpokládá jak předmětná navrhovaná právní úprava, tak pak

		podle jiného právního předpisu^x) je Úřad povinen vyžádat stanovisko příslušného orgánu a v nejvyšší možné míře toto stanovisko zohlednit. XX) Například zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách)...“. Odůvodnění: S ohledem na možný dopad rozhodnutí a opatření obecné povahy vydávaných Úřadem (NÚKIB) do plnění povinností uložených příslušným orgánem (v případě poskytovatelů regulované služby zajišťování veřejné komunikační sítě nebo regulované služby poskytování veřejně dostupné služby elektronických komunikací se jedná o ČTÚ), ČTÚ navrhuje doplnit povinnost, nikoli pouze oprávnění Úřadu (NÚKIB) vyžádat si v rámci přípravy rozhodnutí nebo opatření obecné povahy stanovisko příslušného orgánu (například ČTÚ) a takové stanovisko v maximální možné míře v rámci rozhodovací činnosti zohlednit.	obecná úprava postupu správních orgánů, např. v § 8 odst. 2 zákona č. 500/2004 Sb., správního řádu. Tento postup je rovněž dán principem dobré správy, kdy NÚKIB pro co nejlepší vyhodnocení situace a možných dopadů počítá s dožádáním informací od relevantních orgánů státu v rámci jednotlivých odvětví. Opakování této obecné povinnosti Úřadu proto nepovažujeme za potřebné ani za vhodné. Po schůzce Do ustanovení § 31 byla doplněna součinnost ČTÚ a připomínka byla vypořádána. Připomínkové místo s vypořádáním souhlasí.
530. Český telekomunikační úřad	Z	K bodu 16.1 a 16.2 přílohy k návrhu tezí vyhlášky o regulovaných službách (Teze prováděcích právních předpisů k navrhované právní úpravě) Připomínka ČTÚ: V bodech 16. 1 a 16. 2 přílohy k návrhu tezí vyhlášky o regulovaných službách jsou vymezeny v části I. pod písmeny c) a d) parametry pro zařazení podnikatelů poskytujících veřejně dostupnou službu elektronických komunikací nebo zajišťujících veřejnou komunikační síť do režimu vyšších povinností, a to konkrétně: „c) je poskytovatelem veřejně dostupné služby elektronických komunikací skrze nejméně 350 000 aktivních mobilních SIM karet na maloobchodním trhu na území České republiky, nebo d) je poskytovatelem nejméně 100 000 aktivních pevných internetových přípojek na území České republiky,“.	Neakceptováno Teze prováděcích právních předpisů jsou sice již teď součástí předkládaného materiálu, ale budou následně předmětem samostatného připomínkového řízení při procesu jejich vydávání. Nelze předpokládat, že jedna pevná přípojka (typicky jedna domácnost) odpovídá jedné osobě (tj. jedné SIM kartě), z pohledu účelu právní úpravy tedy není vhodné uvedená kritéria sjednocovat. Pokud jde o konkrétní počty SIM karet a pevných přípojek, uvedený minimální počet aktivních přípojek byl stanoven tak, aby pokryl subjekty poskytující společně podle posledních dostupných dat Českého telekomunikačního úřadu (za rok 2021) většinu všech aktivních přípojek (cca 60 %).

		ČTÚ není bez podrobnějšího zdůvodnění zřejmá, byť vnímá, že se jedná pouze o teze návrhu vyhlášky, rozdílnost těchto hodnot, resp. parametrů pro zařazení do režimu vyšších povinností, tj. 350 000 aktivních mobilních SIM karet na maloobchodním trhu na území České republiky vs. 100 000 aktivních pevných internetových přípojek na území České republiky, bez ohledu na to, zda se jedná o maloobchodní či velkoobchodní trh. ČTÚ tak navrhuje sjednotit hodnoty tak, aby hodnota uvedená v bodu 16. 1 a 16. 2 v části I. pod písmenem d) byla na úrovni hodnoty uvedené v bodu 16. 1 a 16. 2 části I. pod písmenem c), když hodnota 100 000 aktivních pevných internetových přípojek se jeví z hlediska dopadu regulace Návrhu jako příliš nízká. ČTÚ tak navrhuje upravit body 16. 1 a 16. 2 přílohy k návrhu tezí vyhlášky o regulovaných službách ve smyslu této připomínky.	Minimální počet SIM karet pokrývá subjekty, které společně poskytují veřejně dostupné služby elektronických komunikací uživatelům většiny všech aktivních mobilních SIM karet na maloobchodním trhu (cca 92 %). V případě SIM karet je současně zohledněna skutečnost, že uvedené výrazně nadpoloviční většině poskytují veřejně dostupné služby elektronických komunikací pouze tři subjekty. Závěr Po schůzce byly teze v této části zobecněny a konkrétní počet aktivních SIM karet nebo přípojek není uveden. Ten bude dále řešen v průběhu přípravy předmětné vyhlášky. Připomínkové místo s vypořádáním souhlasí.
531. Český telekomunikační úřad	D	K § 30 odst. 2 Návrhu Připomínka ČTÚ: V § 30 odst. 2 je navrhována nová gesce Bezpečnostní rady státu (BRS) vyplývající z navržené povinnosti ji informovat, resp. projednat návrhu opatření obecné povahy, kterým NÚKIB stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu. ČTÚ upozorňuje, že novou činnost BRS bude potřeba promítnout do vnitřních předpisů BRS, především do Statutu BRS, případně rovněž do Jednacího řádu BRS. ČTÚ proto doporučuje, aby taková potřeba úprav vnitřních předpisů BRS byla uvedena v rámci odůvodnění k § 30 odst. 2 Návrhu a gestor těchto předpisů (Úřad vlády ČR) byl na danou potřebu upozorněn.	Akceptováno jinak – nyní § 31 Předmětné ustanovení bylo v návaznosti na připomínky k němu dále rozpracováno a upraveno. Do zákona byl tak mj. doplněn souhlas Bezpečnostní rady státu a jeho význam pro vydávání opatření obecné povahy. Implicitně lze dovodit, že v případě jiné reakce, než souhlasu či vzetí na vědomí Bezpečnostní radou státu, Úřad nebude moci přistoupit k vydání návrhu opatření obecné povahy. Touto úpravou by mělo být dosaženo maximálního souladu s povahou a procesy BRS. Po schůzce Ustanovení § 31 bylo upraveno a připomínka byla vypořádána. Připomínkové místo s vypořádáním souhlasí.

532. Český telekomunikační úřad	D	K § 39 odst. 5 a § 65 Návrhu Připomínka ČTÚ: V § 65 Návrhu je v rámci společných ustanovení stanoveno, že na tam vyjmenované postupy se ustanovení správního řádu upravující vedení správního řízení nepoužijí. V § 39 odst. 5 Návrhu se stanoví, že na rozhodování a ukládání povinností podle tohoto zákona se v době stavu kybernetického nebezpečí nevztahuje správní řád. Z obsahu § 39 odst. 5 Návrhu a jeho odůvodnění není zcela zřejmé, zda bylo úmyslem, aby se v době stavu kybernetického nebezpečí na rozhodování a ukládání povinností podle tohoto zákona nepoužil správní řád vůbec bez výjimky, tj. ani v těch případech, kde to jinak možné je (viz § 62 Návrhu), resp. zda mají být v takovém případě aplikovány základní zásady činnosti správních orgánů uvedené ve správním řádu apod. Navržená úprava vztahu Návrhu ke správnímu řádu, která je v Návrhu řešena na více místech působí nejednoznačně. ČTÚ tak doporučuje § 39 odst. 5 Návrhu, případně jeho odůvodnění upravit ve smyslu této připomínky. Zároveň lze doporučit přesunutí obsahu § 39 odst. 5 Návrhu do společného ustanovení (§ 65 Návrhu), kde je obecně upraven vztah Návrhu ke správnímu řádu.	Akceptováno jinak Úřad je při své činnosti standardně vázán ustanoveními správního řádu, některá specifická jednání však vyžadují úpravu obecných pravidel a proto byla tato úprava v § 65 obsažena. Bylo naznáno, že bude z koncepčního pohledu lepší stanovit vztah zákona za stavu kybernetického nebezpečí ke správnímu řádu explicitně u ustanovení, jež upravuje stav kybernetického nebezpečí pro větší přehlednost v rámci nástrojů a jejich jednotlivých náležitostí/pravidel. Na základě Vaší, ale i dalších připomínek, byl § 65 vypuštěn a jeho obsah byl, pro lepší přehlednost a ucelenost právní úpravy, vnesen do jednotlivých ustanovení, která původně upravoval, aby se zvýšila možnost adresáta právní normy co nejjednodušeji porozumět jejímu obsahu. Vyloučení aplikace správního řádu za stavu kybernetického nebezpečí míří k co nejrychlejšímu vyřešení situace, kdy je značně narušena či ohrožena bezpečnost informací v kybernetickém prostoru, nicméně základní zásady činnosti správních orgánů budou i za takového vyloučení podle § 177 správního řádu zachovány. Zájem pro vyloučení správního řádu směřuje zejména na možnost rychle reagovat na situace, které nastanou, a to ať už za pomoci opatření za stavu kybernetického nebezpečí, tak za použití běžných zákonných nástrojů. Po schůzce Ustanovení § 31 bylo upraveno a připomínka byla vypořádána. Připomínkové místo s vypořádáním souhlasí.

533. Český báňský úřad	D ČBÚ považuje automatické zařazování všech ústředních správních úřadů do kategorie „Regulované služby v režimu vyšších povinností“ za nevhodné. Vzhledem k nižší možnosti vzniku rizik v rámci malých kapitol vyvolává toto zařazení toliko neúměrný tlak na finanční náklady, jejichž vynaložení je z výše uvedeného důvodu neúčelné. Požadujeme tento systém opustit, respektive návrh vyhlášky upravit tak, aby bylo třeba nejprve vyhodnotit míru rizika a teprve následně správní úřad zařazovat do příslušné kategorie regulovaných služeb. <u>Odůvodnění:</u> Součástí předloženého materiálu jsou i teze prováděcích právních předpisů k návrhu zákona o kybernetické bezpečnosti. Podle § 4 odst. 1 návrhu zákona jsou kritéria pro identifikaci regulované služby tvořena kritériem služby a kritériem poskytovatele regulované služby. Z návrhu vyhlášky o regulovaných službách vyplývá, že ústřední orgány státní správy budou zařazeny do kategorie „regulované služby v režimu vyšších povinností“ (bod 1.1 přílohy této vyhlášky) – kritériem služby je výkon svěřených pravomocí a kritériem poskytovatele je ústřední orgán státní správy (tedy i ČBÚ). Navrhovaná vyhláška „O bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností“ stanovuje v § 5 odstavci 6 povinnost vrcholného vedení určit osoby, které budou zastávat bezpečnostní roli: a) manažera kybernetické bezpečnosti, b) architekta kybernetické bezpečnosti, c) garanta aktiva a d) auditora kybernetické bezpečnosti, včetně zajištění zastupitelnosti těchto rolí, přičemž tyto role nemohou zastávat osoby odpovědné za provoz IT.	Vysvětleno Rozumíme Vaším obavám, pokusíme se Vám proto vysvětlit, že Vámi předpokládané náklady mohou být znatelně nižší. Jste instituce státu, který pracuje s informacemi o občanech, kteří nemají volbu tyto informace neposkytnout. Je tedy nutné je z pohledu kybernetické bezpečnosti chránit, i proto jsou ústřední orgány státní správy v režimu vyšších povinností. V režimu vyšších povinností jsou opatření škálována a vybírána na základě výsledků hodnocení rizik. Rovněž je integrálním principem vyhlášky i princip přiměřenosti opatření vůči nákladům za jeho pořízení, tedy takové opatření by nemělo stát více, než jakou škodu by obecně mohlo způsobit, že dojde k realizaci kybernetického útoku. K bezpečnostním opatřením proto nelze přistupovat metodou checklistu, systém řízení bezpečnosti informací je sofistikovanější, což ale rovněž umožňuje přiměřeně jej přizpůsobit potřebám organizace. V případě, že povinná osoba v režimu vyšších povinností je z kybernetického pohledu „nezajímavá“, nedisponuje prakticky žádnými riziky. Zavádění bezpečnostních opatření je tedy pro ni neúčelné s ohledem na hodnocení rizik. Rovněž se domníváme, že organizace, která již byla správcem významných informačních systémů, bude mít spoustu opatření již zavedeno, což by také mělo vést k menší míře nákladů. Garanty aktiv je však nutné mít vždy, jedná se zpravidla o zaměstnance, kteří mají něco na starost (vedoucí, administrátoři apod.). Roli manažera kybernetické bezpečnosti je také možné na základě hodnocení rizik spojit s rolí architekta kybernetické

		Důvodová zpráva (RIA) uvádí velmi hrubý odhad nákladů ve výši 800.000 až 1.500.000 Kč na vytvoření jednoho bezpečnostního systému u jednoho subjektu. Navrhovaná právní úprava bude znamenat v rámci ČBÚ provedení změn v organizaci kybernetické bezpečnosti. Bude nutné rozšířit bezpečnostní role o architekta kybernetické bezpečnosti, garanta aktiva a auditora kybernetické bezpečnosti. Bude také nutné zavést nástroj pro správu a monitorování IT infrastruktury, jehož pořízení a obsluha představuje pro ČBÚ největší finanční zátěž. ČBÚ odhaduje navýšení ročních nákladů na zajištění kybernetické bezpečnosti min. o 860.000 Kč.	bezpečnosti, protože by to pro Vás v opačném případě mohlo být nepřiměřeně zatěžující. V extrémním případě, který nedoporučujeme, může roli manažera kybernetické bezpečnosti vykonávat zaměstnanec zařazený do provozu. Tento postup připadá v úvahu, pokud se jedná o velmi malou organizaci a je v silách jednoho člověka požadavky zvládnout a akceptujete možné riziko střetu zájmů. Obdobně je možné přistoupit k roli auditora, kdy si lze objednat externí audit. Co se týče zastupitelnosti, neznamená to, že je nutné mít jako zástup speciálního člověka. Nezbytné je, aby v případě, že je manažer kybernetické bezpečnosti na dovolené nebo v pracovní neschopnosti (je jedno, zda bude zástup o jednom, nebo o pěti lidech - mohou být i z provozu), vykonával jemu svěřené pravomoci někdo jiný. Pro Vás je tedy zásadní, abyste odhadli efektivně a správně celkové požadavky a tím pádem i budoucí náklady. To vše je nutné postavit na zvládnutém řízení rizik. Vlastnit nástroj pro správu infrastruktur je nezbytné v případě, pokud nějaká infrastruktura existuje. Samotný monitoring infrastruktury je velmi široký pojem – existují programy, které nestojí nic, a v případě, že nejsou finance na zakoupení placeného nástroje, lze to ošetřit plánem zvládnutí rizik a naplánovat podle toho investice do budoucna – je však nutné s tím pracovat a plánovat jeho pořízení pro zajištění prokazatelného kontinuálního zlepšování. Reakce připomínkového místa: Děkujeme za doručení návrhu vypořádání, nicméně s obsahem uvedeným v něm nemůžeme vyjádřit souhlas. Navrhované řešení, zahrnující koncept kumulace funkcí a implementaci softwaru Free-W

		(freeware), zdá se být odvozeno z omezeného porozumění organizační struktury, kompetencí, a především rozpočtových možností orgánů státní báňské správy. 2/ Problémem v případě ČBÚ jako malé rozpočtové kapitoly spočívá v tom, že již v současnosti praktikujeme kumulaci funkcí. K tomu může posloužit jako příklad, že jedna osoba vykonává úlohy bezpečnostního ředitele, webmastera, programátora, projektového manažera pro implementaci informačního systému a architekta informačních systémů na našem úřadě, zatímco v rámci větších kapitol je tato funkcionalita rozdělena mezi několik odborných pracovníků. Reakce ČBÚ na vypořádání: Opatření týkající se Free-W (freeware) jsou již prováděna, avšak je nutno poznamenat, že zde existují jistá omezení. Využívání freeware, konkrétně systému Free-W (freeware), nesouvisí pouze s jeho bezplatnou dostupností, ale přináší s sebou řadu dalších aspektů. Prvním klíčovým prvkem je odbornost personálu. Jelikož freeware často nemá stejnou míru podpory a dokumentace jako placené alternativy, vyžaduje jeho úspěšné nasazení a správa zvýšenou odbornost a znalost uživatelů. Je nezbytné, aby personál měl dostatečné povědomí o technických detailech a schopnostech tohoto konkrétního softwaru, aby mohl využít jeho potenciál plně a především správně. Dalším důležitým aspektem je kybernetická bezpečnost. I když je Free-W (freeware) zdarma, neznamená to, že by neměla být věnována pozornost zabezpečení. Naopak, správa freeware může klást vyšší nároky na kybernetickou bezpečnost, včetně monitorování a prověřování důvěryhodnosti souborů a

		aplikací, které mohou být v systému používány. Je třeba mít na paměti, že zdarma dostupný software může představovat vyšší rizika pro bezpečnost informačního prostředí organizace. Při využívání freeware je také důležité mít na zřeteli, že přestože samotný software je zdarma, mohou existovat další náklady spojené s jeho provozem. To může zahrnovat náklady na školení personálu, případně na další doplňkové licence nebo komponenty, které jsou nezbytné pro plnou funkčnost systému. Je nutné pečlivě zhodnotit veškeré potřebné zdroje a náklady, aby bylo možné správně ocenit celkovou efektivitu a výhody využívání freeware v daném prostředí. Nelze opomenout ani podporu Vámi navrhovaných činností, která nepochybně nese své náklady. Z tohoto důvodu trvá ČBÚ na tom, aby návrh obsahoval konkrétní finanční prostředky nezbytné k zajištění požadavků vyplývajících z návrhu, a zejména aby bylo zajištěno jejich začlenění do rozpočtu jednotlivých rozpočtových kapitol, včetně kapitoly ČBÚ. 3/ S ohledem na vypořádání připomínek k novému zákonu o kybernetické bezpečnosti z Vaší strany vůči vzneseným připomínkám z naší strany, dovolujeme si Vás požádat také o upřesnění termínu „Samotný monitoring sítě“, kdy tento pojem charakterizujete jako "velmi široký". Rádi bychom si termín upřesnili s ohledem na naše vyhodnocení rizik a možnosti ČBÚ. Pro úplnost ČBÚ uvádí, že v současnosti jsme již - krom jiného - zavedli následující opatření v oblasti kybernetické bezpečnosti:

			• Monitorujeme síťový provoz na vstupu a výstupu za pomoci Firewallu ve spojení s systémy detekce/prevence narušení (IDS/IPS). • Vedeme detailní záznamy událostí a aktivit v rámci našich systémů prostřednictvím logování a událostních záznamů (logs). • Pravidelně sledujeme změny v konfiguracích systémů a aplikací. • Monitorujeme stav a výsledky antivirových a antimalwarových skenování s cílem identifikovat potenciálně škodlivé soubory či aktivity. • Částečně monitorujeme síť systémem Nagios. Rádi bychom se ujistili o tom, zda tyto kroky postačují k plnění požadavků stanovených v zákoně o kybernetické bezpečnosti s ohledem na termín “monitoring sítě“. V opačném případě bychom chtěli vědět, zda lze požadavky naplnit prostřednictvím zpřísnění nebo zintenzivněním stávajících opatření, či zda je třeba zavést další monitorovací systém. S ohledem na výše uvedené navrhuje jednání, včetně setkání na úrovni zástupce předsedy ČBÚ. Závěr: Vysvětleno a vypořádáno. Současně připomínkové místo mění připomínku na doporučující.
534. Národní bezpečnostní úřad	Z	K § 29 odst. 3 NBÚ je ústředním správním úřadem s působností v oblasti ochrany utajovaných informací. Informace získané v rámci jím vedeného bezpečnostního řízení slouží výhradně pro zjištění, zda se u účastníka řízení, ať již fyzické nebo právnické osoby, vyskytuje bezpečnostní riziko nebo negativní okolnost. NBÚ při vedení bezpečnostního řízení	Akceptováno jinak - nyní § 30 odst. 3 Do znění § 30 odst. 3 byla přidána lhůta k poskytnutí informací. Návrh týkající se bezpečnostního svazku však neakceptujeme. Ustanovení § 124 odst. 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, říká, že údaje v něm

	nemá žádné výkonné pravomoci, z tohoto důvodu je oprávněn požádat o získání potřebných informací zpravodajské služby. Tyto poskytnuté informace vztahující se k žadateli o osvědčení nebo držiteli osvědčení, jejichž původcem je tedy zpravodajská služba a nikoliv NBÚ, je pak NBÚ povinen chránit podle § 124 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tato ochrana zaručuje zpravodajským službám to, že informace, které získaly, nebudou zpřístupněny neurčitému okruhu osob a nemůže tak dojít ke kompromitaci těchto informací a potažmo i činnosti služby. Prolomení povinnosti ochrany informací pro účely, které zákon sleduje, tedy k prověřování bezpečnosti dodavatelského řetězce, není dle názoru NBÚ přiměřené účelu, ke kterému jsou informace primárně a výlučně shromažďovány, tedy k zajištění personální a průmyslové bezpečnosti v oblasti ochrany utajovaných informací, a zároveň by mohlo ohrozit činnost zpravodajských služeb. NBÚ tedy žádá o zakotvení výjimky pro poskytování informací z bezpečnostního svazku vedeného podle zákona č. 412/2005 Sb. a navrhuje např. tuto formulaci: „(3) Nezíská-li Úřad z vlastní činnosti nebo postupem podle odstavce 1 a 2 informace potřebné pro výkon činnosti podle § 28 odst. 1, poskytnou na základě žádosti Úřadu tyto informace nebo jinou součinnost orgány a osoby neuvedené v odstavci 1 a 2, s výjimkou informací z bezpečnostního svazku vedeného podle jiného právního předpisu^{x)}.“ ^{x)} Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.“	uvedené je možné využít pouze pro potřeby plnění úkolů podle zákona č. 412/2005 Sb. Jedinou výjimkou jsou pak potřeby orgánů činných v trestním řízení. Domníváme se tedy, že současná úprava ani neumožňuje předání informací pocházejících z bezpečnostního svazku na základě žádosti NÚKIB podle § 30 odst. 3. Reakce připomínkového místa: S navrženým vypořádáním NBÚ souhlasí za předpokladu stejného principu neduplicitní úpravy (viz příp. 535). Závěr: Písemně odeslána úprava § 44, která byla ze strany NBÚ odsouhlasena a připomínka je vypořádána.

		Dále považujeme za potřebné, aby i odstavec 3 obsahoval konkrétní zákonnou lhůtu pro poskytnutí informací nebo jiné součinnosti.	
535. Národní bezpečnostní úřad	Z	K § 41 Komplexní institucionální zakotvení kompetencí NÚKIB v oblasti ochrany utajovaných informací obsahuje již zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti, který upravuje působnost NÚKIB v této oblasti. NBÚ v současné době nespátřuje žádný praktický ani teoreticko-právní důvod pro částečnou, duplicitní úpravu v zákonu o kybernetické bezpečnosti. Žádáme proto, aby v § 41 odst. 1 byl ponechán odkaz na zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti a ze všech zbývajících ustanovení § 41 byly vypuštěny kompetence NÚKIB vyplývající ze zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.	Neakceptováno - nyní § 44 Úprava zákona o ochraně utajovaných informací, resp. jeho § 137a shrnuje pravomoci Národního úřadu pro kybernetickou a informační bezpečnost v oblasti ochrany utajovaných informací, které jsou promítnuty do § 44 odst. 1 a na něj pak navazující § 44 odst. 4 písm. c) a d) návrhu zákona. Ustanovení § 44 návrhu zákona (stejně tak jako § 22 v účinném zákoně o kybernetické bezpečnosti) zakotvuje postavení Národního úřadu pro kybernetickou a informační bezpečnost a vymezuje (resp. shrnuje) jeho pravomoci jako ústředního orgánu státní správy komplexně na jednom místě. Navržená úprava není v rozporu s úpravou zákona o ochraně utajovaných informací, naopak je s ní zcela v souladu a přímo na ní odkazuje. Z uvedených důvodů ponecháme předmětnou navrženou úpravu beze změn. Reakce připomínkového místa: S navrženým vypořádáním NBÚ nesouhlasí a i nadále požaduje, aby zakotvení kompetencí NÚKIB v oblasti ochrany utajovaných informací bylo výlučně stanoveno v zákoně č. 412/2005 Sb. Oblast ochrany utajovaných informací je komplexně upravena tímto zákonem, který stanoví mimo jiné působnost NÚKIB na poli ochrany utajovaných informací. Tato úprava je podle našeho názoru zcela dostačující a není žádoucí kompetence NÚKIB zakotvené zákonem č. 412/2005 Sb. duplicitně stanovit rovněž v ZKB. Ostatně přistoupíme-li na argumentaci NÚKIB k připomínce NBÚ k § 29/3 ZKB, kdy je úprava neposkytování

			informací z bezpečnostního svazku v § 124/3 zákona č. 412/2005 Sb. dostatečná a není třeba ji v novém ZKB výslovně upravit, pak by touto optikou měla být zcela dostačující i úprava působnosti NÚKIB v oblasti ochrany utajovaných informací stanovená pouze zákonem č. 412/2005 Sb. Závěr: Písemně odeslána úprava § 44, která byla ze strany NBÚ odsouhlasena a připomínka je vypořádána.
536. Národní bezpečnostní úřad	Z	Zvláštní část Důvodové zprávy, 7. 1. 6. Shrnutí dopadů na státní rozpočet a ostatní veřejné rozpočty, zmiňuje Národní bezpečnostní úřad v souvislosti s výkonem nové agendy prověřování bezpečnostní rizikovitosti dodavatelů. Vzhledem k tomu, že byl NBÚ v předchozí fázi přípravy návrhu zákona z § 29 odst. 2 vypuštěn, měla by být zmínka o NBÚ vyřazena také z Důvodové zprávy.	Akceptováno Zmínka o NBÚ byla z dané části důvodové zprávy odstraněna. Připomínkové místo s vypořádáním souhlasí.
537. Národní bezpečnostní úřad	D	§ 18 odst. 1 stanoví, že Úřad nebo Národní CERT poskytne bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení podle § 17 poskytovateli regulované služby své vyjádření ke kybernetickému bezpečnostnímu incidentu. § 17 v odst. 2 již však stanovuje, že Úřad sdělí poskytovateli regulované služby v režimu vyšších povinností bez zbytečného odkladu, nejpozději do 24 hodin po nahlášení kybernetického bezpečnostního incidentu podle odstavce 1, na základě obsahu hlášení a dalších relevantních informací, zda má kybernetický bezpečnostní incident u poskytovatele regulované služby v režimu vyšších povinností významný dopad na kybernetický prostor státu. Doporučujeme zvážit, zda nejde o částečnou duplikaci § 18 odst. 1. Zároveň upozorňujeme na to, že ačkoliv jsou odstavce 2 a 3 v § 18 uvedeny v rozdílové tabulce, v normativním textu nejsou podtrženy.	Akceptováno Odstavce 2 a 3 byly podtrženy. Co se týče částečné duplikace, Úřadu se jeví jako systematicky vhodnější řešení upravení hlášení tímto způsobem, neboť na sdělení Úřadu podle § 17 odst. 2 navrhovaného znění je navázána povinnost dalšího hlášení, které jinak podle § 18 není vyžadováno. Připomínkové místo s vypořádáním souhlasí.
538. Národní bezpečnostní úřad	D	Nadpis § 21 zní „Výstraha“, ale tento pojem se v jeho odstavcích 1 až 3 vůbec nevyskytuje. Doporučujeme jazykovou úpravu textu obdobnou, jaká je obsažena v § 22 (Varování).	Akceptováno Připomínkové místo s vypořádáním souhlasí.

539. Národní bezpečnostní úřad	D	K Důvodové zprávě: V tabulce agend a souvisejících účelů zpracování osobních údajů, spolu s druhy či kategoriemi zpracovávaných údajů, na základě návrhu zákona, je uveden i požadavek na uvedení místa trvalého pobytu u: - o osoby jednající za žadatele o autorizaci; - o žadatele nebo osoby jednající za žadatele; - o osob zúčastněných na kontrole. Není zřejmé, za jakým účelem je ve všech výše uvedených případech požadavek na uvedení místa trvalého pobytu zaveden a doporučuje se jeho přehodnocení, či vypuštění, a to zejména u osob zúčastněných na kontrole.	Vysvětleno Údaj o trvalém pobytu by měl sloužit pouze pro jednoznačnou identifikaci konkrétní fyzické osoby, v případě kontrol navazuje na oprávnění kontrolujícího dle § 8 písm. a) kontrolního řádu (požadovat prokázání totožnosti fyzické osoby, jež je přítomna na místě kontroly, jde-li o osobu, která plní úkoly kontrolované osoby, nebo osobu, která může přispět ke splnění účelu kontroly). Konkrétní rozsah potřebných údajů bude ještě zváženo a případně změněno s ohledem na nastavení konkrétních procesů NÚKIB. Připomínkové místo s vypořádáním souhlasí.
540. Sdružení samospráv republiky	místních České Z	K Tezím prováděcích právních předpisů, návrhu vyhlášky o regulovaných službách Požadujeme, aby v příloze vyhlášky u služby Výkon svěřených pravomocí byla mezi dotčené poskytovatele zařazena statutární města namísto obcí s rozšířenou působností (ORP), a to v režimu nižších povinností. <u>Odůvodnění:</u> Ačkoliv vnímáme stále narůstající význam kybernetické bezpečnosti, musíme upozornit na to, že zákonná regulace musí vycházet z objektivní reality a ukládat subjektům povinnosti přiměřeně tak, aby je byly schopny po nabytí účinnosti zákona řádně naplňovat. Na základě detailní znalosti prostředí územní samosprávy získané při naší činnosti pochybujeme o tom, že je možné od 18. října 2024 vyžadovat plnění povinností podle návrhu zákona u všech ORP. Kategorie ORP je velmi heterogenní, zahrnuje jak největší statutární města, tak obce kolem 3000 obyvatel. O základě toho mají jednotlivá ORP diametrálně odlišné personální i finanční možnosti a na jejich území je odlišná dostupnost kvalifikované pracovní síly z odvětví informačních technologií. Naproti tomu mezi statutární města patří pouze takové základní územní samosprávné celky, jejichž orgány jsou	Neakceptováno Úvodem je nutné zdůraznit, že regulace směrem k obcím s rozšířenou působností (ORP) je odůvodněna agendou přenesené působnosti, a to v režimu nižších povinností. Mezi ORP a statutárním městem (SM), které je zároveň také v množině ORP, není z pohledu přenesené působnosti, a tedy v odvětví veřejné správy a výkonu svěřených pravomocí, žádný rozdíl. Není tedy žádný relevantní důvod k tomuto vynětí. Velikost ORP, její organizační struktura a vámi zmiňovaná robustnost nemůže být tímto důvodem, protože poskytovaná regulovaná služba musí být poskytnuta ve stejné kvalitě v každé ORP, nehlédě na to, že tyto služby (např. vydání občanského průkazu) musí poskytnout občanovi kterákoliv ORP, a to bez ohledu na trvalý pobyt tohoto občana. Žádná ORP nebude začínat se zajišťováním kybernetické bezpečnosti na „zelené louce“. Aniž se to tak může jevit, některé požadavky kladené na režim nižších povinností má již zavedena většina dotčených

			dostatečně robustní (personálně, finančně) na to, aby se do podzimu příštího zvládli na plnění povinnosti v nižším režimu připravit. S ohledem na důležitost problematiky kybernetické bezpečnosti se nebráníme diskuzi o rozšíření povinností v nižším režimu na všechny ORP a o přeřazení několika největších měst do režimu vyšších povinností. Tomu však musí předcházet pečlivé vyčíslení dopadů, vyřešení otázky financování na místní úrovni, a také intenzivní osvětová a metodická činnost, na níž je SMS ČR připraveno s NÚKIB spolupracovat. V současné situaci však musíme trvat na zúžení povinných subjektů pouze na statutární města.	organizací a mnoho projektů je v realizaci. K tomu slouží např. i financování z výzev IROP. Výdaje na bezpečnostní opatření nebudou jednorázové, ale budou rozloženy v čase (i několika let), jak vyhlášky umožňují. Připravovaný návrh zákona ukládá povinnost plnit, nikoliv direktivně splnit, všechna bezpečnostní opatření. Tzn., že ORP si zavede plán plnění těchto bezpečnostních opatření, který bude postupně realizovat dle svých možností a potřeb dané organizace. Připomínkové místo s vypořádáním souhlasí.
541. Sdružení samospráv republiky	místních České	Z	K obecné části důvodové zprávy Požadujeme v důvodové zprávě detailně vyčíslit dopady na územní samosprávné celky a toto vyčíslení řádně zdůvodnit. <u>Odůvodnění:</u> Důvodová zpráva se věnuje dopadům na územní samosprávné celky jen ve dvou odstavcích, které s jednoduchým zdůvodněním konstatují srovnatelnost s dopady na státní rozpočet. To podle nás nelze považovat za řádné vyčíslení dopadů. S předkladatelovou úvahou navíc nelze souhlasit, neboť především výše zmíněné menší ORP se (narozdíl od státních orgánů) neobejdou bez výrazného navýšení personální kapacity nebo zajištění externího dodavatele, aby mohly požadované povinnosti plnit. Důvodová zpráva pak zcela vynechává dopady na rozpočty krajů, které přitom návrh vyhlášky o regulovaných službách řadí do režimu vyšších povinností. Současně upozorňujeme na známý nedostatek IT specialistů zaměřených na kybernetickou bezpečnost a na fakt, že s ohledem na nastavení odměn není pro tyto pracovníky atraktivní ucházet se o pozice ve veřejné správě. I tento aspekt by měl předkladatel v důvodové zprávě zohlednit a vysvětlit, jak ho hodlá řešit.	Neakceptováno Děkujeme za Vámi zaslanou připomínku. Úvodem je nutné zdůraznit, že regulace směrem k obcím s rozšířenou působností (ORP) je stanovena v režimu nižších povinností. Dopad na veřejné rozpočty je vysvětlen v části 7.1.1., kde je nejdůležitější věta "jen regulovaná organizace samotná by měla být schopná identifikovat své vlastní náklady na zavedení a udržování přiměřené úrovně kybernetické bezpečnosti". Úřad nemůže vyčíslit finanční nákladnost návrhu zákona u jednotlivých ORP, protože např. některá obec má svoje vlastní odpadové hospodářství a jiná obec tuto agendu kompletně svěřila soukromé společnosti, která není touto obcí zřízena. V tomto ohledu došlo i k doplnění důvodové zprávy o výsledky snahy Úřadu udělat průzkum k nákladům. K připomínce navrhovatele o počtu odborníků na kybernetickou bezpečnost v ČR a ke snížení příspěvku státu na výkon přenesené působnosti se Úřad nemůže vyjádřit, neboť tyto nesouvisí s návrhem zákona.

			Dopady na rozpočty krajů se nepředpokládají ve významné výši, protože všechny kraje již jsou v současné době regulovány subjekty. Jsou správci významných informačních systémů dle Vyhlášky č. 317/2014 Sb. Dle návrhu zákona se předpokládá, že budou zařazeny do režimu vyšších povinností, který je obdobou původních povinností ze zákona o kybernetické bezpečnosti, kterými jsou již nyní kraje vázány. Připomínkové místo s vypořádáním souhlasí.
542. Úřad pro ochranu hospodářské soutěže	Z	K § 33 Navrhovaný § 33 upravující omezení rizik spojených s dodavatelem ve veřejných zakázkách stanoví, že „poskytovatel strategicky významné služby v postavení zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek může závazek ze smlouvy na veřejnou zakázku vypovědět bez zbytečného odkladu poté, co zjistí, že v jeho plnění nelze pokračovat, aniž by nebylo porušeno opatření obecné povahy podle § 30.“. Nepovažuji za nutné přijímat specifickou právní úpravu pro ukončení závazku z důvodu porušení opatření obecné povahy podle § 30 návrhu zákona pro zadavatele veřejných zakázek. Možnost závazek vypovědět by měla platit pro všechny poskytovatele strategicky významných služeb. Navrhuji proto následující úpravu textu: „§ 33 Omezení rizik spojených s dodavatelem ~~ve veřejných zakázkách~~ Poskytovatel strategicky významné služby ~~v postavení zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek~~ může závazek ze smlouvy ~~na veřejnou zakázku~~ vypovědět bez	Akceptováno - nyní § 34 Připomínkované ustanovení předkládaného návrhu zákona bylo upraveno podle požadavků připomínky. Možnost ukončení dlouhodobých závazků tak bude přiznána i soukromým subjektům, které nejsou zadavateli podle zákona o zadávání veřejných zakázek. Připomínkové místo s vypořádáním souhlasí.

		zbytečného odkladu poté, co zjistí, že v jeho plnění nelze pokračovat, aniž by nebylo porušeno opatření obecné povahy podle § 30.“.	
543. Úřad pro ochranu hospodářské soutěže	Z	Obecná připomínka k vyznačování transpozičních ustanovení Na příkladu připomínkovaného ustanovení § 33 návrhu zákona lze poukázat na to, že návrh zákona obsahuje řadu ustanovení, která jsou uvedením identifikačního čísla CELEX vyznačeny jako transpoziční. V rozdílové tabulce k předmětnému, a i k dalším ustanovení zákona, je uvedeno následující: <i>„Tato směrnice nebrání členským státům v tom, aby přijímaly nebo ponechaly v platnosti ustanovení zajišťující vyšší úroveň kybernetické bezpečnosti, jsou-li tato ustanovení v souladu s jejich povinnostmi stanovenými v právu Unie.“.</i> Legislativní pravidla vlády v Příloze č. 5 čl. II odst. 1 stanoví, že „v textu každého návrhu zákona nebo nařízení vlády podle čl. I se vyznačí ta ustanovení, jimiž je zajišťována transpozice, adaptace nebo jiná implementace, a to jejich potvrzením, a pod tato ustanovení se na levé straně uvede identifikační číslo (CELEX) příslušného předpisu EU nebo rozhodnutí Soudního dvora Evropské unie.“. Je proto otázkou, zda je za situace, kdy směrnice pouze „umožňuje“ vyšší standard bezpečnosti, důvod označovat předmětná ustanovení jako transpoziční. Považuji za vhodné zvážit takovéto označování a v případě jeho zachování tento přístup vysvětlit a řádně odůvodnit v důvodové zprávě.	Akceptováno Všechna ustanovení, která jsou vykázána pouze s odkazem na čl. 5 nebudou vykázána jako transpoziční a budou vypuštěna z rozdílové tabulky. Připomínkové místo s vypořádáním souhlasí.
544. Úřad pro ochranu osobních údajů	D	Obecně Úřad pro ochranu osobních údajů uplatňuje připomínky, a to včetně zásadních, zejména k osobním údajům. 1. ÚOOÚ upozorňuje na to, že před meziresortním připomínkovým řízením k návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, jej bude nutné dopracovat, konkrétně její § 8 a přílohu č. 1. Pro zavedení	Ad 1: Vysvětleno Příloha je doporučujícího charakteru. Záleží na povinné osobě, zda vyhodnotí zavedení TLP jako potřebné. Jedná se o obecný standart, jeho implementace nevyžaduje žádné technické konfigurace, prostředky ani znalosti ISO norem. Proto jejich bezplatné zpřístupnění není potřebné. Pro

	<i>Traffic Light Protocol</i> (TLP) nejsou stanovena dostatečně jasná pravidla. Bude se vycházet z ISO/IEC 27010:2015, nebo jiného standardu? Pak je nutné dořešit obecnou a bezplatnou přístupnost této technické nomy. 2. Právní norma v § 8 je nedostatečná. Stanoví pouze, že povinná osoba má stanovit pravidla pro klasifikaci informací a pravidla pro označování aktiv „alespoň v rozsahu uvedeném v příloze č. 1“. Pod tím si lze představit cokoliv. Z přílohy č. 1 vyplývá, že každá povinná osoba si v podstatě může pravidla hodnocení aktiv stanovovat libovolně a libovolně tedy k nim například přiřazovat hodnotící TLP označení. Při vzájemné výměně informací mezi zákonem dotčenými subjekty tedy nutně musí docházet k situaci, že informace (dokument) může být označen různě nebo označen TLP s jinou parametrizací. Tedy jednotliví aktéři sdílení dat vůbec netuší, jakou hodnotu pro druhý subjekt informace má i když bude označen podle TLP. 3. I s ohledem na to, se ÚOOÚ nadále domnívá, že by mělo být znovu posouzeno naplnění zásady enumerativnosti veřejnoprávních pretensí a nahradit návrh vyhlášky tam, kde to lze, opatřeními obecné povahy. 4. V souvislosti s přípravou tzv. „single point of entry“ (SPOE) pro hlášení incidentů spojených s agendou NÚKIB, ÚOOÚ a případně dalších úřadů se dovoluujeme dotázat, zda není nezbytná legislativní úprava tohoto systému. 5. ÚOOÚ dále uplatňuje ty připomínky, které se nepodařilo vyřešit v rámci veřejné konzultace.	doplnění, TLP pokrývá sdílení informací, nikoliv další aspekty jako je ukládání, likvidaci atd. TLP se stává postupně čím dál tím rozšířenějším, i když si organizace volí často své vlastní interní klasifikace informací (interní, citlivé atd.) Více k tomu například Legislativní pravidla vlády: Odkaz na technickou normu (1) Odkazuje-li se při stanovení technických požadavků v právním předpisu na českou technickou normu, jinou technickou normu nebo technický dokument mezinárodní, popřípadě zahraniční organizace nebo jiný technický dokument, který obsahuje podrobné technické požadavky (dále jen „technická norma“), použije se přednostně indikativní odkaz. V tomto případě je třeba v právním předpisu výstižně definovat základní technické požadavky a zároveň uvést, že se považují za splněné, postupuje-li se ve shodě s určenou normou nebo její částí, definovanou v § 4a zákona č. 22/1997 Sb., o technických požadavcích na výrobky, která obsahuje podrobné technické požadavky. Shoda s určenou normou je jedním ze způsobů, jak prokázat splnění základních technických požadavků. Určená norma v tomto případě konkretizuje obecný, souhrnný právní požadavek. Tyto požadavky mohou být splněny i jiným technickým řešením garantujícím stejnou nebo vyšší úroveň ochrany oprávněných zájmů. (2) Není-li možné využít indikativního odkazu, odkáže se na technickou normu v právním předpisu formou výlučného odkazu a tato skutečnost se odůvodní v důvodové zprávě (odůvodnění). Tímto se stane technická norma nebo její část pro účely právního předpisu závaznou a její používání se stane povinné. Zároveň se stanoví způsob, jakým bude odkazovaná technická norma zpřístupněna veřejnosti. Technickou normu, na kterou se v právním předpisu odkazuje

		formou výlučného odkazu, je nutné jednoznačným způsobem identifikovat, a to normativním odkazem uvedením označení, data vydání a úplného názvu technické normy v textu právního předpisu. Vyhlášky pro vyšší a nižší režim nejsou součástí tohoto mezirezortního připomínkového řízení. Váš podnět zaevidujeme a bude zahrnut do mezirezortního připomínkového řízení k vyhláškám, které proběhne na začátku příštího roku. Do té doby, pokud vyhodnotíme, že jsou nedostatečně jasná pravidla zavedení TLP, text upravíme či doplníme. Ad 2: Neakceptováno Oblasti uvedené v příloze jedna je nutné zohlednit, máme za to, že § 8 vnímáme rozdílně. TLP není povinný, je na zvážení povinné osoby, zda se rozhodne využívat jiné řešení pro zajištění klasifikace informací, či zda tato potřeba není. Vyhlášky pro vyšší a nižší režim nejsou součástí tohoto mezirezortního připomínkového řízení. Váš podnět zaevidujeme a bude zahrnut do mezirezortního připomínkového řízení k vyhláškám, které proběhne na začátku příštího roku. Ad 3: Neakceptováno Jedná se o transpozici směrnice EU, OPP není dostačující pro naplnění požadavků Komise. Zákonný předpis je proto jedinou možností, jak postupovat. OPP využíváme například nově u problematiky bezpečnosti dodavatelského řetězce. Navíc si neumíme ani prakticky představit, jak by v tomto případě proces vydání OOP probíhal. Ad 4: Vysvětleno

			Zřízení "single point of entry" je v NIS2 ponecháno na dobrovolné bázi, zákonná úprava tak není nutná. Ad 5: Neakceptováno. Bez snahy vyhnout se vypořádání relevantních připomínek a bez snahy jakkoliv poškodit dlouhodobě dobré vztahy mezi ÚOOÚ a NÚKIB je nutné tuto připomínku neakceptovat, protože bez označení konkrétních podnětů, které "se nepodařilo vyřešit v rámci veřejné konsultace", není NÚKIB schopen tyto konkrétně identifikovat - nevíme, které podněty - ať už byly v neoficiálním připomínkovém řízení vypořádány jakýmkoliv způsobem - považuje ÚOOÚ za doposud nevyřešené (i neakceptované podněty mohou být brány jako vyřešené). Připomínkové místo s vypořádáním souhlasí.
545. Úřad pro ochranu osobních údajů	Z	V § 2 odst. 1 písm. e) a na všech ostatních místech se slovo „regulovanou“ nahrazuje slovem „kybernetickou“. <i>Regulovanou službou je prakticky cokoliv, od divadelního představení po zásah dobrovolných hasičů. Je proto vysoce nevhodné takto obecný pojem používat v tak úzkém významu.</i>	Vysvětleno Použití pojmu kybernetická služba by bylo značně zavádějící pro adresáty návrhu zákona. Pod tímto pojmem si typicky nikdo nepředstaví poskytování zdravotnických služeb, provozování ropovodu či distribuci elektrické energie, což jsou mj. odvětví, resp. specifické služby, na něž má návrh zákona dopadat. Obdobně stávající zákon pracuje z pojmem "základní služby", který je obsažen ve směrnících NIS1 a CER. Spektrum odvětví, na které stávající i nový zákon o kybernetické bezpečnosti dopadají, je natolik široký, že je třeba použít obecný pojem, který je v zákoně důsledně definován. Nemůže tak být pochyb o tom, že regulovanou službou dle zákona o kybernetické bezpečnosti nebude výjezd dobrovolných hasičů nebo divadelní představení.

			Závěr: Po písemné komunikaci připomínkové místo od připomínky ustoupilo a připomínka byla tímto vypořádána.
546. Úřad pro ochranu osobních údajů	D	V § 6 odst. 2 se slova „režim vyšších povinností“ nahrazují slovem „strategický“ a slova „režim nižších povinností“ nahrazují slovem „významný“. <i>Pochopitelnější nomenklatura, cf. § 26. Směrnice používá pojmy „základní“ a „důležitý“.</i>	Vysvětleno Návrh zákona se cíleně odklání od výslovného okopírování směrnicí stanoveného rozdělení povinných osob na "essential" a "important" (snahou bylo tuto informaci uvést již na začátku důvodové zprávy - např. "Požadavky stanovené směrnicí NIS 2 jsou ve svém důsledku takové povahy, že návrh zákona musí s ohledem na změnu dosavadního přístupu k oblasti kybernetické bezpečnosti upravit nejen některé dílčí oblasti tak, aby bylo možné sladit požadavky směrnice NIS 2 s dosavadním způsobem regulace kybernetické bezpečnosti, ale především musí dojít k podstatným změnám v oblasti stanovení a identifikace povinných osob, změn interních procesů a dalších náležitostí, které přinesly požadavky na další dílčí úpravy zákona o kybernetické bezpečnosti." apod.). Důvodem pro odklon od směrnicí používaného pojmenování subjektů bylo, že výsledné množiny subjektů ve vyšším a nižším režimu povinností jsou širší, než množiny dané směrnicí, protože nad rámec směrnice reflektují také národní požadavky na kybernetickou bezpečnost (např. z důvodů národní bezpečnosti, tedy mimo působnost směrnice nebo primárního práva EU). Podstatou tedy je, že režim nižších povinností odpovídá množině "important" a dalším národním požadavkům, režim vyšších povinností odpovídá množině "essential" a dalším národním požadavkům. Tento postup je sám směrnicí NIS2 předvídan zejm. čl. 5 - princip minimální

			harmonizace. Odklon od používání pojmů "essential" a "important" ze směrnice byl podpořen také tím, že v českém jazyce není pojmosloví využívané směrnicí vhodné a odpovídající. "Základní" subjekty jsou fakticky významnější než subjekty "důležité", což dlouhodobě způsobuje nepochopení mezi adresáty. Výše uvedené jsme se snažili podchytit v důvodové zprávě zejm. na s. 103. V návaznosti na tuto připomínku uvedeme výše uvedené vysvětlení ještě výslovně v tomto textu. Typ povinné osoby "subjekty poskytující služby registrace jmen domén" obsahuje stejně jako v případě směrnice NIS2 jinou sadu povinností (čl. 28), a i když se mohou subjekty fakticky překrývat (např. registr domén nejvyšší úrovně bude jak poskytovatelem regulované služby v režimu vyšších povinností (ve smyslu "essential"), tak má také povinnosti jako subjekt poskytující registrace jmen domén. Máme za to, že tento postup je se směrnicí souladný. Připomínkové místo s vypořádáním souhlasí.
547. Úřad pro ochranu osobních údajů	Z	Ustanovení §§ 8 a 10 je nezbytné přepracovat. Registrace a evidence je v zásadě to samé. Rozdílová tabulka uvádí k § 10 odkaz na přechodné ustanovení směrnice 32022L2555, a proto není přesvědčivá.	Vysvětleno Čl. 5 odst. 6 Legislativních pravidel vlády: "Připomínky, musejí být formulovány jednoznačně a konkrétně, musejí být řádně odůvodněny a je-li požadováno nahradit určitý text jiným textem, musí být navržena nová formulace." Uvedená připomínka zcela postrádá návrh nové formulace. Přesto k uvedenému připomínce uvádíme, že se skutečně nejedná "v zásadě o to samé". Jedná se o různé fáze celého procesu, kterým se budou subjekty dostávat do regulace. Navržená úprava činí tento proces univerzálně použitelným vůči všem způsobům, jak se může regulovaná služba do evidence dostat (§ 8 odst.

			1 až 4). Tedy sebeidentifikace či doregistrace Úřadem na základě identifikačních kritérií nebo určení regulované služby rozhodnutím Úřadu. Teprve na základě registrace je proveden zápis do evidence. V případě sebeidentifikace k tomu dojde automaticky, a rovněž bude vygenerována automatická notifikace, že byla služba zapsána do evidence (tj. vyznění o zapsání do evidence regulovaných služeb). Od doručení tohoto vyznění se pak spouští téměř všechny zákonné povinnosti v ZKB. Tyto dvě fáze jsou důležité z hlediska funkčnosti celého procesu a samotného portálu NÚKIB. Připomínkové místo s vypořádáním souhlasí.
548. Úřad pro ochranu osobních údajů	Z	Ustanovení § 12 odst. 1 a 2 je nezbytné přepracovat. Pojem „registrační údaje“ není vhodný. Rozlišování registračních údajů jako identifikačních údajů PO a kontaktních údajů jako identifikačních údajů FO je v rozporu s doktrínou. Předdefinování standardních termínů na něco jiného je matoucí.	Vysvětleno Čl. 5 odst. 6 Legislativních pravidel vlády: "Připomínky, musejí být formulovány jednoznačně a konkrétně, musejí být řádně odůvodněny a je-li požadováno nahradit určitý text jiným textem, musí být navržena nová formulace." Uvedená připomínka postrádá návrh nové formulace. Přesto k uvedené připomínce uvádíme, že provedené rozdělení registračních a kontaktních údajů reflektuje, že jde v konečném důsledku o informace hlášené ze strany poskytovatele regulované služby. Navíc je reflektován proces registrace a proces hlášení, kdy může dojít v prvotní fázi k "registraci regulované služby" a následně teprve k nahlášení kontaktních údajů pověřených fyzických osob. Není nám jasné, jaký předpis obsahuje standardní definici těchto pojmů, resp. na jakou doktrínu je odkazováno. Konkrétní obsah těchto pojmů je navíc stanoven ve vyhlášce o Portálu NÚKIB.

			Závěr: Po písemné komunikaci připomínkové místo od připomínky ustoupilo a připomínka byla tímto vypořádána.
549. Úřad pro ochranu osobních údajů	D	V § 38 se slova „zajištění vnitřního či veřejného pořádku a bezpečnosti“ nahrazují slovy „zajištění veřejného pořádku a národní bezpečnosti“. <i>Standardní vymezení kautel.</i>	Neakceptováno - nyní § 39 Na vhodném znění celé soustavy ustanovení o stavu kybernetického nebezpečí spolupracujeme s Ministerstvem vnitra – Generálním ředitelstvím Hasičského záchranného sboru a návrh bude upraven na základě těchto jednání. Vámi navrhovaná změna však neodpovídá plánovanému použití pojmů v rámci krizového řízení, které bylo ujednáno s gestorem krizové legislativy. Připomínkové místo s vypořádáním souhlasí.
550. Úřad pro ochranu osobních údajů	Z	V § 48 je odstavec 2 nezbytné přepracovat. <i>Drtivou většinu těchto údajů již stát má. NÚKIB si je proto musí načerpat pomocí RPP.</i>	Akceptováno - nyní § 51 S ohledem na úpravu bezdlužnosti (viz § 51 odst. 1 písm. d)) bude Úřad jako správní orgán, žádat potvrzení k prokázání daňové bezdlužnosti podle odst. 51 odst. 1 písm. d) bod 1 a 2. od příslušného orgánu Finanční a Celní správy České republiky na základě prolomení daňové mlčenlivosti podle § 53 odst. 1 písm. l) zákona č. 280/2009 Sb., daňový řád ve znění pozdějších předpisů. Žadatel o registraci členství v Komunitě tak nebude zatížen jejich předkládáním. Připomínkové místo s vypořádáním souhlasí.
551. Úřad pro ochranu osobních údajů	Z	V § 53 se zrušuje podtržení. <i>Podle rozdílové tabulky se zde transponuje právní norma: „14. Subjekty, příslušné orgány, jednotná kontaktní místa a týmy CSIRT</i>	Akceptováno Ustanovení nebude podtrženo. Připomínkové místo s vypořádáním souhlasí.

		zpracovávají osobní údaje pouze v rozsahu nezbytném pro účely této směrnice a v souladu s nařízením (EU) 2016/679 a takové zpracování se opírá o článek 6 uvedeného nařízení.“ <i>S tím však nelze souhlasit. Tato právní norma je obecný pokyn pro celý návrh, nikoliv, že má být stanovena explicitně.</i>	
552. Úřad pro ochranu osobních údajů	Z	V § 53 se odstavec 1 zrušuje. <i>Tato právní norma nepřináší žádnou přidanou hodnotu oproti obecným principům ochrany osobních údajů.</i>	Akceptováno Ustanovení bude vypuštěno. Připomínkové místo s vypořádáním souhlasí.
553. Úřad pro ochranu osobních údajů	D	Nadpis § 56 zní: „Správní dozor“. <i>Přesnější pojem.</i>	Neakceptováno - nyní § 58 Chápeme důvod této připomínky, avšak fázi kontroly, kterou upravuje toto ustanovení, provádíme podle kontrolního řádu, preferujeme proto vymezení oproti správnímu řízení, kam přesahuje správní dozor. Správní dozor je také širší množina dohledových činností správních úřadů. Chceme také zachovat kontinuitu s původním názvem ustanovení v předchozí právní úpravě. Dle našeho názoru se "dozor" používá ve spojení např. úřad vykonává dozor nad plněním povinností orgány a osobami podle tohoto zákona nebo úřad vykonává dozor v oblasti kybernetické bezpečnosti. Kontrola se pak používá spíše konkrétněji např. úřad nebo Národní úřad pro kybernetickou a informační bezpečnost kontroluje, zda druhý účastník smlouvy dodržuje ustanovení tohoto zákona, prováděcích právních předpisů a uzavřené smlouvy. Kontrolní činnost máme také vymezenou ustanovení § 44 nZKB, kde se hovoří o kontrole, v rámci terminologické jednotnosti trváme na jejím zachování (obdobně jako tomu je například v zákoně o ochraně utajovaných informací). Cílíme v

			tomto ustanovení na kontrolu v užším slova smyslu nikoliv na obecnou formu / způsob správní činnosti Úřadu. Připomínkové místo s vypořádáním souhlasí.
554. Úřad pro ochranu osobních údajů	D	V § 56 odst. 3 se za slovo „zaměstnanci“ vkládá slovo „v“. <i>NÚKIB nemá právní subjektivitu, a tedy ani žádné zaměstnance.</i>	Akceptováno jinak - nyní § 58 I s ohledem na jiné připomínky jsme vyhodnotili, že nejlepší bude předmětný odst. 3 v § 58 zcela zrušit. Připomínkové místo s vypořádáním souhlasí.
555. Úřad pro ochranu osobních údajů	Z	Část 8 obecné části důvodové zprávy, zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů (dále jen "DPIA"), je nezbytné přepracovat. <i>Ani ve veřejné konzultaci se nepodařilo DPIA dostatečně konkretisovat. Jinde je zase konkretisace přehnaná, zejména ve vymezení agend. Předkladatel při zpracování DPIA sice vyšel návrhu doporučení legislativního DPIA,² ale jeho tvrzení jsou často příliš obecná – týká se to zejména výjimek z ochrany osobních údajů – jinde dokonce nesprávná. Je paradoxní, že § 53 odst. 2 a 3 je podrobnější než DPIA, ačkoliv by to mělo být naopak.</i> <i>Týká se to zejména právního základ zpracování osobních údajů. Tím není „návrh zákona o kybernetické bezpečnosti“, protože to byla definice kruhem. Je totiž nezbytné stanovit, co je právním základem zpracování osobních údajů podle zákona o kybernetické bezpečnosti.</i> <i>Dále do DPIA nepatří hypotézy: „Bude-li konkrétní zpracování osobních údajů spadat do působnosti obecného nařízení o ochraně osobních údajů“, nýbrž je nezbytné rovnou stanovit, které zpracování</i>	Akceptováno Důvodová zpráva bude upravena a doplněna ve smyslu uplatněné připomínky. Připomínkové místo s vypořádáním souhlasí.

² <https://www.uoou.cz/metodika-pro-legislativni-dpia/ds-7270/archiv=1&p1=1257>.

		<i>podléhá GDPR. Stejně tak místo obecného tvrzení: „Veškeré zpracování osobních údajů se pak bude řídit zákonem o zpracování osobních údajů“, by mělo být uvedeno, která zpracování se budou řídit hlavou IV ZZOÚ.</i> <i>Místo obecného odkazu na § 41 by mělo být uvedeno, které pravomoci vyžadují zpracování osobních údajů.</i> <i>V neposlední řadě je třeba opravit terminologii. „Titul“ je právní institut pouze při zpracování těch osobních údajů, které NÚKIB již má, nikoliv těch, které teprve hodlá mít.</i> <i>Dále, byť to není v působnosti ÚOOÚ, lze mít za to, že počet agend je přehnaný. Spíše by měl odpovídat vymezeným účelům, které by pak bylo možné zestručnit na skutečný účel agendy, např. „komunikace Úřadu a regulovaných organizací“, „plnění informační povinnosti Úřadu“/„poskytnutí součinnosti“, „prověřování důvěryhodnosti“/„posouzení způsobilosti“ a „dozor plnění povinností“.</i>	
556. Úřad pro zastupování státu ve věcech majetkových	Z	Kritéria pro identifikaci regulované služby Návrh zákona opouští pojem „významný informační systém“ a s tím související vyhlášku č. 317/2014 Sb. Tato vyhláška užívá pojem „organizační složka státu“ (§ 2 odst. 1 této vyhlášky), od čehož je ovšem v návrhu vyhlášky o regulovaných službách upuštěno – zde jsou v příloze k části „veřejná správa“ zahrnuty ústřední orgány státní správy, správní úřady s celostátní působností, a další vyjmenované veřejnoprávní korporace. Úřad pro zastupování státu ve věcech majetkových je sice organizační složkou státu, ovšem není ústředním orgánem státní správy, ani správním úřadem s celostátní působností, neboť nevykonává „vrchnostenskou moc“, ale vystupuje za stát pouze v soukromoprávních vztazích (srov. např. důvodová zpráva k zákonu č. 51/2016 Sb.).	Akceptováno ÚZSVM bude v příloze vyhlášky o regulovaných službách v části 1.1 doplněn (pod písm. m), subjekty nyní uvedeny pod písm. m) - r) budou přesunuty pod písm. n) - s)). Připomínkové místo s vypořádáním souhlasí.

		Z výše uvedeného důvodu požadujeme výslovné uvedení Úřadu pro zastupování státu ve věcech majetkových do přílohy k vyhlášce o regulovaných službách, a to konkrétně ke službě 1.1 Výkon svěřených pravomocí, I. režim vyšších povinností.	
557. Úřad pro zastupování státu ve věcech majetkových	Z	Speciální úprava předání informací a dat od významného dodavatele Z návrhu ustanovení lze dospět k závěru, že v případě absence smluvního závazku se poskytovatel regulované služby v režimu vyšších povinností nemůže této ingerence NÚKIB dovolat. Tato varianta ale dle našeho názoru nahrává „obstrukčním praktikám“ významných dodavatelů, kteří budou právě s odkazem na toto ustanovení namítat, že nelze se takové ingerence domoci právě s odkazem na nedostatečnost smluvního ujednání. Z ust. odst. 4 tohoto paragrafu je ale zjevné, že záměrem ustanovení je řešit smluvní a správní problematiku odděleně. Jakkoliv toto může být vnímáno jako snaha o zajištění „správného přístupu“ poskytovatelů regulovaných služeb, v konečném důsledku lze mít spíše za to, že tento postup bude kontraproduktivní a postačí pouze obecná povinnost k tomuto jednání dle § 24 návrhu. Požadujeme tedy, aby ingerence NÚKIB dle tohoto ustanovení nebyla podmíněna „výzvou ke splnění smluvního závazku předat informace a data“, ale pouze „výzvou k předání informací a dat“. Rovněž by se toto ustanovení mělo výslovně vymežit vůči autorskoprávní ochraně počítačových programů a databází tak, že tato ochrana sice není dotčena, ale stejně jako jednání o účelně vynaložených nákladech nesmí být překážkou splnění povinnosti.	Akceptováno Povinnost mít předání dat smluvně upraveno byla z dotčeného ustanovení odstraněna s ohledem na skutečnost, že institut předání dat míří na krajní případy, kdy by hrozící či probíhající kybernetický bezpečnostní incident mohl mít závažný vliv na poskytování regulované služby s dopadem na zachování základních funkcí státu, hospodářských činností, bezpečnosti, veřejného zdraví, majetku nebo životního prostředí. V takovém případě převládá zájem státu na odvrácení incidentu s takto významným dopadem nad soukromoprávním dohodou o předání dat. Úřad svou činností nijak nenahrazuje či nesupluje úlohu obecných soudů při řešení soukromoprávních sporů týkajících se výkladu uzavřené smlouvy a jeho činnost končí tam, kde končí ohrožení regulované služby a regulovaných aktiv kybernetickým bezpečnostním incidentem. Vedle toho platí, že poskytovatel regulovaných služeb v režimu vyšších povinností bude povinen zavádět bezpečnostní opatření, jejichž součástí je povinnost zanést do smlouvy specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání povinnou osobou. Vzhledem k tomu, že příslušná ujednání by měla být součástí smluvního vztahu mezi poskytovatelem regulované služby a významným dodavatelem, měl by institut předání dat podle § 25 sloužit jako ultima ratio až poté, co selžou jednání mezi dotčenými stranami.

			Odst. 4 předmětného ustanovení byl upraven následovně: "Jednání o úhradě účelně vynaložených nákladů spojených s předáním informací a dat a případné finanční kompenzaci práv duševního vlastnictví nesmí být překážkou řádného splnění povinnosti předat informace a data." Připomínkové místo s vypořádáním souhlasí.
558. Úřad pro zastupování státu ve věcech majetkových	D	Přechodná ustanovení Dle důvodové zprávy platí, že v případě nižších povinností nebude nutné plnit ta opatření, která v případě nové právní úpravy nebudou, na rozdíl od stávající úpravy, potřebná. V případě vyšších povinností pak platí, že minimální rozsah bude v nové právní úpravě totožný, proto je třeba plnit veškeré povinnosti dle stávající právní úpravy i do budoucna. Bohužel důvodová zpráva nepřibližuje, jak se bude postupovat v případě, kdy režim vyšších povinností bude zakládat zcela nové povinnosti v porovnání se stávající právní úpravou.	Akceptováno Bude opravena chyba ve formátování, věta „a to od okamžiku nabytí účinnosti tohoto zákona až do doby uplynutí lhůt pro zahájení plnění povinností podle tohoto zákona, s výjimkou způsobu hlášení kybernetických bezpečnostních incidentů, který jsou tito poskytovatelé regulované služby povinni realizovat podle tohoto zákona od okamžiku doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb.“ je společná pro body a) i b), tzn. pro oba režimy platí, že dosavadní regulované subjekty plní stanovenou úroveň povinností podle staré úpravy do doby zahájení plnění povinností podle nové úpravy, nejpozději do uplynutí přechodné lhůty 1 roku pro zavedení bezpečnostních opatření podle nové úpravy. Pokud povinnosti stanovené pro vyšší režim stanovují oproti současné úpravě nové povinnosti, tyto nové povinnosti budou zaváděny do praxe postupně ve lhůtě k tomu určené, nejpozději začnou být plněny po uplynutí lhůty pro zahájení plnění povinností. Dále bude pro větší srozumitelnost doplněna i důvodová zpráva k návrhu zákona. Připomínkové místo s vypořádáním souhlasí.

559. Ministerstvo průmyslu a obchodu	D	Doporučujeme celý návrh zákona prověřit z hlediska formulace přestupků tak, aby přestupky reflektovaly pouze povinnosti. V návrhu zákona je často odkazováno na celý paragraf nikoli na povinnost, jejíž porušení dojde ke spáchání přestupku. Např. § 58 odst. 1 písm. g) stanovuje, že poskytovatel regulované služby se dopustí přestupku tím, že v rozporu s § 14 nezavede nebo neprovádí bezpečnostní opatření. Avšak § 14 v odst. 1 stanoví co se rozumí bezpečnostním opatřením, v odst. 2 stanovuje povinnost poskytovateli zavést a provádět bezpečnostní opatření, odst. 3 upravuje lhůtu pro zavedení a provádění bezpečnostních opatření a odst. 4 upravuje, že prováděcí předpis stanoví bezpečnostní opatření odpovídající režimu poskytovatele regulované služby. Vzhledem k tomu, že § 14 odst. 1 a 4 neobsahují povinnosti nelze přestupek vztáhnout obecně na § 14. Obdobně pak u přestupků týkajících se § 21 a § 23.	Akceptováno Upraveno dle připomínky. Připomínkové místo s vypořádáním souhlasí.
560. Ministerstvo průmyslu a obchodu	D	V důvodové zprávě chybí náležitosti podle čl. 9 Legislativních pravidel vlády, a to konkrétně zhodnocení souladu navrhovaného řešení se zásadami tvorby digitálně přívětivé legislativy.	Vysvětleno Zhodnocení souladu se zásadami pro tvorbu digitálně přívětivé legislativy je obsaženo v Závěrečné zprávě z hodnocení dopadů regulace (RIA), konkrétně v kapitole 3. Agregované dopady, u každého relevantního dopadu jde o poslední odstavec. Připomínkové místo s vypořádáním souhlasí.
561. Ministerstvo průmyslu a obchodu	D	K materiálu (III): <u>K § 27, 28 a 30 (a k relevantním částem důvodové zprávy):</u> Oceňujeme, že do zákona byl doplněn výslovný odkaz na bezpečnost a veřejný pořádek. Domníváme se, že znění zákona je díky tomu právně jistější a zvyšuje se pravděpodobnost, že by bylo shledáno jako v souladu s právem WTO. Je zároveň ovšem nutné podotknout, že ve vztahu k dodávkám zboží stále existuje riziko, že by ustanovení mohlo být problematizováno s ohledem na to, že GATT 1994 veřejný pořádek neuvádí v seznamu výjimek pro omezení obchodu zbožím, uvádí jen veřejnou morálku (čl. XX a) GATT 1994).	Vysvětleno Výsledkem rešerše a konzultací k možnému propojení vnitřního a vnějšího pořádku s veřejnou morálkou jsme dospěli k závěru, že tyto instituty za určitých okolností propojit lze (obzvlášť s akcentem na možnost konzultací a přizpůsobení jednotlivých podmínek případného opatření obecné povahy, zakazujícího či omezujícího rizikového dodavatele), tudíž by se v tomto případě (konkrétně z důvodu bezpečnostní výjimky) mělo jednat o soulad s právem

		WTO. Navíc je stále k dispozici výjimka dle článku XXI, která je dle nejnovějšího vývoje tzv. "self-judging" a zaručuje možnost výjimky z důvodu národní bezpečnosti. Reakce připomínkového místa: Vypořádání nepovažujeme za dostatečné. Myšlenku ustavení BDŘ silně podporujeme, a proto nechceme blokovat přijetí zákona. Nicméně otázku souladu mechanismu s mezinárodněprávními závazky ČR považujeme za skutečně velmi důležitou. Uvedené vysvětlení proto vnímáme jako příliš obecné a nedostačující. Neodkazuje na zdroje ani konkrétní poznatky z konzultací. Judikatura WTO pojmy porušení veřejného pořádku a porušení veřejné morálky rozlišuje. Není nám proto jasné, jaká kritéria by měla být naplněna, aby mohlo být porušení veřejného pořádku zahrnuto pod pojem porušení veřejné morálky. Co se týče čl. XXI GATT 1994 a konceptu „self-judging“, máme k němu rozsáhlé výhrady a domníváme se, že není možno se na něj v aktuální situaci odvolávat. Je třeba jej vykládat co nejužší. V opačném případě jde o silně protekcionistický přístup, který není v souladu s dlouhodobou pozicí a zájmy ČR ani EU. V této souvislosti upozorňujeme na snahy Evropské komise v rámci WTO dokázat, že tato bezpečnostní výjimka nemůže být „self-judging“. Pokud NÚKIB provedl rešerše a konzultace, bylo by vhodné jejich výsledky, zvláště pokud potvrzují soulad nástroje s mezinárodním právem, a související úvahy uvést pokud možno co nejdětailněji do důvodové zprávy do části týkající se souladu s

			mezinárodním právem (kap. 6.2 obecné části DZ), popř. do zvláštní části DZ, do vysvětlení k relevantním ustanovením (např. § 31). Vnímáme to i do budoucna za důležitý krok pro případ, že by takový soulad měl být zpochybňován, a jako určitou prevenci toho, aby k tomu vůbec došlo. Reakce NÚKIB: Zaslán návrh na doplnění odůvodnění. Závěr: Vysvětleno. Výsledkem rešerše a konzultací k možnému propojení vnitřního a vnějšího pořádku s veřejnou morálkou jsme dospěli k závěru, že tyto instituty za určitých okolností propojit lze (obzvláště s akcentem na možnost konzultací a přizpůsobení jednotlivých podmínek případného opatření obecné povahy, zakazujícího či omezujícího rizikového dodavatele), tudíž by se v tomto případě (konkrétně z důvodu bezpečnostní výjimky) mělo jednat o soulad s právem WTO. Zároveň se v daném případě bude v návaznosti na konkrétní případy pracovat jak s čl. XX GATT, tak i s výjimkou podle čl. XXI GATT vztahující se k zajištění bezpečnosti země, tzn. bezpečnosti ČR. Důvodová zpráva byla v tomto ohledu doplněna a pracuje tak jak se specifickými výjimkami podle čl. XIV GATS a XX GATT, tak i bezpečnostními výjimkami podle čl. XVIbis GATS a XXI GATT.
562. Ministerstvo průmyslu a obchodu	D	K materiálu (III): <u>K § 29 odst. 1 zákona:</u> Není zde zcela jasné, v jakých případech vyjmenované orgány poskytují stanovisko, kdy informace a kdy pouze součinnost, vč. toho, kdo o tom bude rozhodovat. Zároveň by podle našeho názoru bylo vhodné upřesnit, jakou povahu poskytnuté	Akceptováno - nyní § 30 Důvodová zpráva byla doplněna tímto způsobem: "Stanovisko poskytnuté orgánem státu bude mít nezávaznou povahu, a tudíž k němu bude Úřad toliko

		stanovisko bude mít (zda bude pro Úřad závazné, bude k němu jen přihlížet apod.). Tyto nejasnosti by se možná daly vyřešit podrobnějším vysvětlením v důvodové zprávě (případně i uvedením příkladů). Současná formulace odkazující na kritérium potřeby není zcela jasná. Tato specifikace/vyjasnění má za cíl prevenci procesních nejasností při aplikaci zákona.	přihlížet. Společně s ostatními zdroji pak bude Úřad i na jeho základě vyhodnocovat naplnění kritérií rizikovosti dodavatele.". Vyjmenované orgány budou poskytovat stanovisko nebo informace s přihlédnutím ke konkrétní situaci a potřebám, které vyhodnotí Úřad. Jiná součinnost orgánů v tomto procesu byla ze zákona na základě jiných připomínek vyškrtána. Lze předpokládat, že po uvedených orgánech bude primárně vyžadováno výše zmíněné stanovisko, jehož povaha bude nezávazná, a v případech, kde se bude jevit vhodnější vyžádání informace, tak bude učiněno. Úprava je koncipována tak, aby v případě potřeby mohl Úřad získat další informace a případné vydání opatření obecné povahy tak bylo založeno na největším možném množství informací. Reakce připomínkového místa: Se způsobem vypořádání můžeme souhlasit. Nicméně v souvislosti s úpravou § 30 došlo také k úpravě formulace týkající se výjimek z mlčenlivosti podle jiných právních předpisů. Aby se MPO mohlo efektivně podílet na fungování BDŘ ve smyslu předávání potřebných informací, bude třeba upravit i výjimky z mlčenlivosti podle ZoPZI. Prosíme tedy o doplnění § 30 odst. 5 o nové písm. e) ve znění: „e) Ministerstvem průmyslu a obchodu, jedná-li se o informace zjištěné v souvislosti s řízením nebo konzultací podle zákona o prověřování zahraničních investic^{x)}.“ A doplnění odkazu na poznámku pod čarou ve znění:

			„^{x)} Zákon č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic).“ Reakce NÚKIB: Připomínka byla akceptována a bylo doplněno výše požadované jako nové písmeno d).
563. Ministerstvo průmyslu a obchodu	D	K materiálu (III): <u>K § 58 odst. 3 – formulace přestupku:</u> „...nevynaloží přiměřené úsilí k zjištění informace o dodavateli bezpečnostně významné dodávky podle § 32 odst. 1 písm. a),“ – z hlediska zásad správního trestání je otázkou, zda ve skutkové podstatě přestupku je kritérium „přiměřené úsilí“ dostatečně určité, a to zejména v situaci, když (dokud) nebudou Úřadem vydány metodické či výkladové materiály (jejichž relevance při formulaci/upřesnění skutkové podstaty správního deliktu je ovšem také problematická vzhledem k zásadě <i>nullum crimen sine lege scripta</i>, která se dle našeho názoru aplikuje i na správní trestání)	Akceptováno - nyní § 60 Na základě této a dalších připomínek byl § 60 odst. 3 přetextován a nově již neobsahuje pojem "přiměřené úsilí". Připomínkové místo s vypořádáním souhlasí.
564. Ministerstvo průmyslu a obchodu	D	K materiálu (III): <u>K nadpisu § 62:</u> Nadpis „Vztah ke správnímu a kontrolnímu řádu“ plně neodpovídá obsahu daného paragrafu. Dáváme ke zvážení jeho možné přejmenování.	Akceptováno - nyní § 64 Název ustanovení § 64 změněn na "Zajištění účelu a průběhu řízení", přičemž původní odstavec 4, který zní "Exekuce rozhodnutí Úřadu ukládajícího povinnost předat nebo jinak naložit s informacemi a daty se řídí ustanoveními správního řádu upravujícími exekuci odebráním movité věci.", je přesunutý k § 26, ke kterému se vztahuje. Připomínkové místo s vypořádáním souhlasí.
565. Ministerstvo průmyslu a obchodu	D	K materiálu (III): Dle § 48 odst. 4 písm. c) návrhu zákona je způsobilá požádat o členství v Komunitě kompetencí pro kybernetickou bezpečnost pouze taková právnická osoba, jejíž skutečným majitelem je osoba usazená na území členských států Evropské unie a členských států Evropského sdružení volného obchodu. V čl. 8 odst. 3 nařízení EP a rady	Vysvětleno Máme za to, že omezení je dáno samotným nařízením Evropského parlamentu a Rady (EU) 2021/887. Uvedené omezení plyne ze samotné preambule nařízení, která zdůrazňuje současnou závislost EU v

		č.2021/887, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center je uvedeno, že registrovanými členy Komunity se stávají pouze subjekty usazené v členských státech, nicméně již zde není požadavek na majitele a jeho usazení. Národní požadavek jde tedy zřejmě nad rámec povinností stanovených přímo účinným předpisem Unie. Tento postup může vyslat negativní signál těm partnerům mimo EU, se kterými má ČR jinak intenzivní bilaterální vztahy a spolupracuje s nimi v různých oblastech včetně ekonomické, bezpečnostní a vojenské (zejm. USA, Kanada a Izrael). Žádáme o zvážení zahrnutí i třetích zemí s ekvivalentní právní úpravou, jako má EU.	oblasti kybernetické bezpečnosti na neevropských dodavatelích a formuluje cíl učinit z EU vedoucí sílu v oblasti kybernetické bezpečnosti s cílem zvyšovat mimo jiné bezpečnost sítí a informačních systémů, včetně internetu a dalších infrastruktur s kritickým významem pro fungování společnosti. Vysoká bezpečnost sítí a informačních systémů v celé EU má tak zásadní význam pro společnost a hospodářství, neboť její narušení může mít dopady nejen na jednotlivé členské státy ale i na EU jako celek. Nařízení tak podmiňuje členství v Komunitě tím, že subjekt musí být usazen v členském státu, v našem případě v ČR. Současně nařízení umožňuje každému členskému státu formulovat vlastní bezpečnostní důvody, při jejichž naplnění bude žadatel vyhodnocen jako nezpůsobilý pro členství v Komunitě. Vnitrostátní bezpečnostní důvody jsou tak formulovány s ohledem na skutečnost, že Komunita má představovat rozsáhlou, otevřenou, interdisciplinární a různorodou skupinu evropských zúčastněných stran zapojených do rozvoje technologií kybernetické bezpečnosti, a celkově přispět k posílení konkurenceschopnosti a kapacit EU v oblasti kybernetické bezpečnosti. Reakce připomínkového místa: Nesouhlasíme s vysvětlením. Tímto nijak nechceme zpochybňovat právo členského státu zohledňovat bezpečnostní důvody a možnost na jejich základě odmítnout registraci právnické osoby jako člena Komunity. Návrh ustanovení §51 odst. 5 písm. b) (původní ustanovení §48(4) písm. c)) však v tomto ohledu vykračuje podle našeho názoru nad rámec ustanovení čl. 8 odst. 4 nařízení (EU) 2021/887. Předmětné ustanovení nařízení jasně stanoví, že

		„Kompetenční centrum zaregistruje jako členy Komunity subjekty na jejich žádost po posouzení národním koordinačním centrem členského státu, v němž jsou tyto subjekty usazeny, potvrzujícím, že tyto subjekty splňují kritéria stanovená v odstavci 3 tohoto článku. V tomto posouzení se rovněž zohlední jakékoliv příslušné vnitrostátní posouzení, jež z bezpečnostních důvodů provedly příslušné vnitrostátní orgány.“. Navrhované znění zákona oproti tomu jednoduše předjímá, že je-li skutečný majitel právnické osoby usazený mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, není tato právnická osoba a priori způsobilá k členství v Komunitě, a to aniž by Úřad jakkoliv posuzoval případná bezpečnostní rizika spjata s konkrétním žadatelem/právnickou osobou, která by byla legitimním důvodem pro odmítnutí členství v Komunitě. Jak jsme již uvedli v naší původní připomínce, může úprava v navržené podobě vyslat negativní signál těm partnerům mimo EU, se kterými má ČR jinak intenzivní bilaterální vztahy a spolupracuje s nimi v různých oblastech včetně ekonomické, bezpečnostní a vojenské (zejm. USA, Kanada a Izrael). Silně proto doporučujeme zohlednění této připomínky a zakotvení možnosti odmítnout členství v Komunitě z bezpečnostních důvodů odlišným způsobem, který by odpovídal úpravě předmětného nařízení, tj. posouzení skutečných bezpečnostních rizik až v rámci samotného posuzování žádosti o členství v Komunitě a nespojování způsobilosti k členství s místem usazení skutečných majitelů právnické osoby.

			Reakce NÚKIB: Zaslán návrh na doplnění odůvodnění. Reakce připomínkového místa Nadále doporučujeme upravit navrhované ustanovení § 51 odst. 5 písm. b), neboť se domníváme, že navržené znění jde nad rámec ustanovení nařízení (EU) 2021/887. Schválení zákona v tomto znění by mohlo vést k diskriminaci společností s třetizemským skutečným majitelem usazených v ČR oproti společnostem s třetizemským skutečným majitelem usazeným v jiných ČS a v tomto smyslu by mohlo představovat riziko zahájení řízení o porušení Smlouvy EU. Nicméně finální posouzení ponecháváme gestorovi. Pozice gestora je dle doplněné důvodové zprávy postavena na argumentu transparentnosti vůči všem žadatelům o členství v Komunitě. Text čl. 8 odst. 4 nařízení nicméně dle našeho názoru vyznívá v tom smyslu, že v rámci posuzování splnění (nařízením stanovených) podmínek mají být posouzena i případná bezpečnostní rizika týkající se žadatele. Text nařízení je přitom postaven na principu individuálního posouzení jednotlivých žádostí ve vztahu ke konkrétním žadatelům. Nařízení navíc neumožňuje ČS stanovit si další (obecné) požadavky nad rámec požadavků stanovených nařízením. Obáváme se, že stanovení požadavku v tom smyslu, že skutečným majitelem žadatele / právnické osoby musí být osoba usazená na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, představuje právě takovýto dodatečný národní požadavek jdoucí nad rámec litery nařízení.

			Jelikož požadavek na usazení skutečného majitele v EU/ESVO není dán nařízením, ale českým návrhem zákona, bude se týkat pouze společností, které jsou usazeny v ČR a budou se do Komunity chtít registrovat. Ovšem pokud podobné přísnější ustanovení nepřijmou i ostatní ČS (o čemž v tuto chvíli nemáme informace), lze předpokládat, že v komunitě bude celá řada společností, jejichž „skuteční majitelé“ budou usazeni mimo EU/ESVO. Náš zákon by tedy zásadně mohl znevýhodnit ty společnosti, které by byly usazené v ČR, oproti například těm, které by byly usazené v jiné zemi EU. Tato situace by pak mohla být důvodem budoucího případného infringementu. Pokud však gestor disponuje informacemi o tom, že jiné ČS hodlají přijmout obdobnou právní úpravu, bylo by vhodné tuto skutečnost doplnit do důvodové zprávy. Nepovažujeme rovněž za účelné argumentovat cílem nařízení, protože toho je dosahováno prostřednictvím omezení členství na společnosti usazené v ČS, což nerozporujeme. Pokud by bylo cílem nařízení mířit i na „skutečné majitele“, zřejmě by se tato skutečnost promítla už v samotném nařízení. Závěr Připomínka je vypořádána.
566. Ministerstvo průmyslu a obchodu	D	K návrhu tezí prováděcích právních předpisů (VI): Vyhláška o kritériích rizikovosti dodavatele obsahuje kritéria, která mohou být problematická z hlediska mezinárodněprávních závazků, jak už jsme uváděli dříve, konkrétně např. bod 10: „Je důvodná obava, že činnost dodavatele může ohrozit významné ekonomické zájmy České republiky.“ Takové kritérium nemůže být podřazeno pod	Vysvětleno Uvádíme, že teze prováděcích právních předpisů jsou sice součástí předkládaného materiálu, ale budou následně předmětem samostatného připomínkového řízení při procesu jejich vydávání. Vaši připomínku bereme na vědomí a doporučujeme připomínky k

		posuzování bezpečnosti a veřejného pořádku ČR. Jedná se o čistě ekonomické kritérium, přes něž může být vyhláška a s ní teoreticky i celá konstrukce možnosti omezení nebo zákazu dodavatelů napadnutelná pro rozpor s právem WTO .	vyhláškám uplatnit v rámci připomínkového řízení k prováděcím předpisům, aby mohly být tyto připomínky řádným způsobem vypořádány. Nutno však dodat, že zmíněná kritéria posuzování rizikivosti dodavatele v rámci vyhlášky sloužila primárně jako vodítko/metodika k určení hrozby, přičemž vyhláška o kritériích rizikivosti dodavatele byla, mimo jiné z důvodů uvedených v připomínce, směřujících k mezinárodněprávním závazkům, vyřazena. Kritériem tudíž zůstává bezpečnost ČR a její vnitřní či veřejný pořádek. Připomínkové místo s vypořádáním souhlasí.
567. Ministerstvo průmyslu a obchodu	D	K návrhu tezí prováděcích právních předpisů (VI): Nejasnosti (méně závažného charakteru než rozpor s právem WTO) máme také u některých dalších kritérií vyhlášky o kritériích rizikivosti dodavatele. Např. v § 2 písm. e) se hovoří o svévolně vyvíjeném nátlaku – není tam jasné, jak bude Úřad vyhodnocovat svévolnost a nesvévolnost nátlaku, resp. jaký je právní význam tohoto rozlišování v zákoně. Dále v příloze k této vyhlášce, konkrétně v bodu 9 nám přijde jako velmi přísné kritérium pod písm. d. – dle našeho názoru je otázkou, zda zaměstnavatel může mít pod kontrolou veškeré chování svých zaměstnanců v jejich osobním životě. Máme za to, že toto kritérium může způsobit rizikovitost (optikou vyhlášky) velkého množství dodavatelů. Nutno podotknout, že zde ani není rozlišováno mezi úmyslným a nedbalostním trestním činem či podle jejich závažnosti.	Vysvětleno Uvádíme, že teze prováděcích právních předpisů jsou sice součástí předkládaného materiálu, ale budou následně předmětem samostatného připomínkového řízení při procesu jejich vydávání. Vaši připomínku bereme na vědomí a doporučujeme připomínky k vyhláškám uplatnit v rámci připomínkového řízení k prováděcím předpisům, aby mohla být tyto připomínky řádným způsobem vypořádány. Dodáváme však, že zmíněná kritéria posuzování rizikivosti dodavatele v rámci vyhlášky sloužila primárně jako vodítko/metodika k určení hrozby, přičemž vyhláška o kritériích rizikivosti dodavatele byla, mimo jiné důvodů uvedených ve Vaší připomínce, vyřazena. Kritériem tudíž zůstává bezpečnost ČR a její vnitřní či veřejný pořádek. Připomínkové místo s vypořádáním souhlasí.
568. Ministerstvo průmyslu a obchodu	D	K návrhu tezí prováděcích právních předpisů (VI): Vyhláška o bezpečnostních opatřeních poskytovatele regulované	Vysvětleno

		služby v režimu vyšších povinností vymezuje jak obsah a rozsah bezpečnostních opatření (která dělí na organizační a technická), ale také lokalizaci informací a dat při jejich zpracování v zahraničí. Není srozumitelné, co je zde smyslem – vyhláška vymezuje lokalizaci dat či opatření? Není jasné, co znamená lokalizace informací a dat při jejich zpracování v zahraničí s ohledem na obsah samotné vyhlášky.	Návrh připomínkové vyhlášky neobsahuje povinnosti lokalizace dat a informací. Tyto povinnosti byly z návrhu vyhlášky po veřejných konzultacích vypuštěny. Citované znění z úvodu tezí vyhlášek k předkládanému zákonu tak bylo uvedeno chybně. Připomínkové místo s vypořádáním souhlasí.
569. Ministerstvo průmyslu a obchodu	D	K důvodové zprávě (III): V části 7.1.6. na str. 76 navrhujeme přesunout poslední část třetího odstavce, neboť zaměstnanci Ministerstva průmyslu a obchodu prověřující zahraniční investice nemají k dispozici zmiňovaný informační systém: Ve vztahu k návrhu zákona bude nutné vyhradit jednotky až nízké desítky tabulkových míst u zapojených státních orgánů a rozšíření stávajících či připravovaných informačních systémů k technické obsluze procesu prověřování. Na straně Úřadu a spolupracujících institucí budou muset být vynaloženy náklady, aby mohlo docházet k systematickému a koordinovanému prověřování dodavatelů do strategicky významné infrastruktury. V souladu s principem efektivity a cílem minimalizace ekonomických nákladů se bude maximálně využívat fungující synergie s již existujícími agendami a procesy, jakými jsou kupříkladu prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům veřejné moci <u>(včetně účelného využívání informačních systémů, které tuto agendu podporují)</u> či prověřování zahraničních investorů podle zákona o prověřování zahraničních investic, ~~včetně účelného využívání informačních systémů, které tyto agendy podporují.~~	Neakceptováno Domníváme se, že není nutné provádět navrhovanou změnu důvodové zprávy. V dané větě, která se požaduje upravit, jsou procesy prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům veřejné správy a prověřování zahraničních investorů podle zákona o prověřování zahraničních investic uvedeny pouze jako příklady agend, jejichž synergie s procesem prověřování pro účely mechanismu bezpečnosti dodavatelského řetězce bude využita. Nejedná se o úplný výčet, těchto agend a procesů je vícero. Zmínka o informačních systémech podporujících dané agendy a procesy, které budou využity, se tedy nevztahuje pouze na dva výše uvedené příklady, ale na větší množství agend a procesů. Máme tedy za to, že není třeba danou větu upravovat dle návrhu v připomínce, jelikož i v jejím současném znění z ní nevyplývá, že při prověřování zahraničních investic je určité využíván nějaký informační systém. Připomínkové místo s vypořádáním souhlasí.
570. Ministerstvo průmyslu a obchodu	D	K důvodové zprávě (III): str. 130 - celý první odstavec k § 34: Obecně se nedomníváme, že by zde problematika ukládání dat mimo ČR/EU měla být takto akcentována. Odkazovaný článek se zabývá obecnou dostupností služby z ČR, což skýtá mnohem více aspektů, jak je ostatně uvedeno	Akceptováno Znění důvodové zprávy k předmětnému ustanovení bylo upraveno ve smyslu připomínky. Odstavec 1 byl upraven s ohledem na změny provedené v

		níže ve zdůvodnění. Domníváme se, že odstavec by měl být minimálně posunut níže a případně zkrácen. Např. rizika jmenovaná v souvislosti s přírodními katastrofami apod. mohou nastat i při uložení dat v EU, akcentovat je zde tedy působí zbytečně. V souvislosti s oběma připomínkami se domníváme, že z předložených textů dostatečně nevyplývá, zda je uložena povinnost lokalizace dat na určitém území a v jakých případech. Samotný text zákona na ni neodkazuje (případně požádáme o nasměrování), v tomto kontextu je tedy zvláštní akcent na lokalizaci dat ve zdůvodněních.	legislativním textu. V textu nadále není akcentována původní problematika tohoto ustanovení - lokalizace dat. Povinnost lokalizace dat byla ze zákona odstraněna a nahrazena povinností zajištěním dostupnosti strategicky významné služby (viz aktualizované znění § 35 o zajištění dostupnosti strategicky významných služeb). Připomínkové místo s vypořádáním souhlasí.
571. Ministerstvo průmyslu a obchodu	D	K důvodové zprávě (III): str. 144 - návrh zákona v § 48: Základní způsobilost žadatele o registraci členství v Komunitě udává: (1) Žadatel má základní způsobilost, pokud a) má sídlo nebo místo podnikání na území České republiky, V tom samém paragrafu o pár řádků pod tím je uvedeno: 4) Žadatel není způsobilý, pokud a) je právnickou osobou, která má skutečného majitele, pokud nebylo podle odstavce 3 možné zjistit údaje o jeho skutečném majiteli z evidence skutečných majitelů, b) skutečným majitelem je osoba usazená mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, nebo Obdobně jako v samotném článku by i v důvodové zprávě mělo být zohledněno, že podmínku (1) a) splní žadatel i tím, že má na území ČR místo podnikání (nikoliv však sídlo). Z citované pasáže nařízení (EU) 2021/887 nevyplývá požadavek na sídlo, pouze nějakou formu usazení (established). Dále, stejně jako horizontálně, připomínáme potřebu souladu s mezinárodními závazky.	Neakceptováno Pojem „usazení“ český právní řád užívá spíše v souvislosti s přeshraničním poskytováním služeb a pojem „místo podnikání“ se užívá zase v souvislosti s místem podnikání OSVČ, nicméně i v tomto ohledu došlo ke sjednocení na pojem sídlo jak pro právnické osoby, tak pro OSVČ, a aktuálně se užívá již pouze pojem "sídlo". V návaznosti na to došlo i k úpravě § 51 odst. 1 písm. a), který jako podmínku stanoví, že žadatel má sídlo na území ČR. Dále máme za to, že pokud by v návrhu zákona absentovala podmínka sídla, funkce Úřadu jako Národního koordinačního centra, a tudíž posuzovatele způsobilosti žadatele k přijetí do Komunity by byla ohrožena, neboť by nebyl schopný zajistit požadované ověření u osob se sídlem mimo ČR. Podmínka sídla u člena Komunity je tak logická, aby Národní koordinační centrum mohlo plnit svou funkci v rámci České republiky. Samotné nařízení Evropského parlamentu a Rady (EU) 2021/887 nepředpokládá předávání citlivých informací o žadatelích napříč členskými státy, tento způsob spolupráce neustanovuje a nestanoví tak k tomu potřebné funkční mechanismy.

			Reakce připomínkového místa: Nesouhlasíme s vysvětlením. Není jasné proč je podmínka sídla nezbytná pro plnění funkce Národního koordinačního centra. V tomto kontextu je také relevantní připomínka č. 565. Reakce NÚKIB: Zaslán návrh na doplnění odůvodnění. Závěr Viz vypořádání připomínky č. 565.
572. Ministerstvo průmyslu a obchodu	D	Ke zprávě RIA: Doporučujeme opravit název zákona č. 34/2021 Sb. (str. 19, 22): zákon č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic); ~~ve znění pozdějšího předpisu~~	Akceptováno Připomínkové místo s vypořádáním souhlasí.
573. Ministerstvo průmyslu a obchodu	D	Ke zprávě RIA: 1 na str. 4 navrhujeme přesunout poslední část druhého odstavce této strany, neboť zaměstnanci Ministerstva průmyslu a obchodu prověřující zahraniční investice nemají k dispozici zmiňovaný informační systém: Ve vztahu k návrhu zákona bude nutné vyhradit jednotky až nízké desítky tabulkových míst u zapojených státních orgánů a rozšíření stávajících či připravovaných informačních systémů k technické obsluze procesu prověřování. Na straně Úřadu a spolupracujících institucí budou muset být vynaloženy náklady, aby mohlo docházet k systematickému a koordinovanému prověřování dodavatelů do strategicky významné infrastruktury. V souladu s principem efektivity a cílem minimalizace ekonomických nákladů se bude maximálně využívat fungující synergie s již existujícími agendami a	Neakceptováno Domníváme se, že není nutné provádět navrhovanou změnu RIA. V dané větě, která se požaduje upravit, jsou procesy prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům veřejné správy a prověřování zahraničních investorů podle zákona o prověřování zahraničních investic uvedeny pouze jako příklady agend, jejichž synergie s procesem prověřování pro účely mechanismu bezpečnosti dodavatelského řetězce bude využita. Nejedná se o úplný výčet, těchto agend a procesů je vícero. Zmínka o informačních systémech podporujících dané agendy a procesy, které budou využity, se tedy nevztahuje pouze na dva výše uvedené příklady, ale na větší množství agend a

		procesy, jakými jsou kupříkladu prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům veřejné moci (<u>včetně účelného využívání informačních systémů, které tuto agendu podporují</u>) či prověřování zahraničních investorů podle zákona o prověřování zahraničních investic, ~~včetně účelného využívání informačních systémů, které tyto agendy podporují.~~	procesů. Máme tedy za to, že není třeba danou větu upravovat dle návrhu v připomínce, jelikož i v jejím současném znění z ní nevyplyvá, že při prověřování zahraničních investic je určité využíván nějaký informační systém. Připomínkové místo s vypořádáním souhlasí.
574. Ministerstvo průmyslu a obchodu	D	Ke zprávě RIA: Doporučujeme aktualizovat text o nové znění bezpečnostní strategie (s. 13, 25, 33)	Akceptováno Závěrečná zpráva RIA byla aktualizována požadovaným způsobem. Připomínkové místo s vypořádáním souhlasí.
575. Ministerstvo průmyslu a obchodu	Z	Mechanismus prověřování bezpečnosti dodavatelského řetězce se má vztahovat pouze na tu nejkritičtější část strategické infrastruktury. Předkladatel však ve svém návrhu vymezil jeho rozsah formou vyhlášky o nepominutelných funkcích stanoveného rozsahu, která pro oblast elektronických komunikací obsahuje jak ty nejkritičtější části sítě, jako je jádro sítě, tak i v obecné rovině méně kritické části sítě, jako je rádiová přístupová síť nebo aktiva, které nemají přímý vliv na nedostupnost regulovaných služeb. V návrhu zákona také není dostatečně odůvodněno, proč jsou kritické části stanoveného rozsahu aktiv definovány tak široce. Bylo by proto vhodné specifikovat a rozdělit strategickou infrastrukturu elektronických komunikací na nejkritičtější část strategické infrastruktury, kde bude povinnost řídit se případným zákazem uvedeným v opatření obecné povahy, a na méně kritické části strategické infrastruktury, kde bude dána povinnost zohlednit rizika identifikovaná státem a případně implementovat odpovídající bezpečnostní opatření.	Neakceptováno NÚKIB považuje vyhlášku o nepominutelných funkcích za kritickou, jelikož cílí na vše, co je v rámci fungování veřejných komunikačních sítí kritické, bez ohledu na umístění daných funkcí v rámci architektury sítě. To znamená, že z pohledu kybernetické bezpečnosti je kritická funkčnost jednak jádra sítě, jednak také vybraných funkcí ostatních částí sítě, jako jsou kupříkladu vybrané funkce rádiové přístupové sítě, bez nichž by jádro sítě nemohlo být propojeno s koncovými zařízeními, čímž by došlo k znefunkčnění takové sítě. Vzhledem ke komplexitě telekomunikačních sítí, ale také vysoké úrovni zpracování architektur těchto sítí v rámci mezinárodních standardizačních organizací, má právě toto odvětví vlastní vyhlášku. V případě kompromitace těchto nepominutelných funkcí může být narušeno či porušeno nejen poskytování služeb koncovým uživatelům, ale také dalších strategicky významných služeb, které jsou na telekomunikačních sítích závislé. NÚKIB tedy skutečně cílí na to, co je

			pro fungování ICT infrastruktury strategicky významných služeb kritické, což jsou funkce uvedené v dané vyhlášce o nepominutelných funkcích. Obdobný postup určení nepominutelných funkcí na základě kritičnosti zvolilo také Finsko, Německo či Velká Británie. Co se týče ochrany rádiové přístupové sítě, tak ta je mimo jiné chráněna například v Litvě, Lotyšsku, Švédsku, Finsku či například Belgii. Připomínkové místo s vypořádáním souhlasí.
576. Ministerstvo průmyslu a obchodu	D	K § 4 odst. 2 a § 27 odst. 1 Doporučujeme vyjasnění pojmu “služby” v § 4 odst. 2 a v § 27 odst. 1 („digitální infrastruktura a služby“). Pojem vyvolává zdání, že by se mohlo jednat o digitální služby ve smyslu čl. 6 bodu 23 směrnice NIS2 (tedy, že se jedná o službu informační společnosti). Pokud je tomu tak, navrhovali bychom použít pojem služba informační společnosti nebo alespoň vyjasnit v důvodové zprávě. Nad rámec výše uvedeného upozorňujeme, že pojem “digitální služby” se objevuje také v § 2 odst. 2 zákona č. 12/2020 Sb., o právu na digitální služby, kde se typicky jedná o úkon orgánu veřejné moci.	Akceptováno jinak V návrhu dojde k dílčím změnám, kdy bude zjevnější, o jaké služby konkrétně jde, resp. kde a jakým způsobem jsou stanovena kritéria pro jejich identifikaci či určení. Pojem služba informační společnosti (SIS) neodpovídá pojmu regulovaná služba, byť některé SIS mohou být regulovanými službami dle návrhu zákona, resp. dle vyhlášky o regulovaných službách. Jedno z regulovaných odvětví je také " Digitální infrastruktura a služby", vyhláška o regulovaných službách a její odůvodnění dostatečně vyjasňují rozdíl mezi institutem SIS a regulovanou službou dle návrhu zákona. Připomínkové místo s vypořádáním souhlasí.
577. Ministerstvo průmyslu a obchodu	Z	K § 29 odst. 2 Do § 29 odst. 2 je třeba doplnit součinnost s ČTÚ. Zde je pak vazba na § 30 odst. 2, který odkazuje na instituce podle § 29 odst. 2, se kterými NÚKIB musí projednat návrh OOP. Odůvodnění: Navrhuje doplnit do výčtu institucí Český telekomunikační úřad, neboť jeho role v oblasti elektronických komunikací i ve vazbě na kybernetickou bezpečnost klíčová. Je proto žádoucí, aby tento	Neakceptováno - nyní § 30 NÚKIB v rámci získávání informací dle textu navrhovaného zákona spolupracuje s relevantními orgány státu, v případě jednotlivých sektorů pak zákon v podobě, v jaké je dnes, tuto spolupráci předpokládá s regulátory jednotlivých sektorů (např. telekomunikace, doprava či energetika), je-li to pro konkrétní případ možné.

		sektorový regulátor měl možnost se k implementaci zákazu vyjádřit a NÚKIB musel k jeho stanovisku přihlédnout. Uvedené souvisí rovněž s navrhovanou změnou zákona o elektronických komunikacích v doprovodném změnovém zákonu, kde navrhuje v § 22a zákona č. 127/2005 Sb. doplnit nový odstavec 6: „(6) Předseda Rady může rozhodnout po konzultaci podle § 130 o změně přidělu rádiových kmitočtů, jestliže je to nezbytné pro plnění a) protiopatření podle § 20 zákona o kybernetické bezpečnosti, nebo b) účelu opatření obecné povahy vydaného podle § 30 zákona o kybernetické bezpečnosti.“. <i>Vyznačení změny</i> (2) Nejvyšší státní zastupitelství, Policie České republiky, Úřad pro ochranu hospodářské soutěže, Český telekomunikační úřad, Finanční analytický úřad a zpravodajské služby České republiky za účelem výkonu činnosti podle § 28 odst. 1 poskytnou Úřadu na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů požadované informace nebo jinou součinnost.	Toto je zaručeno mimo jiné § 8 odst. 2 zákona č. 500/2004 Sb, správního řádu. Dále je tento postup dán principem dobré správy, kdy NÚKIB pro co nejlepší vyhodnocení situace a možných dopadů počítá s dožádáním informací od relevantních orgánů státu v rámci jednotlivých odvětví. Závěr Akceptováno jinak Ustanovení § 31 bylo upraveno a byla doplněna součinnost ČTÚ. Připomínkové místo s vypořádáním souhlasí.
578. Ministerstvo průmyslu a obchodu	Z	K § 30 odst. 1 Na konci § 30 odst. 1 doplnit větu: „Úřad může rovněž zohlednit v opatření obecné povahy konkrétní umístění kritické části stanoveného rozsahu na území České republiky.“ <i>Odůvodnění</i> Pro určité případy zejména celoplošné nebo územně rozsáhlé infrastruktury se jeví jako žádoucí, aby NÚKIB explicitně mohl zohlednit při přípravě opatření obecné povahy i lokalizaci kritických částí infrastruktury v rámci ČR. Má se za to, že případná intenzita negativních dopadů u kritických částí infrastruktury v různých územních oblastech je odlišná, a to nejen s ohledem na hustotu obyvatel, ale např. i na přítomnost jiné kritické infrastruktury.	Akceptováno jinak - nyní § 31 Zohlednit umístění kritické části stanoveného rozsahu může Úřad v opatření obecné povahy i bez výslovné zmínky takového oprávnění v zákoně, jelikož to vychází z obecných postupů správního orgánu při vydávání opatření dle správního řádu. Připomínkové místo s vypořádáním souhlasí.

		<i>Vyznačení změny</i> (1) Úřad vydá opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, zjistí-li na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy stanoví Úřad s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby. Úřad může rovněž zohlednit v opatření obecné povahy umístění kritické části stanoveného rozsahu na území České republiky.	
579. Ministerstvo průmyslu a obchodu	Z	K hodnocení dopadů regulace (RIA) a důvodové zprávě: V hodnocení dopadů regulace (RIA) a důvodové zprávě se jeví jako nedostatečné vyhodnocení dopadů na regionální poskytovatele služeb elektronických komunikací, kterých by se mechanismus prověřování bezpečnosti dodavatelského řetězce mohl dotýkat. <i>Odůvodnění</i> Zákon zavádí kromě implementace směrnice NIS 2 i úpravu “prověřování dodavatelského řetězce”. Celá řada národních operátorů má jako dodavatele (např. přístup nebo propojení sítě) regionální hráče různé velikosti, na které se formálně mechanismus nebude vztahovat, ale protože “kritickou částí stanoveného rozsahu” je dle návrhu vyhlášky o nepominutelných funkcích fakticky celá síť, budou regulovanými subjekty i desítky malých a středních firem, protože se stanou dodavateli a jejich dodavatelé subdodavateli. Je vhodné do RIA přiměřeně doplnit dopad na malé regionální poskytovatele internetu jako možné subjekty mechanismu z důvodu, že jsou nebo mohou být dodavateli velkých subjektů.	Neakceptováno NÚKIB v rámci důvodové zprávy operoval s velkým množstvím dostupných dat a poznatků, ovšem vzhledem k nemožnosti předjímat všechny dopady konkrétních opatření obecné povahy, budou-li tyto vydány, není možno dopady na regionální poskytovatele služeb elektronických komunikací blíže specifikovat. Důvodová zpráva se tak drží určité míry obecnosti, ale zároveň se snaží o konkretizaci dopadů do takové míry, do jaké je to na základě odhadů možné. Připomínkové místo s vypořádáním souhlasí.
580. Ministerstvo průmyslu a obchodu	Z	K tezím vyhlášky o regulovaných službách: V pol. 16.1, písm. d) a 16.2, písm. d) Přílohy vyhlášky by minimální počet aktivních pevných internetových přípojek měl být vyšší, v	Neakceptováno

		ideálním případě daný na stejnou úroveň jako minimální počet aktivních SIM karet v případě mobilních služeb. <i>Odůvodnění</i> Disproporce mezi zohledňováním poskytování mobilních služeb a pevných služeb, a v obecné rovině nízká hranice pro poskytovatele přípojek k internetu v pevném místě, nemusí být odůvodnitelná. Nižší úroveň hranice v případě pevných služeb/pevných sítí může ve svých důsledcích vést k ohrožení ekonomického fungování zejména regionálních, malých a středních poskytovatelů pevných služeb.	Teze prováděcích právních předpisů jsou sice již teď součástí předkládaného materiálu, ale budou následně předmětem samostatného připomínkového řízení při procesu jejich vydávání. Nelze předpokládat, že jedna pevná přípojka (typicky jedna domácnost) odpovídá jedné osobě (tj. jedné SIM kartě), z pohledu účelu právní úpravy tedy není vhodné uvedená kritéria sjednocovat. Pokud jde o konkrétní počty SIM karet a pevných přípojek, uvedený minimální počet aktivních přípojek byl stanoven tak, aby pokryl subjekty poskytující společně podle posledních dostupných dat Českého telekomunikačního úřadu (za rok 2021) většinu všech aktivních přípojek (cca 60 %). Minimální počet SIM karet pokrývá subjekty, které společně poskytují veřejně dostupné služby elektronických komunikací uživatelům většiny všech aktivních mobilních SIM karet na maloobchodním trhu (cca 92 %). V případě SIM karet je současně zohledněna skutečnost, že uvedené výrazně nadpoloviční většině poskytují veřejně dostupné služby elektronických komunikací pouze tři subjekty. Po schůzce Vysvětleno Po schůzce byly teze v této části zobecněny a konkrétní počet aktivních SIM karet nebo přípojek není v rámci tezí uveden. Bude upřesněn v rámci připomínkového řízení k samotné vyhlášce. Připomínkové místo s vypořádáním souhlasí.
581. Ministerstvo průmyslu a obchodu	Z	K § 28 návrhu zákona o kybernetické bezpečnosti Odstavce 3 a 4 obsahují zmocnění pro vydání prováděcího předpisu pro stanovení rozsahu aktiv stanoveného rozsahu strategicky významné služby, která zajišťují nepominutelné funkce. Tak významné stanovení kritérií by mělo být stanoveno přímo zákonem, a	Neakceptováno - nyní § 29 K úpravě nepominutelných funkcí na úrovni vyhlášky musíme poznamenat, že úprava nepominutelných funkcí ve vyhlášce představuje proporcionální řešení

		ne v prováděcím právním předpisu, alespoň ty nejzásadnější s nejintenzivnějším dopadem.	konfliktu mezi širokým správním uvážením NÚKIB, a vymezením funkcí na úrovni zákona. Obdobný postup navíc již funguje v případě tzv. vyhlášky o zápisu do katalogu cloud computingu vydané NÚKIB, tj. vyhláška č. 316/2016 Sb. Je nasnadě podotknout, že úprava kritérií formou podzákonného právního předpisu je skutečně běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, tak ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, jež je předkladatel povinen řádně vypořádat. Obdobný postup NÚKIB zvolil v případě zmíněné úpravy zápisu do katalogu cloud computingu, kde toto nečiní žádné aplikační potíže. Nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu. Připomínkové místo s vypořádáním souhlasí.
582. Ministerstvo průmyslu a obchodu	Z	Předkládaný materiál jako takový obsahuje RIA, což chválíme. Nicméně Zpráva RIA minimálně v části, která se týká dopadu na podnikatelské prostředí, zcela rezignovala na jakoukoliv kvantifikaci přibližných nákladů na tento segment a je zde uvedeno pouze toto: <i>„Výši finančních dopadů není možné předem stanovit a veškeré předchozí požadavky na jejich vyčíslení vedly k vytvoření odhadů s nízkou vypovídající hodnotou.“</i> S jistou mírou benevolence se můžeme s touto konstatací i spokojit, ač je to proti obecným zásadám, jak by měla být zpráva RIA vytvořena. Kde však musíme trvat na kvantifikaci a požadujeme větší detail, je následující teze: <i>Z důvodu rozsahu transponované směrnice dojde k přinejmenším patnáctinásobnému nárůstu regulovaných subjektů, což přinese značné ekonomické a finanční dopady na podnikatelské prostředí v ČR. Naprostá většina z nově regulovaných subjektů bude ze soukromého sektoru.</i> Další konkrétní informace chybí a je to škoda. Prosíme doplnit alespoň: 1) Jak byl zjištěn 15ti násobný nárůst?	Akceptováno Problematika jakéhokoliv výpočtu nákladů nebo odhadů je v oblasti kybernetické bezpečnosti dlouhodobě problematická. Se směrnicí NIS2 přibývá do tohoto procesu další neznámá - ještě v tuto chvíli, několik měsíců po přijetí směrnice, probíhají na úrovni EU diskuze o tom, jak některé definice povinných osob chápat a pojímat, případně jak aplikovat velikostní kritérium. NÚKIB se dlouhodobě snaží vyjednávat racionální přístup a tím omezovat počet regulovaných osob na účelné minimum. Stanovený počet minimálně 6000 regulovaných osob, který NÚKIB dlouhodobě komunikuje, vychází z porovnání těch regulovaných služeb, u kterých je jejich rozsah jasný, a není předmětem diskuse, při současné aplikaci kritéria velikosti více než 50 zaměstnanců (nebo

		2) Typově jakých firem se bude týkat, pokud je to možné uvést alespoň příklad nebo charakteristiku takové firmy? Ať si i laik udělá jasnější představu. 3) Kolika firem se to bude v absolutních číslech týkat? 4) Jedná se o transpozici EU směrnice, takže tato data mohou být pro potřeby RIA částečně přenositelná, též prosíme o reflexi.	využití jiného počtu zaměstnanců, relevantně dle směrnice). Pokud je za současného stavu regulovaných osob cca 400 (v čase se také proměňuje), vychází pak při porovnání těchto dvou čísel právě zmíněný 15násobek. Typové označení regulovaných firem pak odpovídá vyhlášce o regulovaných službách. Demonstrativní výčet je možné v důvodové zprávě uvést. Kolika firem se to bude v absolutních číslech týkat není v tuto chvíli možné odhadnout. Je to dáno jednak tím, co je uvedeno výše, jednak tím, že pro úplné srovnání a stanovení velikostního kritéria je nutný alespoň omezený přístup k obratu a hodnotě aktiv relevantních společností, což je ovšem informace, kterou Generální finanční ředitelství nemůže před účinností zákona poskytnout. Na tuto skutečnost reaguje původní návrh § 65 odst. 4. Toto shrnutí bude doplněno do hodnocení dopadů. Připomínkové místo s vypořádáním souhlasí.
583. Ministerstvo průmyslu a obchodu	D	Zavedení mechanismu bezpečnosti dodavatelského řetězce zřejmě bude mít mimo jiné dopady také na provozovatele energetické infrastruktury. Jejich rozsah však nejsme, i s ohledem na velmi krátký čas, v němž bylo třeba se s danou problematikou seznámit a k uvedenému návrhu zákona se vyjádřit, schopni podrobněji vyhodnotit. V tomto směru si dovoluji upozornit, že mezi očekávané negativní dopady patří potenciální redukce nabídky dodávek některých technologií v důsledku omezení rizikových dodavatelů, což může vést k nárůstu cen dodávaných technologií, a tedy i ke zvýšeným nákladům na straně regulovaných subjektů (což je v materiálu zmíněno). Konkrétně v energetice pak lze předpokládat, že náklady vyvolané návrhem zákona budou moci být považovány za uznatelné náklady pro účely cenové regulace, a tudíž by mohly být přeneseny na spotřebitele a způsobit případně rovněž dopady do sociální oblasti	Vysvětleno Pokud jde o požadavek na uvedení, jak konkrétně spolupráce Úřadu s odbornými svazy ovlivnila znění návrhu zákona, je nutno konstatovat, že uvedená spolupráce není jediným faktorem, který měl podíl na prvotní formulaci návrhu, respektive na následných úpravách této formulace. Do podoby návrhu se promítly také vnitroodborové a meziodborové konzultace v rámci Úřadu, výstupy z komunikace s jinými státními orgány nebo podněty zaslané fyzickými a právnickými osobami po prvním zveřejnění návrhu zákona a prováděcích vyhlášek. Jako konkrétní příklad spolupráce s odbornými svazy lze nicméně uvést zavedení možnosti Úřadu stanovit

		(což v materiálu takto do důsledků již uvedeno není). Dalším negativním dopadem může teoreticky být i potenciální zpomalení realizace některých investic a implementace technologií souvisejících s probíhající transformací energetického sektoru. Z důvodové zprávy a z hodnocení dopadů regulace pak sice vyplývá, že v rámci konzultačního procesu byly osloveny i příslušné odborné svazy, nicméně není příliš zřejmé, jak tato spolupráce ovlivnila znění návrhu či do jaké míry detailu byly dopady na dotčené subjekty, respektive dotčená odvětví ekonomiky, zkoumány. S ohledem na výše uvedené žádáme o bližší vysvětlení.	lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle § 31 odst. 1 návrhu zákona či zavedení možnosti Úřadu povolit podle § 32 odst. 1 návrhu zákona povolit výjimku z podmínek či zákazu stanovených opatření obecné povahy podle § 31. V tomto směru je namístě konstatovat, že spolupráce s odbornými svazy měla za výsledek zmírnění případných negativních dopadů zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce. Co se týče Vámi uvedených dopadů do sociální oblasti, podle bodu 10.5 obecných zásad pro hodnocení dopadů regulace (RIA), účinných od 3. 2. 2016 se mezi sociálními dopady uvádějí dopady na rodiny, na specifické sociální skupiny obyvatel a jejich práva, např. na sociálně slabé, osoby se zdravotním postižením, národnostní menšiny, sociálně vyloučené či na zaměstnance. V rámci hodnocení lze mezi sociálními dopady uvést okolnosti mající dopad na zhoršení sociální rovnosti, pracovní právní vztahy, sociální začleňování, sdružování, práva menšin či sociální dialog. S ohledem na výše uvedené máme za to, že v závěrečné zprávě RIA je správně uvedeno, že návrh zákona nebude mít sociální dopady. Vámi uváděné případné negativní dopady v podobě zpomalení realizace některých investic a implementace technologií lze mít za následek zvýšení nákladů dotčených podnikatelů, a takto byly vzaty v potaz při hodnocení všech zohlednitelných dopadů (včetně pozitivních), jak jsou podrobně specifikovány v bodě 3.3 závěrečné zprávy RIA. S odkazem na poslední zmíněnou pasáž je nicméně nutno zopakovat, že přesnou výši finančních dopadů není možné předem

			stanovit a veškeré předchozí požadavky na jejich vyčíslení vedly k vytvoření odhadů s nízkou vypovídací hodnotou. Připomínkové místo s vypořádáním souhlasí.
584. Ministerstvo průmyslu a obchodu	D	§ 17 Náležitosti hlášení kybernetických bezpečnostních incidentů Rozumíme stanoveným lhůtám v uvedeném § 17 návrhu zákona o kybernetické bezpečnosti, nicméně zde existuje důvodná obava, že nebudou dodrženy s ohledem na to, že není zajištěn nepřetržitý provoz (24/7) nebo nejsou drženy pohotovosti. Z tohoto důvodu žádáme o návrh řešení (např. omezení lhůty na pracovní dobu, navýšení personálních kapacit nebo financí na zajištění těchto kapacit.	Vysvětleno Lhůta pro hlášení incidentů je vázána na okamžik zjištění tohoto incidentu, který se nemusí shodovat s reálným časem, kdy incident skutečně nastal. Pokud tedy incident nastane např. v sobotu, ale je nahlášen až v pondělí bezodkladně po tom, co se o něm příslušný zaměstnanec dozvěděl, je zákonná povinnost splněna. Takto stanovená lhůta má zajistit případnou rychlou reakci Vládního CERT, příp. Národního CERT při řešení incidentu a napomoci navazujícím preventivním či analytickým aktivitám Vládního CERT, příp. Národního CERT. Obsahové náležitosti prvotního hlášení jsou omezeny na nezbytné minimum, díky kterému bude Vládní CERT schopen posoudit, zda má incident významný dopad na kybernetický prostor státu, a zároveň by předání těchto informací nemělo představovat pro ohlašovatele nadměrnou administrativní zátěž. Poskytovatelé regulované služby v režimu nižších povinností hlásí pouze kybernetické bezpečnostní incidenty s významným dopadem, poskytovatelé regulované služby ve vyšším režimu hlásí všechny kybernetické bezpečnostní incidenty. Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u

			těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob. Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnicí NIS2, tzn. pokud bychom do zákona nezahrnuli požadavek na lhůtu, která je podle čl. 23 odst. 4 písm. a) NIS2 stanovena na "bez zbytečného odkladu, nejpozději však do 24 hodin po zjištění", byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Z uvedeného důvodu národní právní úprava tento požadavek kopíruje. Připomínkové místo s vypořádáním souhlasí.
585. Ministerstvo průmyslu a obchodu	D	K § 29 odst. 1 Není zde zcela jasný proces. Bylo by vhodné blíže vyjasnit konkrétní proces a povinnosti v případě MPO.	Vysvětleno - nyní § 30 Co se týče daného procesu, tak jak je uvedeno v dotčeném ustanovení a důvodové zprávě k němu, Ministerstvo průmyslu a obchodu, spolu s ostatními zmíněnými orgány státu, za účelem výkonu činnosti podle § 29 odst. 1, tj. shromažďovat a vyhodnocovat informace a data spojené s orgánem či osobou, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek, poskytne Úřadu na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů ode dne obdržení žádosti, stanovisko k rizikovosti dodavatele (v původním znění navázáno na kritéria rizikovosti dodavatele) nebo požadované informace.

			Postup ani forma připomínkové úpravy návrhu zákona se v tomto ohledu zásadně neliší např. od postupu podle § 11 odst. 2 a 3 zákona o prověřování zahraničních investic, pouze neupravuje oblasti, které zde nejsou relevantní, např. postup Úřadu v případě neposkytnutí stanoviska - vydání opatření k omezení rizika spojeného s dodavatelem totiž nepodléhá lhůtě pro vyřízení žádosti dle správního řádu. Oproti textu, který byl k dispozici v rámci mezirezortního připomínkového řízení už ovšem nebude stanovisko rizikovosti dodavatele konkrétním orgánem či osobou navázáno na kritéria rizikovosti dodavatele stanovená vyhláškou. Dále byla zrušena jiná součinnost z důvodu lepší srozumitelnosti a určitosti procesu uvedeného ustanovení. Připomínkové místo s vypořádáním souhlasí.
586. Ministerstvo zahraničních věcí	Z	K § 41 odst. 4 písm. d) bod 2 Navrhovaný text svěčuje Národnímu úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“) sjednávání a uzavírání smluv o mezinárodní spolupráci. MZV si je vědomo, že již ve stávajícím zákoně č. 181/2014Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, je ustanovení čl. 22 písm. h) a i), jejichž obsah je v předkládaném návrhu zákona sloučen v § 41 odst. 4 písm. d) bod 2. MZV nicméně upozorňuje, že sjednávání mezinárodních smluv jako takových přísluší podle Ústavy České republiky (čl. 63 odst. 1 písm. b)) prezidentu republiky, který tuto pravomoc může přenést na vládu nebo s jejím souhlasem na jednotlivé členy vlády. Úřad takovou pravomoc nemá a ani prezident republiky ji na něj nemůže přenést. MZV proto navrhuje §41 odst. 4 písm. d) bod 2 z návrhu zákona <u>vypustit</u>. Taková úprava bude mj. odpovídat i právní úpravě	Akceptováno jinak - nyní § 44 Příslušné ustanovení návrhu bylo uvedeno do souladu s kompetenčním zákonem; nově zní: „<i>zajišťuje mezinárodní spolupráci v souladu s právními předpisy upravujícími činnost ústředních orgánů státní správy</i>“¹³“, přičemž v pozn. pod čarou č. 13 je uveden odkaz na § 25 kompetenčního zákona. Reakce připomínkového místa V případě připomínky uvedené ve vypořádací tabulce pod č. 586 uvádím, že lze v zásadě s jejím vypořádáním souhlasit. Dotčená poznámka pod čarou č. 13 (u ust. § 44 odst. 4 písm. d), bod 2) se nicméně týká rovněž následujícího bodu 3 („plní další úkoly ...“), proto se považuje za potřebné ji vztáhnout na bod

		pravomocí Národního bezpečnostního úřadu, obsažené v § 137 zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů. <u>Alternativně</u> MZV navrhuje § 41 odst. 4 písm. d) bod 2 úžeji vymezit a přeformulovat, např. takto: „2. zajišťuje mezinárodní spolupráci v oblasti kybernetické bezpečnosti a v rámci své působnosti sjednává a uzavírá se zahraničními partnery dohody o spolupráci.“ Zároveň takovéto vymezení, včetně upřesnění, že se nejedná o mezinárodní smlouvy dle čl. 63 odst. 1 písm. b) Ústavy ČR, uvést v důvodové zprávě.	2 i 3, tj. sloučit body 2 a 3 do jednoho, popřípadě odkaz na tuto poznámku uvést i v bodě 3. Reakce NÚKIB Akceptováno, text návrhu zákona upraven. Připomínkové místo s vypořádáním souhlasí.
587. Ministerstvo zahraničních věcí	Z	K transpozičním ustanovením a ke srovnávací tabulce ke směrnici MZV navrhuje znovu posoudit vyhodnocení slučitelnosti některých ustanovení směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2), (dále jen „směrnice“). Některá ustanovení směrnice jsou vyhodnocena jako nerelevantní z hlediska transpozice, a to i přes to, že tato ustanovení mají být provedena navrhovanými předpisy, jak plyne z rozdílové tabulky k předloženému návrhu zákona. Další „nerelevantní“ ustanovení směrnice svěřují pravomoc nebo stanoví povinnost pro vnitrostátní orgány, toto může být provedeno pouze zákonem (čl. 2 odst. 3 Ústavy). Jiná „nerelevantní“ ustanovení pak zakládají práva	<i>Čl. 1 odst. 1 směrnice je nesprávně vyhodnocen jako netransponovaný, ačkoli za jeho provedení lze považovat navrhovaný § 1 odst. 1 a 2 návrhu. Do srovnávací tabulky by mělo být doplněno znění § 1 odst. 1 a 2, a to včetně znění poznámky pod čarou.</i> Akceptováno jinak. Vzhledem ke sloučení obsahu odstavců 1 a 2 bude pro čl. 1 odst. 1 směrnice NIS 2 vykázán jako transpoziční § 1 odst. 1 návrhu zákona. <i>Čl. 2 odst. 7 směrnice je nesprávně vyhodnocen jako nerelevantní z hlediska transpozice, přestože dané ustanovení směrnice fakticky upravuje působnost směrnice, tj. též působnost příslušných transpozičních opatření by měla tomuto ustanovení odpovídat. Do srovnávací tabulky by mělo být doplněno, ze kterých ustanovení navrhovaných nebo jiných vnitrostátních právních předpisů, působnost takto definovaná směrnicí plyne.</i>

	jednotlivcům a jako taková by s ohledem na judikaturu Soudního dvora měla být provedena. Taková ustanovení, která byla navrhovatelem vyhodnocena jako nerelevantní a tedy bez nutnosti transpozice, mohou být naopak Evropskou komisí vyhodnocena jako neúplná transpozice směrnice, pro kterou může Komise zahájit řízení pro nesplnění povinnosti podle čl. 258 Smlouvy o fungování EU. Komise v takových případech zpravidla také navrhuje použití postupu dle čl. 260 odst. 3 Smlouvy o fungování EU, tj. možnosti uložení peněžité sankce již při prvním předložení věci Soudnímu dvoru EU. Dále jsou uvedena některá ustanovení směrnice, u nichž by měla být relevantnost, resp. potřeba transpozice, přehodnocena: Čl. 1 odst. 1 směrnice je nesprávně vyhodnocen jako netransponovaný, ačkoli za jeho provedení lze považovat navrhovaný § 1 odst. 1 a 2 návrhu. Do srovnávací tabulky by mělo být doplněno znění § 1 odst. 1 a 2, a to včetně znění poznámky pod čarou. Čl. 2 odst. 7 směrnice je nesprávně vyhodnocen jako nerelevantní z hlediska transpozice, přestože dané ustanovení směrnice fakticky upravuje působnost směrnice, tj. též působnost příslušných transpozičních opatření by měla tomuto ustanovení odpovídat. Do srovnávací tabulky by mělo být doplněno, ze kterých ustanovení navrhovaných nebo jiných vnitrostátních právních předpisů, působnost takto definovaná směrnicí plyne. K čl. 2 odst. 8 a čl. 24 odst. 1 směrnice by měly být doplněny důvody, proč dané ustanovení je nerelevantním z hlediska provedení směrnice. Důvodem je zejména fakultativní povaha předmětných ustanovení, kdy je členským státům dána možnost rozhodnout se, zda zde uvedené subjekty budou osvobozeny ve smyslu směrnice. Pokud se tedy Česká	Akceptováno. Článek 2 odst. 7 je transponován navrhovaným § 70 návrhu zákona o kybernetické bezpečnosti, který zužuje působnost zákona v případě zpravodajských služeb. Do poznámky v transpoziční tabulce k směrnici NIS 2 pak bude u čl. 2 odst. 7 uvedeno, že na ostatní subjekty v oblasti veřejné správy uvedené v čl. 2 odst. 7 se povinnosti vyplývající ze směrnice NIS 2 vztahují, a to z důvodu národního rozhodnutí. Takový postup je zcela v souladu s principem minimální harmonizace, uvedeném v čl. 5 směrnice NIS 2. <i>K čl. 2 odst. 8 a čl. 24 odst. 1 směrnice by měly být doplněny důvody, proč dané ustanovení je nerelevantním z hlediska provedení směrnice. Důvodem je zejména fakultativní povaha předmětných ustanovení, kdy je členským státům dána možnost rozhodnout se, zda zde uvedené subjekty budou osvobozeny ve smyslu směrnice. Pokud se tedy Česká republika rozhodla dotčené subjekty osvobodit, pak jí nevznikla povinnost toto ustanovení provést.</i> Akceptováno. Bylo doplněno, že zmíněné články jsou nerelevantní pro transpozici z důvodu fakultativní povahy předmětných ustanovení. <i>Čl. 2 odst. 11 směrnice by měl být transponován, jelikož zakládá povinnost České republiky toto ustanovení týkající se působnosti směrnice provést, s ohledem na to, že by měly mít také vliv na působnost navrhovaných předpisů.</i> Akceptováno. Článek 2 odst. 11 bude transponován nově vloženým ustanovením. Do ustanovení návrhu

	republika rozhodla dotčené subjekty osvobodit, pak jí nevznikla povinnost toto ustanovení provést. Čl. 2 odst. 11 směrnice by měl být transponován, jelikož zakládá povinnost České republiky toto ustanovení týkající se působnosti směrnice provést, s ohledem na to, že by měly mít také vliv na působnost navrhovaných předpisů. Čl. 2 odst. 13 směrnice je také nutno do českého práva provést. Sice se zdánlivě týká vztahů mezi členským státem a Komisí, ve skutečnosti se jedná o pravidla pro zachovávání důvěrnosti obchodních informací, což může mít dopad na práva a povinnosti jednotlivců. Současně se jedná se o ustanovení, které upřesňuje působnost směrnice, když stanoví podmínky, za kterých se vyměňují některé informace postupem dle směrnice. Odpovídajícím způsobem by tedy měla být upravena také působnost navrhovaných předpisů. V neposlední řadě nutnost provést dotčené ustanovení směrnice vyplývá ze skutečnosti, že se dotýká oblasti bezpečnosti České republiky, resp. čl. 346 Smlouvy o fungování EU. Čl. 9 odst. 3 směrnice by měl být proveden, jelikož ukládá jednak povinnost České republice a jednak jde o ustanovení, které může mít vliv na práva a povinnosti jednotlivců v podobě stanovení postupů a prostředků, které mají být dle tohoto ustanovení nasazeny v případě krize. Čl. 10 odst. 10 směrnice je vyhodnocen jako netransponovaný, ačkoli první část navrhovaného textu § 41 odst. 4 písm. d) bod 2 lze za jeho provedení lze považovat. Citované ustanovení směrnice zakládá pravomoc vnitrostátních orgánů vyžádat si mezinárodní spolupráci, přičemž takové zmocnění musí být výslovně obsaženo ve vnitrostátním právu (čl. 2 odst. 3 Ústavy) a musí být také ve srovnávací tabulce, aby mohlo být oznámeno Evropské komisi.	zákona o kybernetické bezpečnosti týkajícího se informační povinnosti (NÚKIB byl doplněn nový odstavec (§ 66 odst. 2), který zní: „Úřad za účelem plnění informační povinnosti podle odstavce 1 neposkytuje informace, jejichž zpřístupnění by bylo v rozporu se zásadními zájmy členských států Evropské unie v oblasti národní bezpečnosti, veřejné bezpečnosti nebo obrany. Aniž je dotčen přímo použitelný předpis Evropské unie³³⁾, informace, které jsou důvěrné podle unijních či vnitrostátních pravidel, jako jsou pravidla pro zachovávání důvěrnosti obchodních informací, se vyměňují s Evropskou komisí a jinými příslušnými orgány Evropské unie v souladu s příslušným předpisem Evropské unie³⁴⁾ pouze v případě, že je tato výměna nutná pro jeho účely. Vyměňované informace se omezí na informace, které jsou relevantní a přiměřené účelu této výměny. Při těchto výměnách informací se zachovává důvěrnost předmětných informací a jsou chráněny bezpečnost a obchodní zájmy dotčených orgánů a osob.“. Poznámky pod čarou pak zní: 33) Článek 346 Smlouvy o fungování Evropské unie. 34) Směrnice Evropského parlamentu a Rady (EU) 2022/2555.“ Čl. 2 odst. 13 směrnice je také nutno do českého práva provést. Sice se zdánlivě týká vztahů mezi členským státem a Komisí, ve skutečnosti se jedná o pravidla pro zachovávání důvěrnosti obchodních informací, což může mít dopad na práva a povinnosti jednotlivců.

	U čl. 14 odst. 4 směrnice by měla být znovu vyhodnocena slučitelnost, resp. to, zda je skutečně celé ustanovení odst. 4 irelevantní z hlediska transpozice. Sice se většina ustanovení týká postupů mezi orgány EU, některé pravomoci tímto ustanovením zřizovaného orgánu se týkají také pravomoci příslušných vnitrostátních orgánů, jako je např. výměna informací předvídaná čl. 14 odst. 4 písm. f) nebo k), a proto by měla být dotčená ustanovení čl. 14 odst. 4 směrnice provedena do českého práva. Pro čl. 15 odst. 3 a čl. 16 odst. 3 směrnice rovněž platí poznámka k čl. 14 odst. 4. Čl. 19 odst. 5, 6 a 8 směrnice by měl být do českého práva proveden, protože stanoví povinnost členských států předávat zde uvedené výsledky sebehodnocení odborníkům na kybernetickou bezpečnost a předávání dalších informací členským státem odborníkům na kybernetickou bezpečnost. Aby mohly příslušné vnitrostátní orgány tento krok učinit, pak by podle čl. 2 odst. 3 Ústavy pravomoc k tomuto postupu měla být zakotvena v zákoně. Čl. 25 odst. 2 směrnice je vyhodnocen jako irelevantní z hlediska transpozice, avšak z rozdílové tabulky vyplývá, že jej provádí § 14 odst. 1, 2 a 4 a § 15 předloženého návrhu zákona, resp. též prováděcí předpisy podle § 14 odst. 4 předloženého návrhu zákona. Čl. 25 odst. 3 směrnice stanoví povinnost členským státům zohlednit doporučení ENISA. Vzhledem k tomu, že se jedná o uložení povinnosti České republice, mělo by být toto ustanovení do českého práva provedeno. Čl. 27 odst. 1 stanoví povinnost členským státům předávat zde uvedené informace, což předpokládá jeho provedení ve vnitrostátním právu. V rozdílové tabulce je uveden § 58 odst. 1 a 2 předloženého návrhu zákona jako prováděcí ustanovení k čl. 27. Zároveň by k čl. 27	<i>Současně se jedná se o ustanovení, které upřesňuje působnost směrnice, když stanoví podmínky, za kterých se vyměňují některé informace postupem dle směrnice. Odpovídajícím způsobem by tedy měla být upravena také působnost navrhovaných předpisů. V neposlední řadě nutnost provést dotčené ustanovení směrnice vyplývá ze skutečnosti, že se dotýká oblasti bezpečnosti České republiky, resp. čl. 346 Smlouvy o fungování EU.</i> Akceptováno. Článek 2 odst. 13 bude transponován nově vloženým ustanovením. Do ustanovení návrhu zákona o kybernetické bezpečnosti týkajícího se informační povinnosti (NÚKIB byl doplněn nový odstavce (§ 66 odst. 2), který zní: „Úřad za účelem plnění informační povinnosti podle odstavce 1 neposkytuje informace, jejichž zpřístupnění by bylo v rozporu se zásadními zájmy členských států Evropské unie v oblasti národní bezpečnosti, veřejné bezpečnosti nebo obrany. Aniž je dotčen přímo použitelný předpis Evropské unie³³⁾, informace, které jsou důvěrné podle unijních či vnitrostátních pravidel, jako jsou pravidla pro zachovávání důvěrnosti obchodních informací, se vyměňují s Evropskou komisí a jinými příslušnými orgány Evropské unie v souladu s příslušným předpisem Evropské unie³⁴⁾ pouze v případě, že je tato výměna nutná pro jeho účely. Vyměňované informace se omezí na informace, které jsou relevantní a přiměřené účelu této výměny. Při těchto výměnách informací se zachovává důvěrnost předmětných informací a jsou chráněny bezpečnost a obchodní zájmy dotčených orgánů a osob.“

	odst. 1 směrnice mohl jako prováděcí opatření být uveden také § 64 písm. d) předloženého návrhu zákona. Čl. 31 odst. 4 směrnice stanoví povinnost členským státům zajistit zde uvedené pravomoci příslušným orgánům. České republice tedy vznikla povinnost tyto pravomoci zavést a tedy provést čl. 31 odst. 4 směrnice do českého práva. Čl. 32 odst. 6 směrnice požaduje, aby členské státy zajistily, aby zde uvedené fyzické osoby měly pravomoc zajistit dodržování této směrnice. Toto ustanovení tedy nejen ukládá povinnost České republice, ale také zakládá práva jednotlivcům, a je tedy nutné jej provést. Čl. 32 odst. 7 směrnice by neměl být vyhodnocen jako irelevantní z hlediska transpozice, protože stanoví podmínky pro rozhodování o výši pokuty. Dotýká se práv jednotlivců, a jako takový by měl být transponován, což by mohlo být provedeno v předloženém návrhu zákona, nebo v obecných předpisech týkajících se přestupkového řízení a správního trestání. Čl. 32 odst. 8 směrnice by neměl být vyhodnocen jako irelevantní z hlediska transpozice, protože stanoví požadavky na rozhodování příslušných orgánů. Zejména požadavek na odůvodnění takových rozhodnutí a oznámení přijatých opatření lze považovat za založení práv jednotlivců, což zakládá povinnost České republiky toto ustanovení provést do českého práva, resp. ověřit, zda jsou tyto požadavky splněny např. předpisy správního řízení. Čl. 34 odst. 1 by neměl být vyhodnocen jako irelevantní z hlediska transpozice, protože stanoví povinnost České republice zavést systém přiměřených, účinných a odrazujících pokut, a je tedy nutné jej do českého práva provést. Opět se jedná o ustanovení, které zakládá práva jednotlivcům, a tudíž by mělo být transponováno, což částečně	Poznámky pod čarou pak zní: 33) Článek 346 Smlouvy o fungování Evropské unie. 34) Směrnice Evropského parlamentu a Rady (EU) 2022/2555.“ <i>Čl. 9 odst. 3 směrnice by měl být proveden, jelikož ukládá jednak povinnost České republice a jednak jde o ustanovení, které může mít vliv na práva a povinnosti jednotlivců v podobě stanovení postupů a prostředků, které mají být dle tohoto ustanovení nasazeny v případě krize.</i> Akceptováno. Co se týče čl. 9 odst. 3, směrnice NIS 2, budou tyto požadavky zajištěny primárně nikoliv prostřednictvím předloženého návrhu zákona o kybernetické bezpečnosti, ale prostřednictvím připravované legislativy v oblasti krizového řízení státu, která primárně není v gesci NÚKIB; ve vztahu k působnosti NÚKIB budou tyto požadavky zajištěny podle § 44 odst. 4 písm. f) a g) návrhu zákona o kybernetické bezpečnosti prostřednictvím NÚKIB. <i>Čl. 10 odst. 10 směrnice je vyhodnocen jako netransponovaný, ačkoli první část navrhovaného textu § 41 odst. 4 písm. d) bod 2 lze za jeho provedení lze považovat. Citované ustanovení směrnice zakládá pravomoc vnitrostátních orgánů vyžádat si mezinárodní spolupráci, přičemž takové zmocnění musí být výslovně obsaženo ve vnitrostátním právu (čl. 2 odst. 3 Ústavy) a musí být také ve srovnávací tabulce, aby mohlo být oznámeno Evropské komisi.</i> Akceptováno.

		lze vidět v § 58 předloženého návrhu zákona, nebo v obecných předpisech týkajících se přestupkového řízení a správního trestání. Čl. 34 odst. 2 směrnice by neměl být vyhodnocen jako irelevantní z hlediska transpozice, protože stanoví možnost uložení pokuty spolu s některým se zde uvedeným opatřením, tj. opět jde o ustanovení týkající se práv a povinností fyzických a právnických osob.	<i>U čl. 14 odst. 4 směrnice by měla být znovu vyhodnocena slučitelnost, resp. to, zda je skutečně celé ustanovení odst. 4 irelevantní z hlediska transpozice. Sice se většina ustanovení týká postupů mezi orgány EU, některé pravomoci tímto ustanovením zřizovaného orgánu se týkají také pravomoci příslušných vnitrostátních orgánů, jako je např. výměna informací předvídaná čl. 14 odst. 4 písm. f) nebo k), a proto by měla být dotčena ustanovení čl. 14 odst. 4 směrnice provedena do českého práva.</i> Akceptováno jinak. Dotčenou část směrnice, nejen odst. 4, ale odst. 1 až 5 článku 14 provádí § 44 odst. 4 písm. f) návrhu zákona o kybernetické bezpečnosti, přičemž navrhovaná úprava vychází ze stávající úpravy § 22 písm. s) účinného zákona o kybernetické bezpečnosti, která se dlouhodobě osvědčila jako vhodná a funkční. <i>Pro čl. 15 odst. 3 a čl. 16 odst. 3 směrnice rovněž platí poznámka k čl. 14 odst. 4.</i> Akceptováno. Transpozice čl. 15 odst. 3 je provedena § 44 odst. 5 písm. j) návrhu zákona o kybernetické bezpečnosti, v případě čl. 16 odst. 3 je transpozičním § 44 odst. 4 písm. f) návrhu zákona o kybernetické bezpečnosti. Povinnost vůči síti CSIRT plní i NÚKIB, neboť účast jeho zaměstnanců i mimo vládní CERT je v určitých situacích žádána. <i>Čl. 19 odst. 5, 6 a 8 směrnice by měl být do českého práva proveden, protože stanoví povinnost členských států předávat zde uvedené výsledky sebehodnocení</i>

		<i>odborníkům na kybernetickou bezpečnost a předávání dalších informací členským státem odborníkům na kybernetickou bezpečnost. Aby mohly příslušné vnitrostátní orgány tento krok učinit, pak by podle čl. 2 odst. 3 Ústavy pravomoc k tomuto postupu měla být zakotvena v zákoně.</i> Vysvětleno. Z informací získaných v průběhu přípravy směrnice NIS2 máme za to, že vzájemné hodnocení jako proces je prozatím těžko představitelný a ve směrnici nový. Máme za to, že veškeré náležitosti spojené se stanovením procesu výběru expertů, stejně jako praktické aspekty výkonu jejich funkce (zminěná mlčenlivost), jsou ovládány metodikou podle čl. 19 odst. 1, tj. že tento proces je vytvářen de facto na evropské úrovni. Členské státy se následně mohou do takto vytvořeného rámce už jen zapojit nebo nezapojit ("účast je dobrovolná, a srov. § 44 odst. 4 písm. h) návrhu zákona o kybernetické bezpečnosti"). Z tohoto důvodu máme za to, že ustanovení není transpoziční. <i>Čl. 25 odst. 2 směrnice je vyhodnocen jako irelevantní z hlediska transpozice, avšak z rozdílové tabulky vyplývá, že jej provádí § 14 odst. 1, 2 a 4 a § 15 předloženého návrhu zákona, resp. též prováděcí předpisy podle § 14 odst. 4 předloženého návrhu zákona.</i> Vysvětleno. V rozdílové tabulce nevykazujeme čl. 25 odst. 2, nýbrž článek 25 odst. 1, který provádí § 14 odst. 1 a 2 (původně odst. 1, 2 a 4, odst. 4 byl po úpravách přesunut do § 15) a § 15 návrhu zákona o kybernetické bezpečnosti.

		<i>Čl. 25 odst. 3 směrnice stanoví povinnost členským státům zohlednit doporučení ENISA. Vzhledem k tomu, že se jedná o uložení povinnosti České republice, mělo by být toto ustanovení do českého práva provedeno.</i> Akceptováno jinak. Pravděpodobně máte na mysli čl. 25 odst. 2, který stanovuje zmiňovanou povinnost. Bude doplněno, že ustanovení je provedeno § 44 odst. 4 písm. f) návrhu zákona o kybernetické bezpečnosti. <i>Čl. 27 odst. 1 stanoví povinnost členským státům předávat zde uvedené informace, což předpokládá jeho provedení ve vnitrostátním právu. V rozdílové tabulce je uveden § 58 odst. 1 a 2 předloženého návrhu zákona jako prováděcí ustanovení k čl. 27. Zároveň by k čl. 27 odst. 1 směrnice mohl jako prováděcí opatření být uveden také § 64 písm. d) předloženého návrhu zákona.</i> Akceptováno jinak. Domníváme se, že vámi uvedená povinnost členských států je stanovena čl. 27 odst. 2 a 3. Uvedená ustanovení však na odst. 1 odkazují. Za nejvhodnější je tak podle našeho názoru vykázat § 66 odst. 1 písm. d) (dříve § 64 písm. d) návrhu zákona o kybernetické bezpečnosti jako transpoziční pro celý čl. 27 směrnice. <i>Čl. 31 odst. 4 směrnice stanoví povinnost členským státům zajistit zde uvedené pravomoci příslušným orgánům. České republice tedy vznikla povinnost tyto pravomoci zavést a tedy provést čl. 31 odst. 4 směrnice do českého práva.</i> Vysvětleno. Máme za to, že současně účinné znění § 22 zákona o kybernetické bezpečnosti, stejně tak jako

		navrhované znění § 44 (v původním návrhu § 41) naplňuje požadavek na transpozici zmíněného článku. Návrhem zákona je jasně dáno, že kontrola má probíhat podle zákona a v mezích zákona, přičemž není prostor pro ovlivňování výkonu kontroly. NÚKIB je už dnes při výkonu kontroly a ukládání sankcí nezávislý. V minulosti s tímto ani neexistoval náznak pochybnosti, že by tomu tak nemělo být. NÚKIB ukládá pokuty ostatním orgánům státní správy, stejně tak jako celá řada státních orgánů dává sankce jiným státním orgánům, aniž by to muselo být nutně uvedeno podrobným ustanovením o nezávislosti z rámci daného předpisu. Máme také za to, že protože výnosy vlády (která i přesto že je vrcholným orgánem státní správy) nejsou nad zákonem, resp. že předseda vlády je toliko dle současného i navrhovaného znění nadřízeným ředitelem NÚKIB, nicméně jejich role je toliko koordinační a informační, a proto premiér nemá možnost ovlivňovat výkon zákonné působnosti. <i>Čl. 32 odst. 6 směrnice požaduje, aby členské státy zajistily, aby zde uvedené fyzické osoby měly pravomoc zajistit dodržování této směrnice. Toto ustanovení tedy nejen ukládá povinnost České republice, ale také zakládá práva jednotlivcům, a je tedy nutné jej provést.</i> Akceptováno. Pokud jde o oprávnění fyzické osoby jednat za základní subjekt, provedení tohoto ustanovení lze spatřovat v § 161 až 167 občanského zákoníku, které upravují jednání za právnickou osobu. Stanovení odpovědnosti pak lze nalézt v § 159 občanského zákoníku, který upravuje výkon funkce člena voleného orgánu.

		Čl. 32 odst. 7 směrnice by neměl být vyhodnocen jako irelevantní z hlediska transpozice, protože stanoví podmínky pro rozhodování o výši pokuty. Dotýká se práv jednotlivců, a jako takový by měl být transponován, což by mohlo být provedeno v předloženém návrhu zákona, nebo v obecných předpisech týkajících se přestupkového řízení a správního trestání. Akceptováno. Nutnost nalezení řešení odpovídajícího okolnostem daného případu, je jednou z obecně platných zásad pro činnost veřejné správy a jako tzv. zásada přiměřenosti je zakotvena v § 2 odst. 4 správního řádu. V případě trestání se pak uplatňuje tzv. princip individualizace trestu, který zavazuje k tomu, aby všechny individuální okolnosti a specifika daného případu stejně jako osoba pachatele byly řádně zohledněny tak, aby trest odpovídal těmto specifickým. Pravidla pro ukládání správních trestů zohledňujících požadavky daného ustanovení směrnice (určení druhu a výměry správního trestu, povaha a závažnost přestupku, polehčující okolnosti, přitěžující okolnosti, ukládání správních trestů za více přestupků) jsou obsaženy v § 36 až § 41 zákona o odpovědnosti za přestupky a řízení o nich. Příslušná ustanovení zmiňovaných právních předpisů budou vykázána jako transpoziční pro čl. 32 odst. 7. Čl. 32 odst. 8 směrnice by neměl být vyhodnocen jako irelevantní z hlediska transpozice, protože stanoví požadavky na rozhodování příslušných orgánů. Zejména požadavek na odůvodnění takových rozhodnutí a oznámení přijatých opatření lze

		<i>považovat za založení práv jednotlivců, což zakládá povinnost České republiky toto ustanovení provést do českého práva, resp. ověřit, zda jsou tyto požadavky splněny např. předpisy správního řízení.</i> Akceptováno. Odůvodnění je podle § 68 odst. 1 správního řádu zásadně součástí každého správního rozhodnutí. V odůvodnění se pak podle § 68 odst. 3 správního řádu uvedou důvody výroku nebo výroků rozhodnutí, podklady pro jeho vydání, úvahy, kterými se správní orgán řídil při jejich hodnocení a při výkladu právních předpisů, a informace o tom, jak se správní orgán vypořádal s návrhy a námitkami účastníků a s jejich vyjádřením k podkladům rozhodnutí. Tato ustanovení proto budou vykázána k čl. 32 odst. 8 směrnice. Dále bude vykázán § 9 a 10 kontrolního řádu, v nichž jsou upravena práva a povinnosti kontrolujícího a kontrolované osoby. V návaznosti na kontrolu může kontrolovaná osoba podle § 13 odst. 1 kontrolního řádu podat námitky proti kontrolnímu zjištění uvedenému v protokolu o kontrole, a to ve lhůtě 15 dnů ode dne doručení protokolu o kontrole. Toto ustanovení bude tedy též vykázáno. <i>Čl. 34 odst. 1 by neměl být vyhodnocen jako irrelevantní z hlediska transpozice, protože stanoví povinnost České republiky zavést systém přiměřených, účinných a odrazujících pokut, a je tedy nutné jej do českého práva provést. Opět se jedná o ustanovení, které zakládá práva jednotlivcům, a tudíž by mělo být transponováno, což částečně lze vidět v § 58 předloženého návrhu zákona, nebo v obecných</i>

		<i>předpisech týkajících se přestupkového řízení a správního trestání.</i> Akceptováno. Nutnost nalezení řešení odpovídajícího okolnostem daného případu, je jednou z obecně platných zásad pro činnost veřejné správy a jako tzv. zásada přiměřenosti je zakotvena v § 2 odst. 4 správního řádu. V případě trestání se pak uplatňuje tzv. princip individualizace trestu, který zavazuje k tomu, aby všechny individuální okolnosti a specifika daného případu stejně jako osoba pachatele byly řádně zohledněny tak, aby trest odpovídal těmto specifickým. Pravidla pro ukládání správních trestů zohledňujících požadavky daného ustanovení směrnice (určení druhu a výměry správního trestu, povaha a závažnost přestupku, polehčující okolnosti, přitěžující okolnosti, ukládání správních trestů za více přestupků) jsou obsaženy v § 36 až § 41 zákona o odpovědnosti za přestupky a řízení o nich. Příslušná ustanovení zmiňovaných právních předpisů budou vykázána jako transpoziční pro čl. 34 odst. 1. Dále bude v souladu s vaším návrhem jako transpoziční vykázán § 60 odst. 15 písm. a), b, d), f) a g) návrhu zákona o kybernetické bezpečnosti. <i>Čl. 34 odst. 2 směrnice by neměl být vyhodnocen jako irelevantní z hlediska transpozice, protože stanoví možnost uložení pokuty spolu s některým se zde uvedeným opatřením, tj. opět jde o ustanovení týkající se práv a povinností fyzických a právnických osob.</i>

			Akceptováno. Uvedená opatření (v návrhu zákona o kybernetické bezpečnosti provedena v podobě informační povinnosti podle § 20, protiopatření podle § 21, nápravných opatření podle § 59, pozastavení platnosti certifikace podle § 62, pozastavení výkonu řídicí funkce podle § 63) jsou odlišnými instituty s jiným účelem od pokut ukládaných za spáchané přestupky, které jsou uvedeny v § § 60 odst. 15 písm. a), b, d), f) a g) návrhu zákona o kybernetické bezpečnosti. Ustanovení tedy lze vykázat pouze tak, že se ke čl. 34 odst. 2 uvedenou všechna zmíněná ustanovení. Připomínkové místo s vypořádáním souhlasí.
588. Ministerstvo obrany	Z	K § 2 odst. 1 Požadujeme do odstavce 1 vložit nové písmeno „g) <i>kybernetickou bezpečností činností nezbytné k ochraně sítí a informačních systémů, uživatelů a dalších osob dotčených kybernetickými hrozbami</i>“. Dosavadní písmeno g) označit jako písmeno h). Odůvodnění: Návrh zákona o kybernetické bezpečnosti široce používá pojem „kybernetická bezpečnost“, aniž by jej definoval. Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2), přitom definici pojmu „kybernetická bezpečnost“ obsahuje, respektive přebírá jej z nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře	Vysvětleno Co se týče pojmu kybernetické bezpečnosti, jeho obsah se oproti aktuálně účinnému zákonu významně nemění. Kybernetická bezpečnost je definována stejně jako v aktuálním zákoně přes kybernetický prostor a bezpečnost informací. Kybernetická bezpečnost regulované služby je cílem zavádění bezpečnostních opatření, nemůže být tedy zároveň prostředkem (souhrnem opatření). Připomínkové místo s vypořádáním souhlasí.

	ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“). Důvodová zpráva k návrhu zákona uvádí, že stejně jako v případě stávajícího zákona o kybernetické bezpečnosti nebyly až na výjimky do návrhu zákona zahrnuty definice těch pojmů, které jsou definovány ve směrnici NIS 2, kterou zákon transponuje, a to s odůvodněním, že je potřebné aplikovat tzv. eurokonformní výklad. Eurokonformním výkladem přímo neaplikovatelného právního předpisu, jakým je směrnice EU, a tedy i směrnice NIS 2, lze řešit ustanovení nebo definice v zákoně obsažené, které nejsou jednoznačné nebo působí jiné výkladové problémy. Nelze, jím však řešit situaci, kdy dotčená ustanovení nebo definice v zákoně zcela chybí. Důvodová zpráva k návrhu pak zároveň uvádí, že pojem „kybernetická bezpečnost“ je definován stejně jako v zákoně o kybernetické bezpečnosti přes kybernetický prostor a bezpečnost informací. Výkladový slovník kybernetické bezpečnosti, 5. vydání, Praha 2022, vydaný pod záštitou NÚKIB, pak definuje pojem „kybernetická bezpečnost“ hned dvěma způsoby, a to jako: a) „souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru“, a b) „zajištění důvěrnosti, integrity a dostupnosti informací v kybernetickém prostoru.“. Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 pak definovala pojem „kybernetická bezpečnost“ jako „souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění	

		zabezpečeného, chráněného a odolného kyberprostoru v České republice“. Pokud tak existuje společenská potřeba kybernetickou bezpečnost regulovat a kontrolovat její zajišťování orgánem veřejné moci, měl by být pojem „kybernetická bezpečnost“ definován způsobem, který poskytne dostatečnou právní jistotu regulovaným subjektům. A to zvláště za situace, kdy existuje definice pojmu „kybernetická bezpečnost“ ve směrnici NIS 2 a současně je užíváno několik od této definice odlišných definic ve vnitřním prostředí České republiky. Vložení definice pojmu „kybernetická bezpečnost“ tak bude podstatným přínosem pro právní jistotu i srozumitelnost právního předpisu také s ohledem na násobné navýšení počtu regulovaných subjektů.	
589. Ministerstvo obrany	Z	K § 13 odst. 1 až odst. 5 a) Požadujeme text v odstavci 1 změnit následovně: <i>„(1) Poskytovatel regulované služby</i> <i>a) identifikuje všechna primární aktiva v rámci celé organizace, která souvisejí s poskytováním regulované služby,</i> <i>b) u primárních aktiv určených podle písm. a) identifikuje a určí související organizační části organizace a podpůrná aktiva.“.</i> b) Požadujeme text v odstavci 2 opravit následovně: <i>„(2) Organizační části a aktiva identifikovaná podle odstavce 1 písm. a) b) a c) tvoří rozsah řízení kybernetické bezpečnosti (dále jen „stanovený rozsah“).“.</i> c) Požadujeme text v odstavci 3 upravit, a to následovně: <i>„(3) O provedení identifikace a určení organizačních částí a aktiv podle odstavce 1 vede poskytovatel regulované služby dokumentovaný záznam, a to včetně evidence primárních aktiv, která byla ze stanoveného rozsahu vyjmuta, a odůvodnění jejich vyjmutí.“.</i> d) Požadujeme odstavec 4 a 5 vypustit.	Vysvětleno Stanovený rozsah se vztahuje na aktiva související s regulovanou službou (nikoliv všechna identifikovaná primární aktiva - pokud všechna nesouvisí s regulovanou službou). Pracuje se s typovými aktivy, nikoliv s každou službou/informací jako takovou zvlášť. Jde o základní identifikaci služeb, které organizace poskytuje (za jakým účelem je vytvořena a co jsou její core služby). Primární aktiva, která nesouvisí s regulovanou službou není potřeba hodnotit (návrh zákona to nepožaduje). Nepovažujeme tuto změnu při identifikaci aktiv za nepřiměřenou Je pravda, že v tomto ustanovení se projevují zkušenosti Úřadu z kontrolní činnosti, kdy správně stanovit rozsah ISMS organizacím způsobuje značné problémy. Oproti platné právní úpravě došlo k otočení způsobu identifikace primárních aktiv, na která se nyní pohlíží z pohledu celé organizace a určují se ta, která

		Odůvodnění: Jak vyplývá z textu návrhu zákona i důvodové zprávy k návrhu, okruh adresátů návrhu zákona je stanoven na „poskytovatele regulované služby“. Je tak nepřiměřeným zásahem do práv zákonem dotčených osob a porušením zásady hospodárnosti, respektive zásady veřejného práva zatěžovat dotčené osoby co nejméně, pokud se vytváří regulace a s tím související kontrolní činnost i pro oblast, která není předmětem regulace, tj. v případě připomínkovaného ustanovení pro primární aktiva organizace nesouvisející s poskytováním regulované služby. Požadavkem na evidenci veškerých primárních aktiv organizace je vytvářena pro organizace ekonomická i časová zátěž, která zejména u rozsáhlých organizací nebo organizací, u nichž je poskytování regulované služby pouze okrajovou záležitostí, má na tyto organizace zásadní dopad, aniž by byla taková regulace odůvodnitelná a ospravedlnitelná veřejným zájmem nebo měla faktický vliv na kybernetickou bezpečnost regulovaných služeb. Zároveň ustanovením § 13 odst. 1 dává návrh zákona najevo, že NÚKIB nedůvěřuje schopnostem organizací určit si, která primární aktiva organizace souvisejí s poskytováním regulované služby.	souvisejí s regulovanou službou. Nesouhlasíme s tím, že na zajištění kybernetické bezpečnosti současné znění předmětného ustanovení nebude mít vliv, a že se jedná o nepřiměřený zásah do práv povinných subjektů. Naopak naší snahou je zmírnění požadavků směrnice NIS 2 zavádět opatření na celou organizaci v tom smyslu, že se nejprve povinná osoba podívá na celou organizaci, ale opatření zavádí na těch aktivech, která se přímo dotýkají poskytování regulované služby. Připomínkové místo s vypořádáním souhlasí.
590. Ministerstvo obrany	Z	K § 16 odst. 1 a odst. 3 a) Požadujeme doplnit text v odstavci 1, a to následovně: <i>„(1) Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a mají významný dopad na poskytování regulované služby.“.</i> b) Požadujeme text v odstavci 3 upravit, a to následovně:	Neakceptováno Požadavek na hlášení všech kybernetických bezpečnostních incidentů bez ohledu na to, zda mají významný dopad, reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto

		„(3) <i>Způsob stanovení významného dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby poskytovatelem regulované služby v režimu nižších povinností stanoví prováděcí právní předpis.</i>“. Odůvodnění: Hlášení každého incidentu bez ohledu na jeho významnost (například výpadky webových služeb v řádu sekund) dostatečně nevyrovnává administrativní náročnost zpracování hlášení málo významných nebo nevýznamných incidentů jak ze strany NÚKIB, tak ze strany poskytovatelů regulovaných služeb. Pokud i samotný NÚKIB v důvodové zprávě v souvislosti s hlášením incidentů subjekty v režimu nižších povinností uvádí, že „<i>Úřad nemůže u těchto incidentů nabídnout relevantní podporu pro jejich zvládnutí</i>“, lze předpokládat, že NÚKIB bude ve shodné situaci i v případě nevýznamných incidentů poskytovatelů regulované služby v režimu vyšších povinností. Omezení hlášení incidentů pouze na incidenty s významným dopadem je přitom zcela v souladu s cílem směrnice NIS 2 zajistit vysokou společnou úroveň kybernetické bezpečnosti v EU, jelikož i samotná směrnice NIS 2 vyžaduje ve svém čl. 23 odst. 1 oznamování pouze významných incidentů. Úřadem navrhovaná povinnost oznamovat každý incident jde rovněž proti odst. 102 preambule směrnice NIS 2, v němž je uvedeno: „<i>Členské státy by měly zajistit, aby povinnost podat toto včasné varování nebo následné oznámení incidentu neodváděla zdroje oznamujícího subjektu od činností souvisejících s řešením incidentu, které by měly být upřednostněny, aby se zabránilo tomu, že kvůli povinnosti oznamování incidentů dojde buď k odvádění zdrojů z řešení reakce na významný incident, nebo se jinak naruší úsilí subjektů v tomto ohledu.</i>“.	subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob. Obsahové náležitosti prvotního hlášení jsou omezeny na nezbytné minimum, díky kterému bude Vládní CERT schopen posoudit, zda má incident významný dopad na kybernetický prostor státu, a nemělo by ohlašovatele nadměrně zatěžovat. Následující fáze hlášení budou požadovány pouze u incidentů, u nichž byl ze strany Vládního CERT vyhodnocen významný dopad na bezpečnost státu. Závěr: Po ústním projednání a úpravě ustanovení připomínkové místo s vypořádáním souhlasí.
591. Ministerstvo obrany	Z	K § 18 odst. 2 Požadujeme odstavec 2 upravit, a to následovně:	Akceptováno Připomínkové místo s vypořádáním souhlasí.

		„(2) Na žádost dotčeného poskytovatele regulované služby poskytne Úřad nebo Národní CERT metodickou podporu k provádění možných zmírňujících opatření, a případnou další technickou podporu ke zvládnutí hlášeného kybernetického bezpečnostního incidentu s významným dopadem na poskytovatele regulované služby nebo na kybernetický prostor státu.“. Odůvodnění: Ustanovení v původním znění neumožňuje žádat o metodickou a/nebo technickou podporu poskytovateli regulovaných služeb v režimu vyšších povinností, jehož incident nemá významný dopad na kybernetický prostor státu, přestože může mít takový incident fakticky významný dopad na poskytování regulované služby. Stanovení významného dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby se dle ustanovení § 16 odst. 2 provádí pouze u poskytovatele regulované služby v režimu nižších povinností. Návrh zákona o kybernetické bezpečnosti tak nezná kybernetický bezpečnostní incident s významným dopadem na poskytování regulované služby poskytované poskytovatelem v režimu vyšších povinností.	
592. Ministerstvo obrany	Z	K § 23 Požadujeme do § 23 vhodným způsobem doplnit následující nebo významově obdobný text: „V dostatečném předstihu před vydáním rozhodnutí podle odstavce 1 nebo opatření obecné povahy podle odstavce 4, a pokud to konkrétní okolnosti umožňují, vyrozumí Úřad o záměru vydat a o obsahu rozhodnutí nebo opatření obecné povahy státní orgány podílející se na zajištění kybernetické bezpečnosti a kybernetické obrany.“ Odůvodnění: Reaktivní protiopatření má s ohledem na svou povahu mít efekt v kybernetickém prostoru a pozitivní efekt na kybernetickou	Akceptováno jinak - nyní § 24 Cíl připomínky bude upraven v rámci vzájemné spolupráce na úrovni interního řízení obou organizací. Připomínkové místo s vypořádáním souhlasí.

		bezpečnost, zároveň však nelze vyloučit, že může podstatně ovlivnit činnosti dalších státních orgánů, vedle NÚKIB, podílejících se na zajištění kybernetické bezpečnosti a kybernetické obrany a na řešení konkrétního incidentu. Např. reaktivní opatření, jehož obsahem bude uložení povinnosti poskytovateli internetového připojení omezit či vypnout přístup k internetu určitému okruhu orgánů a osob, může mít za následek omezení možnosti České republiky efektivně zakročit proti kybernetickému útoku pomocí aktivního zásahu (viz § § 16g zákona č. 289/2005 Sb., o Vojenském zpravodajství) nebo může vést k narušení sledování pachatele trestné činnosti – např. narušení sběru důkazů o trestné činnosti. K vyhodnocení dopadů případného reaktivního protiopatření a přijetí adekvátní reakce státními orgány podílejícími se na zajištění kybernetické bezpečnosti a kybernetické obrany proto navrhuje zavést s ohledem na aktuální situaci notificační povinnost Úřadu vůči těmto orgánům. Zároveň s ohledem na citlivost předmětné informace považujeme za vhodné okruh adresátů takové informace omezit pouze na státní orgány. V případě, že by předkladatel považoval okruh adresátů za příliš široký, navrhuje zachování zde navrhovaného ustanovení a omezení rozsahu adresátů pouze na Vojenské zpravodajství, které je, jak je uvedeno výše, pověřeno ze zákona zakročit proti kybernetickému útoku nebo hrozbě. Zakročení proti útoku nebo hrozbě lze předpokládat jako pravděpodobný následek, zejména v situaci trvajícího kybernetického útoku, v případě, kdy přijetí reaktivního protiopatření by nebylo dostatečné.	
593. Ministerstvo obrany	Z	K § 40 Požadujeme do § 40 vhodným způsobem doplnit následující nebo významově obdobný text: „V dostatečném předstihu před vydáním opatření k řešení stavu kybernetického nebezpečí podle odst. 1 písmeno e) nebo f), a pokud	Akceptováno jinak - nyní § 41 Cíl připomínky bude upraven v rámci vzájemné spolupráce na úrovni interního řízení obou organizací. Připomínkové místo s vypořádáním souhlasí.

		to konkrétní okolnosti umožňují, vyrozumí Úřad o záměru vydat a o obsahu tohoto opatření státní orgány podílející se na zajištění kybernetické bezpečnosti a kybernetické obrany.“ Odůvodnění: Obsah povinnosti ukládané v rámci opatření během stavu kybernetického nebezpečí může mít dopady na činnost ostatních státních orgánů, které se podílejí na zajištění kybernetické bezpečnosti a obrany. Blíže viz odůvodnění k předchozí připomínce.	
594. Ministerstvo obrany	Z	K § 45 S ohledem na níže uvedené aspekty rizikovosti penetračních testů navrhuje uzákonit vedení evidence všech provedených penetračních testů s uvedením osob, které penetrační test prováděly, aby v případě zjištění kybernetického bezpečnostního incidentu v návaznosti na nekalé jednání osob provádějících penetrační test bylo možné přikročit k odpovídajícím nápravným / kontrolním krokům i u ostatních poskytovatelů regulované služby, u nichž byl penetrační test prováděn stejnou osobou. V návaznosti na evidenci dále navrhuje stanovení povinnosti poskytovatelům regulovaných služeb informovat NÚKIB o provedení penetračního testu s uvedením doby a osoby provádějící penetrační test. Uvedené informace bude možné využít, v případě jejich zpracování v rámci informačního systému, i pro automatickou kontrolu plnění povinnosti provádět penetrační test minimálně jednou za 2 roky (5 let v případě částí). Odůvodnění: Návrh zákona uvádí, že NÚKIB vede evidenci penetračních testů, nikde v návrhu však není explicitní povinnost pro poskytovatele regulovaných služeb NÚKIB o provedení penetračního testu informovat, či předat zprávu z provedení penetračního testu. NÚKIB	Neakceptováno - nyní § 48 Jakkoliv si uvědomujeme potenciální výhody, které by zavedení takového procesu návrhu zákona mohlo přinést, nemáme za to, že se jedná o řešení proporcionální k zátěži, kterou by především povinným osobám, ale také Úřadu přinesla. Na základě této připomínky však dojde k upřesnění náležitostí evidence proběhlých penetračních testů u povinných subjektů, tj. jaké náležitosti mají být zaznamenány, když si subjekt bude nechávat penetrační testování v souladu s vyhláškou o bezpečnostních opatřeních pro režim vyšších povinností dělat - tato úprava bude do vyhlášky o bezpečnostních opatřeních pro režim vyšších povinností upřesněna před zahájením mezirezortního připomínkového řízení k této vyhlášce a připomínka může být dále upřesněna v tomto řízení. Připomínkové místo s vypořádáním souhlasí.

		je oprávněn nařídit provedení penetračního testu v rámci opatření během vyhlášeného stavu kybernetického nebezpečí. Při provádění penetračních testů získá osoba provádějící penetrační test mnohdy přístup k citlivým informacím poskytovatele. Jelikož tatáž osoba může provádět penetrační testy u více poskytovatelů regulované služby, může tak shromažďovat informace napříč státní správou i soukromou sférou. Zároveň je třeba vzít v úvahu skutečnost, že pro zachování nezávislosti a reálnosti útoku zvenku jsou zpravidla osobami provádějící penetrační test externisté, tj. osoby, nad kterými poskytovatel regulované služby má nižší míru kontroly.	
595. Ministerstvo obrany	Z	K § 58 odst. 15 písm. a), b) a g) Požadujeme dotčená písmena upravit, a to následovně: <i>„a) 250 000 000 Kč nebo do výše 2 % čistého celosvětového ročního obratu dosaženého právnickou osobou nebo, pokud je obviněný součástí konsolidačního celku, dosaženého konsolidačním celkem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 1 písm. a), písm. d) až ~~k~~g) a písm. m) až p), odstavce 3 písm. a), e) a f), odstavce 6 písm. b) a odstavce 8 písm. a) a b),“</i> <i>„b) 175 000 000 Kč nebo do výše 1,4 % čistého celosvětového ročního obratu dosaženého právnickou osobou nebo, pokud je obviněný součástí konsolidačního celku, dosaženého konsolidačním celkem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 2 písm. a), písm. d) až ~~k~~g) a písm. m) až p) a odstavce 8 písm. d),“</i> <i>„g) 2 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. h) až k), odstavce 2 písm. h) až k), odstavců 10, 11 a 12 a odstavce 14 písm. d),“</i>. Odůvodnění:	Neakceptováno - nyní § 60 Sankce, resp. jejich minimální výše, za připomínkované skutkové podstaty přestupků vyplývá z implementované směrnice NIS 2. Závěr: Po ústním projednání a úpravě § 16 návrhu připomínkové místo s vypořádáním souhlasí.

		Stanovená maximální výše pokut u přestupků uvedených v § 58 odst. 1 písm. h) až l) je zjevně nepřiměřená povaze sankcionovaného přestupku. Jedná se fakticky o oznamovací povinnosti, které nemají přímý dopad na kybernetickou bezpečnost poskytované regulované služby, a není tak odůvodněné, aby za takový přestupek mohla být uložena pokuta ve výši až 250 000 000 Kč, respektive 175 000 000 Kč.	
596. Ministerstvo obrany	Z	K § 59 odst. 2 Požadujeme dotčený odstavec vypustit. Odůvodnění: Uvedené ustanovení je nepřípustné v právním řádu demokratického právního státu, a to z důvodu, že zásadně odporuje pravidlu „in dubio pro reo“ (v pochybnostech ve prospěch obviněného) vycházejícího z principu nevinu, které je navíc zakotveno i v § 69 odst. 2 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, konkrétně: „<i>Dokud není pravomocným rozhodnutím o přestupku vyslovena vina obviněného, hledí se na něj jako na nevinného. V pochybnostech správní orgán rozhodne ve prospěch obviněného.</i>“. Jak se vyjádřil i Ústavní soud, také přestupková řízení podléhají procesním garancím obvyklým pro trestní právo (z takové premisy vychází nálezy II. ÚS 192/05). V právním státě je tak nepřípustné takovým způsobem přenášet povinnost správního orgánu unést důkazní břemeno prokázání viny a transformovat ji, navíc zcela nesystémově, na povinnost pachatele prokázat svou nevinu. A tím zásadním způsobem zasáhnout do již výše uvedené presumpce nevinu.	Akceptováno Připomínkové ustanovení bylo z návrhu zákona vypuštěno. Připomínkové místo s vypořádáním souhlasí.
597. Ministerstvo obrany	Z	K § 59 odst. 3 Požadujeme dotčený odstavec upravit, a to následovně:	Vysvětleno - nyní § 61 Úprava vypuštění ustanovení o zákazu <i>reformationis in peius</i> v případě příkazu vychází z obdobné úpravy v rámci „velkého“ trestního práva. Zásada zákazu

	„(3) Na postup Úřadu podle tohoto zákona se ustanovení § 43, § 68 písm. b), § 70, § 71, § 80 odst. 3, § 88 odst. 2, § 89, ~~§ 90 odst. 3~~, § 95 odst. 3 a § 96 odst. 1 písm. b) zákona o odpovědnosti za přestupky a řízení o nich¹⁷⁾ nepoužijí.“. Odůvodnění: Ustanovení § 90 odst. 3 zákona o odpovědnosti za přestupky stanoví: „Pokud byl proti příkazu podán odpor, nelze obviněnému v řízení uložit jiný druh správního trestu s výjimkou napomenutí nebo vyšší výměru správního trestu, než mu byly uloženy příkazem; to neplatí, pokud správní orgán v řízení změnil právní kvalifikaci skutku.“. Z výše uvedeného vyplývá, že se NÚKIB návrhem zákona pokouší o prolomení zákazu „reformationis in peius“ (zákaz změny k horšímu), který je dle našeho názoru nedílnou součástí práva na spravedlivý proces a který je zjevně důvodně zakotven nejen v zákoně o odpovědnosti za přestupky a řízení o nich, ale rovněž i ve správním řádu, a je tedy běžnou součástí procesu v rámci správního trestání. Zásada zákazu „reformationis in peius“ má zabránit situaci, kdy budou odporovatelé odrazováni od podání odporu obavou, že jim může být přihráno. Je na správním orgánu, aby provedl řádné šetření skutku již před vydáním příkazu, nikoliv až po podání odporu proti příkazu. Obavy navrhovatele zákona vyjádřené v důvodové zprávě, že nebude možné rozšířit předmět řízení a uložit vyšší pokutu, než která byla stanovena v příkazu, jsou zjevně liché, když § 90 odst. 3 zákona o odpovědnosti za přestupky výslovně umožňuje uložit vyšší výměru správního trestu, tj. i vyšší pokutu. Nelze tedy souhlasit s myšlenkou, že by se předmět přestupkového řízení v případě podání odporu rozšířil o nové skutky. Takový postup není v demokratickém právním státě přípustný.	<i>reformationis in peius</i> neplatí v trestním řízení při zrušení trestního příkazu, přičemž tato úprava nikdy nebyla shledána v rozporu s právem na spravedlivý proces. Zásada zákazu <i>reformationis in peius</i> v případě příkazu není součástí práva na spravedlivý proces a je tudíž v dispozici zákonodárce, zda ji s ohledem k regulované oblasti zavede. V oblasti kybernetické bezpečnosti se nejeví vhodné, aby nebylo po zrušení příkazu možné reflektovat případné nové skutečnosti v uložení vyšší pokuty, a to například za situace, kdy je primárním cílem ukládané pokuty donutit obviněného ke splnění porušované povinnosti. Ustanovení § 90 odst. 3 zákona o odpovědnosti za přestupky přitom výslovně neumožňuje uložit vyšší výměru správního trestu, tj. i vyšší pokutu, pokud byl proti příkazu podán odpor. Zásada zákazu <i>reformationis in peius</i> v případě odvolání podle § 90 odst. 3 správního řádu zůstává zachována. Obviněný tak není nikterak odrazován od podání řádného opravného prostředku. Formulace v důvodově zprávě týkající se rozšíření předmětu přestupkového řízení o nové skutky v případě podání odporu bude upravena. Připomínkové místo s vypořádáním souhlasí.

		Pokud bude mít návrhovaatel potřebu rozšířit předmět řízení o nové skutky, bude potřeba, aby o těchto nových skutečích vedl nové přestupkové řízení.	
598. Ministerstvo obrany	Z	K § 69 odst. 1 a 2 Požadujeme do § 69 doplnit nový odstavec, který zní: „Ustanovení odstavců 1 a 2 se nevztahují na Vojské zpravodajství. Vojské zpravodajství má povinnost se řídit pravidly a doporučeními tohoto zákona v rozsahu, ve kterém to povaha jeho činnosti umožní.“ Odůvodnění: S ohledem na specifické postavení a především činnosti Vojského zpravodajství požadujeme zakomponovat obecnou výjimku z povinností souvisejících s regulací a nastavením bezpečnostních opatření. Kromě zpravodajské činnosti se Vojské zpravodajství významně podílí i na aktivní obraně České republiky v kybernetickém prostoru. Tyto činnosti jsou či mohou být neslučitelné s některými požadavky vyplývajícími z návrhu zákona. Význam dopadů navrhovaného zákona vůči Vojskému zpravodajství spočívá v oblasti vzájemné součinnosti a spolupráce, nikoliv v rovině regulatorních dopadů vůči Vojskému zpravodajství jakožto subjektu veřejné správy. Zdůrazňujeme, že navrhovaná výjimka se nevztahuje k povinnostem v oblasti spolupráce a součinnosti – viz odst. 3. Obecnou výjimkou není snaha „vyvinut“ se z povinností. Vojské zpravodajství považuje za nutné trvat na nutnosti legislativně deklarovat závazek, že i Vojské zpravodajství dodržuje a řídí se zněním navrhované právní úpravy.	Neakceptováno Ačkoliv plně respektujeme postavení Vojského zpravodajství jako významné a specifické složky podílející se na bezpečnosti České republiky, nepovažujeme za vhodné nahradit stávající režim v § 33 odst. 1 současného zákona úplným odstraněním Vojského zpravodajství z návrhu nového zákona. Na základě připomínek však došlo k další úpravě ustanovení § 70 a jeho dalšímu přiblížení současnému znění § 33 odst. 1. Zaprvé došlo k odstranění odkazování na celé hlavy návrhu a ustanovení jsou vyjmenována jednotlivými paragrafy. Došlo k odstranění celé soustavy servisních ustanovení týkajících se procesu registrace a zápisu, případně jejich změn - v tomto byla zavedena přiměřenost užití § 10 o zápisu do evidence, bez tohoto ustanovení by návrh už nijak neupravoval postavení zpravodajských služeb mezi regulovanými službami. Z tohoto důvodu však také muselo dojít k doplnění regulované služby, tedy orientačního bodu, podle kterého je celá regulace vystavěna. Tady je opět nutné zdůraznit, že z Hlavy I je zachován současný § 1 odst. 3, tedy že utajované systémy jsou zcela mimo působnost zákona - § 70 v návrhu se tedy orientuje vždy a výhradně na ty části organizace, které jsou neutajované. Došlo také k odstranění použití ustanovení o stavu kybernetického nebezpečí nebo o výjimce z práva na informace (původně celá Hlava IV). Do ustanovení o součinnosti byly vedle už uvedeného („nebrání-li plnění povinností zvláštní předpis“) ještě navíc doplněno ustanovení, že předávání informací zpravodajskými

			službami se vždy řídí zákonem o zpravodajských službách. Reakce připomínkového místa: Ministerstvo obrany trvá na připomínce. Požadujeme pracovní setkání se zástupci NÚKIB kvůli věcnému vypořádání připomínky. Závěr: Po schůzce byla připomínka vypořádána.
599. Ministerstvo obrany	D	K § 2 odst. 2 písm. k) Doporučujeme před slovo „hrozbami“ vložit slovo „kybernetickými“: „k) zranitelností slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více kybernetickými hrozbami.“. Odůvodnění: Návrh zákona v § 2 odst. 2 písm. c) definuje pojem „kybernetická hrozba“. Pokud se tedy v dalších ustanoveních zákona má na mysli kybernetická hrozba, měl by být v takových ustanoveních používán definovaný pojem „kybernetická hrozba“ a nikoliv pouze nedefinovaný pojem „hrozba“.	Neakceptováno Považujeme za důležité, aby se v souvislosti se zranitelnostmi uvažovalo pouze o hrozbě v obecném slova smyslu, jelikož definice směřuje na původ hrozby (která může být i mimo kyber), kdyby zde byla kybernetická hrozba jako pojem, který odkazuje na hrozbu, která má vliv na kyber, neplnila by svůj účel. Hrozba je obecně o tom, že se něco s nějakou pravděpodobností stane (požár, mráz, ztráta el., neoprávněné zpracování osobních údajů, porušení zákonů apod.). Připomínkové místo s vypořádáním souhlasí.
600. Ministerstvo obrany	D	K § 29 odst. 2 Doporučujeme do důvodové zprávy doplnit význam pojmu "jiná součinnost" nebo zvažít jeho zrušení. Odůvodnění: Pojem je dle našeho názoru neurčitý.	Akceptováno - nyní § 30 Formulace "a jinou součinnost" byla odstraněna. Připomínkové místo s vypořádáním souhlasí.
601. Ministerstvo obrany	D	K § 34 odst. 3 Doporučujeme nahradit dosavadní slova „strategicky významné služby“ slovy „regulované služby, která je strategicky významnou službou, do evidence“.	Akceptováno jinak - nyní § 35 Připomínkované ustanovení bylo upraveno následovně: „Poskytovatel strategicky významné služby začne plnit povinnosti uvedené v odstavcích 1 a

		Odůvodnění: Návrh zákona neupravuje doručování vyrozumění o zápisu strategicky významné služby, resp. nehovoří o vyrozumívání ze strany NÚKIB, upravuje jen vyrozumívání o zápisu regulované služby.	2 pro každou strategicky významnou službu nejpozději do 1 roku ode dne doručení písemného vyrozumění o označení regulované služby jako významné služby v evidenci regulovaných služeb podle § 28 odst. 3. “. Připomínkové místo s vypořádáním souhlasí.
602. Ministerstvo obrany	D	K § 58 odst. 1 a 2 a) Doporučujeme doplnit odstavec 1 písm. d), a to následovně: <i>„d) při stanovení rozsahu řízení kybernetické bezpečnosti neidentifikuje všechna primární aktiva, která souvisejí s poskytováním regulované služby, podle § 13 odst. 1 písm. a),“.</i> b) Doporučujeme upravit text odstavce 1 písm. e), a to následovně: <i>„e) při stanovení rozsahu řízení kybernetické bezpečnosti neurčí všechny organizační části a podpůrná aktiva související s poskytováním regulované služby podle § 13 odst. 1 písm. b) ~~všechna primární aktiva související s poskytováním regulované služby podle § 13 odst. 1 písm. b) nebo organizační části a podpůrná aktiva podle § 13 odst. 1 písm. c),~~“.</i> c) Doporučujeme doplnit odstavec 2 písm. d), a to následovně: <i>„d) při stanovení rozsahu řízení kybernetické bezpečnosti neidentifikuje všechna primární aktiva, která souvisejí s poskytováním regulované služby, podle § 13 odst. 1 písm. a),“</i> d) Doporučujeme upravit text odstavce 2 písm. e), a to následovně: <i>„e) při stanovení rozsahu řízení kybernetické bezpečnosti neurčí všechny organizační části a podpůrná aktiva související s poskytováním regulované služby podle § 13 odst. 1 písm. b) ~~všechna primární aktiva související s poskytováním regulované služby podle § 13 odst. 1 písm. b) nebo organizační části a podpůrná aktiva podle § 13 odst. 1 písm. c),~~“.</i>	Neakceptováno - nyní § 60 Vzhledem k tomu, že nebyla akceptována připomínka k § 16, není možné akceptovat ani tuto připomínku. Závěr: Po ústním projednání a úpravě § 16 připomínkové místo s vypořádáním souhlasí.

		Odůvodnění: Návrh úpravy § 58 odst. 1 a 2 souvisí s navrhovanou úpravou § 13 odst. 1 obsaženou v zásadní připomínce č. 3. Při akceptaci zásadní připomínky č. 3 by znění uvedených ustanovení § 58 odst. 1 a 2 neodpovídalo znění § 13.	
603. Ministerstvo financí	Z	Obecně Obecně vždy platí, že kapitola státního rozpočtu, která předkládá podobný materiál ve své gesci (v tomto případně 378 – Národní úřad pro kybernetickou a informační bezpečnost a další dotčené kapitoly), si musí zajistit finanční krytí v rámci svého rozpočtu. Zároveň je zapotřebí respektovat ustanovení § 25 odst. 4 zákona č. 218/2000 Sb., rozpočtová pravidla, ve znění pozdějších předpisů, podle něhož nemůže-li organizační složka státu zajistit úhradu nutného výdaje, protože na jeho úhradu částka nebyla v dostatečné výši rozpočtována, je povinna zajistit prostředky státního rozpočtu na úhradu tohoto výdaje přednostně přesunem prostředků uvnitř svého rozpočtu.	Neakceptováno S ohledem na skutečnost, že se v rámci návrhu jedná o podstatné rozšíření povinností a návrh má veliké finanční dopady, přičemž ale zároveň podstatná část návrhu je transpozicí směrnice nebo byla uložena ke zpracování úkolem Bezpečnostní rady státu, není možné hradit náklady z aktuálního rozpočtu NÚKIB, neboť toto rozšíření nebylo možné předpokládat. Není možná ani relokace stávajících zdrojů, neboť tyto jsou plně vytíženy v souladu s aktuálně schválenou koncepcí NÚKIB, která s touto změnou nepočítá. Reakce připomínkového místa Ministerstvo financí trvá na svých zásadních připomínkách. Zásadní připomínky Ministerstva financí týkající se rozpočtových dopadů návrhu zákona o kybernetické bezpečnosti a návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti, nebyly akceptovány. Na připomínkách uplatněných v rámci MPŘ trváme a s návrhem vypořádání ze strany předkladatele materiálu nesouhlasíme. Po schůzce Byla navržena úprava materiálu (předkládací zpráva, RIA, odůvodnění) ve smyslu uplatněné připomínky.

			Návrh úprav byl ze strany připomínkového místa odsouhlasen. Připomínkové místo s vypořádáním souhlasí.
604. Ministerstvo financí	Z	Obecně Navyšování rozpočtu kapitol nad rámec výdajových limitů MF nepovažuje za možné, vzhledem k současné situaci rozpočtového hospodaření. Celkové výdaje státního rozpočtu byly v letech 2020 a 2021 velmi výrazně ovlivněny epidemií COVID-19, v letech 2022 a 2023 konfliktem na Ukrajině a rovněž růstem mandatorních sociálních výdajů s dopadem do dalších let. Naopak nyní je nutná konsolidace státního rozpočtu, vláda ČR připravila návrh konsolidačního úsporného balíčku, který byl zveřejněn dne 11. 5. 2023. Součástí "Ozdravného balíčku 2024/2025" je návrh snížení výdajů průřezově u většiny kapitol. Jelikož je kybernetická bezpečnost považována za prioritu, kapitoly budou nuceny hledat o to větší úspory v jiných oblastech svých výdajů.	Neakceptováno Uvedené konstatování chápeme, právě v souvislosti s probíhající válkou na Ukrajině a celkovým zhoršováním bezpečnostní situace v Evropě je alokace potřebných zdrojů na zabezpečení a obranu (tj. v tomto případě kybernetickou bezpečnost) otázkou priority. Reakce připomínkového místa Ministerstvo financí trvá na svých zásadních připomínkách. Zásadní připomínky Ministerstva financí týkající se rozpočtových dopadů návrhu zákona o kybernetické bezpečnosti a návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti, nebyly akceptovány. Na připomínkách uplatněných v rámci MPŘ trváme a s návrhem vypořádání ze strany předkladatele materiálu nesouhlasíme. Po schůzce Byla navržena úprava materiálu (předkládací zpráva, RIA, odůvodnění) ve smyslu uplatněné připomínky. Návrh úprav byl ze strany připomínkového místa odsouhlasen. Připomínkové místo s vypořádáním souhlasí.
605. Ministerstvo financí	Z	Obecně	Neakceptováno

		MF zásadně nesouhlasí s dopady do personální a platové oblasti, které by měly být nad rámec současných limitů stanovených pro NÚKIB, respektive nad rámec limitů stanovených pro další dotčené rozpočtové kapitoly. Zvýšenou potřebu v personální a platové oblasti, která není v materiálu nikterak konkrétně vyčíslena, MF požaduje pokrýt výhradně v rámci stanovených limitů počtu míst a objemu prostředků na platy, např. na úkor agend, které se přirozeně utlumují, tj. bez nároku na jejich jakékoliv navýšení. Výše uvedené MF požaduje zpracovat a explicitně uvést do všech relevantních částí materiálu.	V souladu s výše uvedeným je potřeba tak jako tak provést aktualizaci schválené koncepce NÚKIB, a tyto oblasti náležitě upravit. Není možné vykonávat ani utlumit v této situaci (jak s ohledem na válečný konflikt a potřebu zvyšování bezpečnosti ve všech oblastech, tak s ohledem na nárůst agendy spojený s směrnicí NIS2) agendu NÚKIB, případně ji vykonávat stávajícím způsobem a je potřeba tyto kapacity navýšit. Pokud by k tomu nedošlo, není možné zajišťovat bezpečnost v poptávané kvalitě, pokud vůbec. Je také potřeba mít na paměti, že NÚKIB jako úřad, který vznikl teprve v roce 2017 a vykonává velkou šíři vysoce aktuální a potřebné agendy (kybernetická bezpečnost, bezpečnost utajovaných systémů, kryptografie,...), která se rozvíjí, než aby stagnovala nebo se utlumovala, je na hraně kapacit již nyní. Reakce připomínkového místa Ministerstvo financí trvá na svých zásadních připomínkách. Zásadní připomínky Ministerstva financí týkající se rozpočtových dopadů návrhu zákona o kybernetické bezpečnosti a návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti, nebyly akceptovány. Na připomínkách uplatněných v rámci MPŘ trváme a s návrhem vypořádání ze strany předkladatele materiálu nesouhlasíme. Po schůzce Materiál byl na základě dohody s připomínkovým místem upraven a připomínka je vypořádána. Připomínkové místo s vypořádáním souhlasí.

606. Ministerstvo financí	Z	Obecně MF požaduje, aby rozpočtové dopady připravovaného zákona byly zabezpečeny v rámci schválených finančních limitů kapitoly NÚKIB a v rámci schválených finančních limitů příslušných dotčených kapitol státního rozpočtu bez požadavku na jejich navýšení. Tato skutečnost by měla být výslovně uvedena ve všech relevantních částech materiálu (návrh usnesení vlády, předkládací zpráva, důvodová zpráva, závěrečná zpráva RIA).	Neakceptováno S ohledem na výše uvedené je takový požadavek nesplnitelný a pokud by byl v dokumentech uveden, byl by nepravdivý. Reakce připomínkového místa Ministerstvo financí trvá na svých zásadních připomínkách. Zásadní připomínky Ministerstva financí týkající se rozpočtových dopadů návrhu zákona o kybernetické bezpečnosti a návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti, nebyly akceptovány. Na připomínkách uplatněných v rámci MPŘ trváme a s návrhem vypořádání ze strany předkladatele materiálu nesouhlasíme. Po schůzce Byla navržena úprava materiálu (předkládací zpráva, RIA, odůvodnění) ve smyslu uplatněné připomínky. Návrh úprav byl ze strany připomínkového místa odsouhlasen. Připomínkové místo s vypořádáním souhlasí.
607. Ministerstvo financí	Z	K předkládací zprávě V souvislosti se závazkem vlády k zefektivnění hospodaření státu a hledání úspor MF požaduje do materiálu doplnit konstatování, že veškeré výdaje a personální nároky spojené s implementací nově navrhovaného zákona o kybernetické bezpečnosti včetně prováděcích předpisů ve všech dotčených rozpočtových kapitolách budou čerpány ze schválených rozpočtových limitů, tj. bez dodatečného	Neakceptováno Takovéto konstatování by nebylo pravdivé, a proto není možné jej uvést do příslušných dokumentů. Povinné osoby, jejichž okruh téměř výhradně pochází z požadavků transpozice směrnice NIS2, nejsou a neměly doposud možnost s adekvátním množstvím prostředků počítat, a tento nárůst požadavků nebyl z

		rozpočtového dopadu. Financování je třeba zajistit i s maximálním využitím finančních prostředků z EU.	jejich strany očekávatelný. V souladu s prioritou vlády na zajišťování bezpečnosti České republiky bude naopak potřeba vyčlenit adekvátní finanční prostředky tak, aby mohl být bezpečnost u těchto subjektů zajištěna a průběžně zajišťována. Reakce připomínkového místa S navrženým vypořádáním nesouhlasíme, přičemž uvádíme: 1. Pokládáme za nezbytné, aby NÚKIB vypracoval aktualizovanou „Koncepci rozvoje NÚKIB“, která by měla být schválena vládou stejně jako v případě nyní již neaktuální předchozí verze. V ní by měly být zapracovány i veškeré nezbytné potřeby úřadu spojené s aktuálně předkládanými legislativními materiály strategického charakteru. 2. Dále upozorňujeme na skutečnost, že předmětný návrh zákona je dotčeným kapitolám znám již řadu měsíců (byl zpracován i věcný záměr zákona), přičemž měly možnost s MF projednat v rámci přípravy SR 2024 a SDV 2025-26 veškeré své nadpožadavky. Nyní je již návrh SR projednáván ve vládě. Do návrhu zákona proto požadujeme uvést, že veškeré výdaje kapitol vyvolaných touto právní úpravou budou vykryty v rámci výdajových limitů schváleného zákona o SR na tyto roky bez navyšujících personálních a finančních požadavků. Na připomínkách uplatněných v rámci MPŘ trváme a s návrhem vypořádání ze strany předkladatele materiálu nesouhlasíme. Po schůzce Byla navržena úprava materiálu (předkládací zpráva, RIA, odůvodnění) ve smyslu uplatněné připomínky.

			Návrh úprav byl ze strany připomínkového místa odsouhlasen. Připomínkové místo s vypořádáním souhlasí.
608. Ministerstvo financí	Z	K předkládací zprávě Ze závěrů obsažených v předloženém materiálu finanční nároky na státní rozpočet vyplývá, že je nezbytné (s ohledem na čl. IV odst. 7 Jednacího řádu vlády a náležitosti obsahu předkládací zprávy) pro jednání schůze vlády i do překládací zprávy uvést rozpočtové dopady a konkrétní zdroj, z kterého budou tyto nároky pokryty (přesun v rámci rozpočtu kapitoly nebo snížení výdajů jiné kapitoly státního rozpočtu a podobně).	Vysvětleno Otázky zdrojů budou řešeny na ústním vypořádání se zástupci Ministerstva financí. Reakce připomínkového místa Ministerstvo financí trvá na svých zásadních připomínkách. Zásadní připomínky Ministerstva financí týkající se rozpočtových dopadů návrhu zákona o kybernetické bezpečnosti a návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti, nebyly akceptovány. Na připomínkách uplatněných v rámci MPŘ trváme a s návrhem vypořádání ze strany předkladatele materiálu nesouhlasíme. Po schůzce Byla navržena úprava materiálu (předkládací zpráva, RIA, odůvodnění) ve smyslu uplatněné připomínky. Návrh úprav byl ze strany připomínkového místa odsouhlasen. Připomínkové místo s vypořádáním souhlasí.
609. Ministerstvo financí	Z	Z návrhu zákona o kybernetické bezpečnosti byly zrušeny pojmy provozovatel informačního systému a správce informačního systému a byl zaveden pouze pojem poskytovatel regulované služby, který je	Vysvětleno S ohledem na obsah připomínky je potřeba uvést, že obě premisy obsažené v připomínce nejsou bohužel

	nositelem odpovědnosti za plnění zákonných požadavků včetně plnění bezpečnostních opatření vyplývajících z návrhů prováděcích předpisů k zákonu o kybernetické bezpečnosti, což má významný dopad v oblasti plnění povinností, které GFR není, jako nový poskytovatel regulované služby v režimu vyšších povinností, schopné ovlivnit (zejména se jedná o plnění povinností souvisejících s provozováním informačního systému, resp. provozováním regulované služby, tj. zajišťováním funkčnosti technických a programových prostředků, které tvoří informační systém – např. akvizice, vývoj a údržba probíhá zcela mimo GFR na základě historických smluvních ujednání a je velmi obtížné a téměř nereálné tato smluvní ujednání změnit, neboť dodavatelé na nové požadavky odmítají přistoupit), - § 6 odst. 2 – stanovit určující kritéria pro poskytovatele regulované služby v režimu nižších povinností, např. prováděcím právním předpisem, - § 7 odst. 1 a 2 – tímto ustanovením se současné VIS (do budoucna regulované služby v režimu nižších povinností) dostanou do režimu KII, resp. do režimu vyšších povinností vůči všem regulovaným službám, které jsou poskytovány poskytovatelem regulované služby, což s sebou přinese velmi významné výdaje na zavedení bezpečnostních opatření v organizacích, zejména zásadní dopad je ve veřejné správě, kde rozpočtové prostředky jsou omezené.	zcela pravdivé. První premisou je, že dosavadní právní úprava VIS odpovídá nyní nově navrhované právní úpravě v režimu nižších povinností, a že tedy se změnou právní úpravy dostávají stávající systémy navrhovatele regulované doposud jako VIS na úrovni KII. Stávající VIS se transformují do režimu vyšších povinností, čemuž ovšem z pohledu bezpečnostních opatření odpovídá dosavadní právní úprava VIS, stejně tak jako KII. Obojí je v současné právní úpravě ovládáno vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti, a proto se o zvýšení v duchu připomínky nejedná, byť významné informační systémy měly některé výjimky stran samotných zaváděných bezpečnostních opatření. Povinnosti spojené s režimem nižších povinností jsou diametrálně nižší a taková úroveň nemá v současné právní úpravě analogii, určitě není odpovídající stávající regulaci VIS. V otázce druhé premisy, tedy že zrušením institutu provozovatele systému dochází k přenesení nerealizovatelných požadavků na ministerstvo, je nutné stejně tak konstatovat, že takové tvrzení není zcela pravdivé. I za současné právní úpravy je na správci systému komplexní plný balík povinností zavádět bezpečnostní opatření a řešit bezpečnost spojených s dodavateli. Taková pravidla odpovídají i návrhu právní úpravy. Zmíněné povinnosti ("např. akvizice, vývoj a údržba probíhá zcela mimo GFR na základě historických smluvních ujednání a je velmi obtížné a téměř nereálné tato smluvní ujednání změnit, neboť dodavatelé na nové požadavky odmítají přistoupit") jsou součástí regulace již nyní a institut provozovatele je k nim jen doplňkem, určitě není tím, co zajišťuje funkčnost systému. Připomínkové místo s vypořádáním souhlasí.

610. Ministerstvo financí	Z	Ustanovení § 4 upravuje působnost zákona, ta je pak s ohledem na odstavec 2 stanovena vyhláškou. Přitom platí, že působnost by měla být stanovena zákonem a nikoliv podzákonným právním předpisem. Navíc platí, že meze zmocnění pro určení kritérií podle § 4 odst. 2 jsou velmi široké.	Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech (§ 3 a § 2 písm. d)), tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby (§ 3, ve spojení s § 2 písm. i) a k) a § 22a). Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon (§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)), a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá (§ 3 a § 2 písm. b)). Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Připomínkové místo s vypořádáním souhlasí.
611. Ministerstvo financí	Z	V §8, §9, §10 a následně v i §11 - Neexistuje popis procesu „Výmazu z evidence poskytovatelů regulovaných služeb“ z podnětu Poskytovatele regulované služby v případě, že Poskytovatel nemá již oprávnění tuto službu poskytovat (např. změnou legislativy). MF navrhuje rozšířit §11, aby podnět pro výmaz z evidence regulovaných	Akceptováno Na základě této, ale i dalších souvisejících připomínek, došlo k tomu, že bude umožněn výmaz z evidence na žádost poskytovatele regulované služby.

		služeb mohl dát i sám Poskytovatel regulovaných služeb. Tento způsob je efektivnější a personálně a odborně méně náročný pro Úřad a současně sám Poskytovatel regulované služby ví, která jeho služba patří či nepatří do regulovaných služeb.	Subjekty však záměrně samy nemohou přes portál službu z evidence smazat, musí o tom rozhodnout vždy Úřad. Do výmazu regulované služby z evidence pak platí fikce, že se na službu zapsanou v evidenci vždy hledí jako na regulovanou službu. Poskytovatel regulované služby tudíž musí plnit vůči této službě všechny povinnosti plynoucí mu ze zákona Připomínkové místo s vypořádáním souhlasí.
612. Ministerstvo financí	Z	V §23 odst. 3 - Nevzetí na vědomí zaslání rozhodnutí prostřednictvím datových schránek. Úřad v odst. 3 zasílá Rozhodnutí o povinnosti provést reaktivní protiopatření adresátovi do vlastních rukou do 72 hodin od jeho vydání. Není zřejmé jakým mechanismem a jakou garantovanou službou toho chce dosáhnout. V případě použití papírové formy je zde riziko, že adresát nebude do 72 hodin informován. Dále není jasné, zda se rozhodnutí týká i FO nepodnikajících. Pod pojmem osoba MF vnímá PO a FO podnikající. Ty v současné době mají povinně zřízenou datovou schránku. MF navrhuje, jako efektivní způsob zaslání Rozhodnutí o povinnosti provést reaktivní protiopatření adresátovi do datové schránky.	Vysvětleno Ustanovení míří především na situace, kdy by bylo třeba bezprostředně reagovat na obsah reaktivního opatření a soukromoprávní poskytovatel regulované služby (vždy podnikající FO nebo PO) bude oddalovat doručení pomoci datové schránky. Varianta doručení do vlastních rukou listinným dopisem nebyla vůbec zvažována (s ohledem na povinnost podnikajících FO a PO mít datovou schránku a povinnost Úřadu do ní doručovat). Sekundárně bude adresát vyrozuměn v rámci Portálu NÚKIB, nicméně doručení v rámci tohoto systému nesplňuje požadavky správního řádu stran doručování rozhodnutí, proto bude takové reaktivní protiopatření vždy doručováno do datové schránky. Připomínkové místo s vypořádáním souhlasí.
613. Ministerstvo financí	Z	V §27 Kritéria pro identifikaci a určení strategicky významné služby odst. 1 ... v odvětvích. Pro odstranění nejistoty a současně tam, kde je to možné zavést jednotný přístup k udržení vnitřní bezpečnosti ČR, MF navrhuje, bylo doplněno do odvětví písmeno e) souhrnně pojmenované jako „výkonné složky vnitřní bezpečnosti“, mezi které patří: a) ozbrojené bezpečnostní sbory jakou jsou Policie ČR, Vězeňská služba ČR, Celní správa ČR a Generální inspekce	Neakceptováno - nyní § 28 Pojem strategicky významná služba je navázán pouze na návrh zákona o kybernetické bezpečnosti. Nemá ambici (a ani to není v kompetenci Úřadu) nijak vyjadřovat celkovou významnost všech subjektů v České republice. Co se zmíněných bezpečnostních orgánů týče, ty jsou dle své významnosti zařazeny buď

		bezpečnostních sborů; b) záchranné sbory a služby kam patří Hasičský záchranný sbor ČR a Zdravotnická záchranná služba; c) přiměřeně i zpravodajské služby jako jsou Bezpečnostní informační služba a Úřad pro zahraniční styky a informace.	jako poskytovatelé regulovaných služeb ve vyšším režimu povinností, nebo poskytovatelé regulovaných služeb v nižším režimu povinností. Základním argumentem pro zařazení mezi strategicky významné služby je pak tzv. „spillover effect“. Tedy kybernetický incident by měl tendenci ovlivnit i další poskytovatele regulovaných služeb. Ministerstvem financí navržené subjekty, jakkoliv bezpochyby důležité pro chod státu, tento přesah v kyberprostoru nemají. Rozpor Naše připomínka směřovala jen na výkonné složky vnitřní bezpečnosti i s ohledem na nynější § 28 odst. 2, kde je uvedeno: „<i>Kritéria pro identifikaci strategicky významné služby zohledňují významnost dopadu narušení regulované služby na bezpečnost České republiky nebo vnitřní či veřejný pořádek.</i>“. Bezpečnost a veřejný pořádek tedy zajišťují (službou) ony námi jmenované výkonné bezpečnostní složky. Zmiňovaná tzv. „spillover effect“ v případě ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku existuje. A případný kybernetický incident má tendenci ovlivnit i další poskytovatele regulovaných služeb, jako jsou například energetika, finance apod. Navíc ohrožení kybernetickým útokem na základní potřeby by vedlo k sekundárním jevům právě zmíněného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Na připomínkách uplatněných v rámci MPŘ trváme a s návrhem vypořádání ze strany předkladatele materiálu nesouhlasíme. Po schůzce

			Připomínkové místo s vypořádání souhlasí.
614. Ministerstvo financí	Z	§ 28 odst. 3 obsahuje nejednoznačně formulovanou definici kritické části stanoveného aktiva, přičemž předložený návrh vyhlášky řeší pouze oblast veřejných komunikačních sítí (a i tuto oblast řeší výčtem různorodých funkcí a komponent). I s ohledem na přístupy používané v zahraničí požadujeme dostatečně přesné vymezení kritických částí například provázáním jejich nedostupnosti s nedostupností celé strategicky významné služby tak (přímý vliv), aby takto zavedené kritérium bylo aplikovatelné i v dalších oblastech (např. energetice). U jiných než kritických aktiv a kritických částí, jejichž nedostupnost má přímou na nedostupnost či kompromitaci strategicky významné služby je možné na základě analýzy rizik realizovat i další opatření.	Neakceptováno - nyní § 29 Navrhovaná definice kritické části stanoveného rozsahu byla důkladně konzultována a vychází z pojetí aktiv v zákoně a jejich hodnocení. Její jednoznačnější vymezení dle našeho názoru není možné v zákoně zpracovat tak, aby zůstala zachována obecnost normy. Ačkoliv NÚKIB akcentuje autonomii poskytovatelů v oblasti řízení rizik a hodnocení aktiv, identifikoval potřebu vymezit nepominutelné funkce stanoveného rozsahu pro regulovanou službu zajišťování veřejné komunikační sítě a regulovanou službu poskytování veřejně dostupné služby elektronických komunikací. V případě, že NÚKIB (ať už sám, nebo ve spolupráci s partnery) nabude přesvědčení, že je potřeba podobně upravit i jiné služby, učiní tak. Odmítáme také navázání mechanismu bezpečnosti dodavatelského řetězce pouze na dostupnost služby. Cílem mechanismu, a i celého zákona je zajištění bezpečnosti informací, tedy důvěrnosti, integrity a dostupnosti informací a dat. Reakce připomínkového místa Na připomínkách uplatněných v rámci MPŘ trváme a s návrhem vypořádání ze strany předkladatele materiálu nesouhlasíme. Po schůzce Připomínkové byla vypořádána.

615. Ministerstvo financí	Z	V § 29 požadujeme doplnit povinnou součinnost a stanovisko oborového regulátora, pokud se jedná o strategicky významnou službu z oblasti, která podléhá regulaci (ERÚ, ČTÚ).	Neakceptováno – nyní § 30 Dle návrhu zákona NÚKIB v rámci procesu získávání informací spolupracuje s relevantními orgány státu, v případě jednotlivých sektorů pak zákon v podobě, v jaké je dnes, tuto spolupráci předpokládá s regulátory jednotlivých sektorů (např. telekomunikace a energetika), je-li to v případě daného sektoru možné. Toto je zaručeno mimo jiné § 8 odst. 2 zákona č. 500/2004 Sb., správního řádu. Dále je tento postup dán principem dobré správy, kdy NÚKIB pro co nejlepší vyhodnocení situace a možných dopadů počítá s dožádáním informací od relevantních orgánů státu v rámci jednotlivých odvětví. Důvodem, proč tyto orgány nejsou uvedeny přímo v zákoně je ten, že zákon ve svém ustanovení § 29 počítá se součinností těch orgánů, které jsou relevantní napříč všemi sektory. Tyto orgány pak budou mít dle § 30 odst. 2 možnost projednání návrhu opatření obecné povahy, kde bude žádoucí získat pohled relevantních sektorových regulátorů na dopady případného omezení či zákazu. Reakce připomínkového místa Na připomínkách uplatněných v rámci MPŘ trváme a s návrhem vypořádání ze strany předkladatele materiálu nesouhlasíme. Po schůzce Ustanovení § 31 bylo upraveno a připomínka byla vypořádána. Připomínkové místo s vypořádáním souhlasí.
616. Ministerstvo financí	Z	Návrh zákona má v § 29 odst. 2 ambici prolomit mlčenlivost zaměstnanců Finančního analytického úřadu a dát jim povinnost	Akceptováno jinak - nyní § 30

	součinnosti. V souvislosti s povinností součinnosti pak je zřejmě tato norma v rozporu se směrnicí Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES, zejména s čl. 32 odst. 3. V § 29 odst. 2 se navrhuje vypustit slova „Finanční analytický úřad“ a zakotvit v novém odst. 3, že FAÚ poskytuje jen ty informace, kterými již disponuje. Proto k §29 MF (FAÚ) navrhuje vložit nový odstavec (3) „(3) Finanční analytický úřad za účelem výkonu činnosti podle § 28 odst. 1 poskytne Úřadu na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů informace, které získal při své činnosti podle zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.“ Vysvětlení: Prolomení mlčenlivosti vůči NÚKIB musí být promítnuto do § 39 odst. 1 písm. r) zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, aby nedocházelo k nepřímé novele tohoto zákona. Zákon č. 253/2008 Sb. § 39 odst. (1) písmeno r) Národnímu úřadu pro kybernetickou a informační bezpečnost při shromažďování a vyhodnocování informací a dat spojených s orgánem či osobou, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovitosti dodavatele. V § 29 MF (FAÚ) následně navrhuje za vložený odstavec (3) přechýšlovat původní odstavec (3) na odstavec (4) a odstavec (4) na odstavec (5).	První část připomínky je akceptována zcela, druhá část byla akceptována v jiné podobě, neboť na základě jiné připomínky došlo k úpravě znění § 30, a to takto: (1) Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí a Ministerstvo vnitra za účelem výkonu činnosti podle § 28 odst. 1 poskytnou Úřadu na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů ode dne obdržení žádosti, stanovisko o naplnění kritéria rizikovitosti dodavatele konkrétním orgánem či osobou nebo požadované informace. (2) Nejvyšší státní zastupitelství, Policie České republiky, Úřad pro ochranu hospodářské soutěže a zpravodajské služby České republiky za účelem výkonu činnosti podle § 28 odst. 1 poskytnou Úřadu na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů ode dne obdržení žádosti, požadované informace. (3) Finanční analytický úřad za účelem výkonu činnosti podle § 28 odst. 1 poskytne Úřadu na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů ode dne obdržení žádosti, požadované informace, které získal při své činnosti podle zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. (4) Nezíská-li Úřad z vlastní činnosti nebo postupem podle odstavce 1 a 2 informace potřebné pro výkon činnosti podle § 28 odst. 1, poskytnou na základě žádosti Úřadu tyto informace orgány a osoby neuvedené v odstavci 1 a 2 a to do 30 dnů ode dne obdržení žádosti.

		(5) Při poskytování informací podle tohoto ustanovení není porušením povinnosti mlčenlivosti poskytnutí informace a) orgánem činným v trestním řízení, ledaže by poskytnutí informace, na kterou se mlčenlivost vztahuje, zmařilo účel trestního řízení, b) Finančně analytickým úřadem, c) správcem daně podle daňového řádu, d) orgánem Celní správy České republiky. (6) Při poskytování informací podle tohoto ustanovení není porušením bankovního tajemství poskytnutí informace bankou. Zároveň s úpravou § 30 budou také upraveny související zvláštní zákony (včetně změny zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu) v doprovodném zákoně. Rozpor Souhlasíme s vypořádáním první části připomínky (tj. aby FAÚ poskytoval jen požadované informace, které získal při své činnosti podle zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu). S vypořádáním druhé části připomínky však nesouhlasíme, a to z níže uvedených důvodů. Ve vztahu k nově upravenému § 30 odst. 5 písm. b) požadujeme reflektovat korektiv výjimek z povinnosti mlčenlivosti FAÚ podle § 39 odst. 4 zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (dále

		jen „AML zákon“). V tomto směru připadají v úvahu dva přístupy. První přístup (který jsme navrhovali v připomínce) spočívá ve vypuštění písmene b) a řešení otázky průlomu do mlčenlivosti Finančního analytického úřadu pro NÚKIB výlučně v doprovodném změnovém zákonu, kterým by byl NÚKIB doplněn do § 38 odst. 1) písm. a) AML zákona, protože by se i na tento průlom uplatnil korektiv uvedený v § 39 odst. 4 AML zákona. Tuto cestu bychom preferovali. Alternativně by bylo možné tento korektiv zreplikovat v § 30 odst. 5 písm. b). Pak bychom navrhovali následující znění: „5) Při poskytování informací podle tohoto ustanovení není porušením povinnosti mlčenlivosti poskytnutí informace a) orgánem činným v trestním řízení, ledaže by poskytnutí informace, na kterou se mlčenlivost vztahuje, zmařilo účel trestního řízení, b) Finančně analytickým úřadem za podmínky, že výjimka z povinnosti mlčenlivosti 1. se uplatní jen v nezbytně nutném rozsahu podle účelu poskytované informace, a to zejména s ohledem na ochranu informací o oznamovatelích podezřelých obchodů podle právního předpisu upravujícího opatření proti legalizaci výnosů z trestné činnosti a financování terorismu, 2. nelze uplatnit, pokud by poskytnutí informací mohlo zmařit nebo ohrozit šetření podezřelého obchodu nebo probíhající trestní řízení, nebo jestliže by poskytnutí informací bylo zjevně nepřiměřené oprávněným zájmům osoby,

			jíž se informace týká, nebo účelu, pro který byla žádost podána, c) správcem daně podle daňového řádu, d) orgánem Celní správy České republiky.“ Pokud by tato otázka nebyla řešena, pak by mohly vyvstávat pochybnosti o souladu s 5. AML směrnicí. Rovněž by byl NÚKIB jediným orgánem, vůči kterému je mlčenlivost prolomena, aniž by se na to vztáhl korektiv § 39 odst. 4 AML zákona. Konečně by ve výjimečných případech hrozilo narušení činnosti FAÚ. To lze ilustrovat na příkladu kolize s § 30 odst. 5 písm. a), kde byl ve vztahu k orgánu činnému v trestní řízení doplněn korektiv „ledaže by poskytnutí informace, na kterou se mlčenlivost vztahuje, zmařilo účel trestního řízení,“. Ačkoli by tedy informace citlivá pro trestní řízení byla u OČTŘ chráněna, mohla by být vydána skrz FAÚ. Zde je třeba mít na paměti, že rozhodující část z výstupů FAÚ je adresována ÚČTŘ (a proto také korektiv v § 39 odst. 4 AML zákona zmiňuje ohrožení probíhajícího trestního řízení). Vypořádáno Zpracováno a vyřešeno.
617. Ministerstvo financí	Z	V rámci odstavců 3 a 4 se § 29 dotýká problematiky oznamovací povinnosti, resp. infomační povinnosti orgánů veřejné moci vůči Úřadu. V této souvislosti je navrhováno stanovit, že „Poskytnutí informací podle tohoto ustanovení není porušením mlčenlivosti podle jiného právního předpisu.“. Ministerstvo financí považuje za nutné v této souvislosti upozornit na skutečnost, že popsany způsob prolomení zákonné povinnosti mlčenlivosti jiného orgánu veřejné moci nedopadá na tzv. speciální povinnosti mlčenlivosti, které standardně	Akceptováno Dotčené ustanovení bylo přepracováno, obdobně jako u sankčního zákona je prolomení mlčenlivosti v současné době koncipováno tak, že v § 30 odst. 5 jsou vyjmenovány orgány, ve vztahu k nimž se mlčenlivost výslovně prolamuje (orgány činné v trestním řízení, Finanční analytický úřad, správce daně, orgány Celní správy České republiky). V případě potřeby získání

	není možné prolomit obecným stanovením oznamovací či informační povinnosti, popřípadě obecným (paušálním) prolamovacím ustanovením, ale které vyžadují výslovné, resp. adresné prolomení, které je zacílené právě na danou jednotlivě určenou povinnost mlčenlivosti (ve vztahu k paušálně pojatému průlomu si úprava uvedených povinností mlčenlivosti totiž nadále podrží svůj status lex specialis). Uvedená paušální ustanovení § 29 odst. 4 zákona o kybernetické bezpečnosti proto nedopadají zejména na tzv. daňovou mlčenlivost podle § 52 a násl. zákona č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů (dále jen „daňový řád“), mlčenlivost podle zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů (dále jen „AML zákon“), a mlčenlivost podle zákona č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů (dále jen „zákon o provádění mezinárodních sankcí“). Podobně neprolamuje uvedené paušální ustanovení například povinnost mlčenlivosti příslušníků zpravodajských služeb či notářů (jednajících jako orgány veřejné moci). Do jisté míry zůstává otázkou, zda je skutečně cílem zákona o kybernetické bezpečnosti aby došlo uvedeným paušálním způsobem k prolomení speciálních povinností mlčenlivosti (z celkového kontextu včetně znění důvodové zprávy lze usuzovat, že ano a to i s ohledem na speciální úpravu mlčenlivosti advokáta podle právního předpisu upravujícího výkon advokacie), avšak navržený paušální způsob není způsobilý tohoto cíle dosáhnout, neboť nereflektuje stávající stav právního řádu, kdy průlomy speciálních povinností mlčenlivosti jsou realizovány adresnými speciálními normami (v některých případech i doplněním tzv. „zrcadlového“ ustanovení do předpisu, který danou povinnost mlčenlivosti konstituuje, byť takový krok nelze považovat za nezbytný). Z důvodové zprávy je tedy nutno vyškrtnout nepravdivou informaci, že poskytnutí informací pro účely prověřování rizik	jiných informací krytých povinností mlčenlivosti bude přistoupeno k podání žádosti o zproštění povinnosti mlčenlivosti. Dále byl doplněn § 30 odst. 6, který od prolomení povinnosti mlčenlivosti odlišuje prolomení bankovního tajemství. Změny týkající se § 30 odst. 5 a 6 byly zrcadlově promítnuty do doprovodného zákona v podobě změn zákonů upravujících činnost orgánů označených v § 30 odst. 5 a 6. Reakce připomínkového místa - Rozpor Navrhovaným způsobem vypořádání bylo vyhověno požadavku výslovného legislativního prolomení povinnosti daňové mlčenlivosti. Na jednání dne 16. srpna 2023 bylo nicméně shodnuto, že v případě poskytování informací potřebných pro výkon činnosti Úřadu, budou tyto informace poskytovány pouze ze strany orgánů Finanční a Celní správy ČR, a to obdobně jako je tomu podle § 65 odst. 4 návrhu tohoto zákona. Tyto informace by tedy byly na žádost poskytnuty Generálním finančním ředitelstvím nebo Generálním ředitelstvím cel s tím, že Generální finanční ředitelství nebo Generální ředitelství cel žádosti vyhoví, ledaže by poskytnutím informací mohlo dojít k narušení řádného výkonu správy daní. Po schůzce Materiál upraven a připomínka vypořádána.

		spojených s dodavatelem se proto podle odstavce 4 nepovažuje za porušení zákonem stanovené či uznané povinnosti mlčenlivosti například podle § 52 daňového řádu nebo § 16 zákona o provádění mezinárodních sankcí. Na tomto místě je třeba rovněž uvést, že právě otázka případného prolomení daňové mlčenlivosti v případech oznamovací, resp. infomační povinnosti podle zákona o kybernetické bezpečnosti byla již v minulosti řešena. Ministerstvo financí již tehdy jasně deklarovalo, že se paušálními průlomy do mlčenlivosti orgánů veřejné moci v zákoně o kybernetické bezpečnosti necítí být ve vztahu k daňové mlčenlivosti vázáno. Tehdejší rozsah oznamovací, resp. infomační povinnosti, kvůli kterému byl případný průlom do daňové mlčenlivosti diskutován, současně považovalo Ministerstvo financí za nepřiměřeně široký a neodpovídající požadavku, aby průlom do daňového tajemství představoval proporcionální nástroj ultima ratio a byl zaváděn pouze tam, kde společenský zájem na poskytnutí informací zásadně převažuje nad společenským zájmem na řádném výkonu správy daní a ochraně práva na infomační sebeurčení daňových subjektů. Následná diskuze pak vedla ke konkrétnímu závěru, kterým byla legislativní úprava navržena v § 63 tohoto zákona. Pokud jde o výše uvedené paušální prolomení povinnosti mlčenlivosti orgánů veřejné moci, je třeba rovněž podtrhnout, že se nejedná pouze o problém systematický či o otázku jednoty a bezrozpornosti právního řádu, ale především též o principiální otázku legislativně-věcnou. Jak bylo uvedeno výše, speciální povinnosti mlčenlivosti je možné prolomit pouze na základě provedení testu proporcionality a na základě zvážení protichůdných společenských zájmů, které se v daném případě střetávají. Tento test nelze per definitionem provést paušálně, neboť každá speciální povinnost mlčenlivosti slouží ochraně odlišných informací a odlišných subjektů. Právě proto je v těchto případech nezbytné provést adresné posouzení a následně také adresné legislativní prolomení dané povinnosti	

		mlčenlivosti, pokud to bude shledáno nezbytným. Paušální průlom takový postup neumožňuje, a to mimo jiné i proto, že se fakticky týká též případných budoucích speciálních povinností mlčenlivosti, které v době přijetí takového paušálního průlomu ani nejsou známy. Ministerstvo financí proto zcela zásadně nesouhlasí s tím, aby se v právním řádu vyskytovala ustanovení, která usilují o paušální průlom všech speciálních povinností mlčenlivosti a obcházela tak nutnost adresného posouzení odůvodněnosti takového prolomení (resp. vytvářela v tomto smyslu nedůvodná zdání, že je takový paušální průlom možný). Z hlediska prolomení mlčenlivosti Finančního analytického úřadu se za účelem funkčnosti navržené právní úpravy navrhuje upravit § 16 zákona o mezinárodních sankcích, případně § 39 AML zákona, podle rozsahu informací, které bude NÚKIB vyžadovat.	
618. Ministerstvo financí	Z	Obecně k tématu bezdlužnosti, kde se MF se dlouhodobě snaží o sjednocení formulace úpravy bezdlužnosti ve všech právních předpisech napříč právním řádem. Ve vazbě na uvedenou snahu MF nyní předloženém návrhu zákona o kybernetické bezpečnosti MF navrhuje upravit podmínku bezdlužnosti tak, aby její formulace reflektovala úpravu týkající se bezdlužnosti používanou napříč právním řádem a zároveň respektovala terminologii zákona č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů (dále jen „daňový řád“). Je přitom především na věcném garantu příslušného právního předpisu, jestli bude požadovat, aby určitá osoba byla daňově (v širším smyslu slova) bezdlužná. V tomto směru jsme tedy k požadavku NÚKIB neutrální, neboť je věcí tohoto úřadu, jestli uzná za vhodné, aby předmětné osoby byly bezdlužné a v jakém rozsahu.	Akceptováno Požadavek na sjednocení formulace úpravy bezdlužnosti v návrhu zákona zohledněn a upraven v souladu s požadavkem připomínkového místa. Připomínkové místo s vypořádáním souhlasí.
619. Ministerstvo financí	Z	V §30 odst. 1 - v souvislosti s poskytováním regulovaných služeb a strategicky významné služby a proběhlým útokům na nemocnice v ČR navrhuje MF rozšířit rozsah chráněných hodnot o oblast	Neakceptováno - nyní § 31

		zdravotnictví. MF navrhuje doplnit text „(1) Úřad vydá opatření... možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku a <i>zdraví</i>.“	NÚKIB si plně uvědomuje důležitost poskytovatelů zdravotních služeb, a proto je odvětví zdravotnictví zařazeno mezi regulované služby podle vyhlášky o regulovaných službách. NÚKIB důkladně zvažoval, zda by toto odvětví nemělo být zařazeno i do mechanismu prověřování bezpečnosti dodavatelského řetězce. Neučinil tak zejména proto, že nemocnice nejsou síťovým odvětvím. V případě výpadku jedné nemocnice, nedojde k výpadku celé služby na území, které by bylo signifikantní z důvodu jejich zastupitelnosti jinými. Také je ověřeno, že výpadek nemocnice nezpůsobí krizový stav. Závěr Po schůzce vypořádáno.
620. Ministerstvo financí	Z	Celá HLAVA III - V případě technologických domén řízených např. Active Directory např. s názvy Úřad, Firma, apod. může dojít k duplicitám. Předmětem ochrany v hlavě III jsou internetové domény, jejich vlastní názvy a jejich majitelé i registrátoři. V textu v §36 je pojem „internetová doména“ použit, a proto MF navrhuje, aby v celé Hlavě III bylo terminologicky sjednoceno pojmosloví „internetová doména“.	Neakceptováno S ohledem na znění NIS2, kde je v čl. 6 odst. 21 uvedena definice "registru domén nejvyšší úrovně", Úřad přistoupil k odstranění nadbytečného výrazu "internetová" od jména domény a sjednocení dotčeného textu. Slovní spojení "internetová doména" se nejeví jako vhodné vzhledem k tomu, že obdobné termíny silně redukuje to, co internet ve skutečnosti je. Internet není jen webová služba a webové stránky, ale i další služby, například e-mail, FTP, streaming, DNS atd. Předmětem ochrany je jméno domény - držitel jména domény fakticky vlastní jméno, nikoliv doménu. Ve vztahu k subjektům poskytujícím služby registrace jmen domén se pak pojem "jméno domény" jeví jako jednoznačný, proto bylo znění zákona příslušně upraveno. Připomínkové místo s vypořádáním souhlasí.

621. Ministerstvo financí	Z	V §40 odst. 1, písm. d) - Opatření k řešení stavu kybernetického nebezpečí Konflikt mezi Návrhem zákona a další legislativou, zejména Zákoníkem práce, Zákonem o státní službě a Zákonem o služebním poměru příslušníků bezpečnostních sborů. Z textu plyne oprávnění ředitele Úřadu, že v době stavu kybernetického nebezpečí za účelem jeho řešení je oprávněn d) nařídít práci v pohotovostním režimu. Tuto pravomoc může ředitel Úřadu uplatnit jen v rámci řízení Úřadu, nikoli na povinné osoby tzn., že zde dochází k překročení kompetencí ředitele Úřadu dané zákonem, protože zaměstnanci může nařídít práci v pohotovostním režimu jen jeho nadřízený. Z tohoto důvodu MF navrhuje, aby byl mechanismus nastaven na povinnou osobu dle zákona, a ta v rámci svých pravomocí může nařídít práci nejen v pohotovostním režimu, ale i přesčas.	Akceptováno jinak - nyní § 41 Ustanovení návrhu bylo upraveno a zpřesněno v návaznosti na konzultaci s gestorem krizového řízení Ministerstvem vnitra - GRHZS. Připomínkové místo s vypořádáním souhlasí.
622. Ministerstvo financí	Z	V §40 odst. 1, písm. e) - Opatření k řešení stavu kybernetického nebezpečí Konflikt mezi Návrhem zákona a povinnostmi povinných osob, zejména však Poskytovatelů strategicky významných služeb. Jen Poskytovatelé strategicky významných služeb umí zhodnotit důsledky a dopady zákazu používání technických aktiv, které zajišťují strategické významné služby. Z tohoto důvodu MF navrhuje, aby byl mechanismus nastaven na povinnou osobu dle zákona, a ta v rámci svých pravomocí zhodnotí dopady a minimalizaci následků tohoto zákazu používání technických aktiv.	Neakceptováno - nyní § 41 Zákaz podle tohoto ustanovení je dán pouze orgánům a osobám, které jsou k tomu Úřadem vyzvány. Není tedy bez dalšího koncipován jako celoplošný nástroj, právě za tím účelem, aby nebylo zasaženo do fungování těch nejvýznamnějších služeb bez předchozího zhodnocení dopadů. Připomínkové místo s vypořádáním souhlasí.
623. Ministerstvo financí	Z	V §41 Národní úřad pro kybernetickou a informační bezpečnost v odst. 3, v odst. 4 a v odst. 5 v rámci zajištění celorepublikové kybernetické bezpečnosti Úřad ani Vládní CERT, který je součástí Úřadu nemají v tomto zákoně povinnosti sdílení informací při řešení jednotlivých kybernetických bezpečnostních incidentů nebo při stavu kybernetického nebezpečí s příslušnými orgány Policie ČR, ZSI či Vojenského zpravodajství. To by mělo zajistit koordinované činnosti	Vysvětleno - nyní § 44 Sdílení informací se řídí obecnou zásadou spolupráce podle § 8 odst. 2 zákona č. 500/2004 Sb., správního řádu, přičemž v případě zjištění skutečností nasvědčujících tomu, že byl spáchán trestný čin, bude postupováno dle § 8 odst. 1 zákona č. 141/1961 Sb., trestního řádu. Vládní CERT také podle § 44 odst. 5

		a zlepšení úrovně zajištění kybernetické bezpečnosti v ČR. MF navrhuje doplnit povinnost sdílení informací přímo do zákona.	písm. f) návrhu zákona o kybernetické bezpečnosti spolupracuje s orgány a osobami působícími v oblasti kybernetické bezpečnosti. Úřad dále podle § 48 odst. 2 návrhu zákona o kybernetické bezpečnosti poskytuje v odůvodněných případech údaje z evidencí orgánům veřejné moci na jejich žádost, je-li to nezbytné pro výkon jejich působnosti. Spolupráce s Vojenským zpravodajstvím je upravena v § 16b zákona č. 289/2005 Sb., o Vojenském zpravodajství, přičemž zpravodajské služby mezi sebou spolupracují na základě § 9 zákona č. 153/1994 Sb., o zpravodajských službách České republiky. Praxe vyplývající z aktuálního zákona o kybernetické bezpečnosti není nijak ovlivněna. Připomínkové místo s vypořádáním souhlasí.
624. Ministerstvo financí	Z	V § 42 odst. 1 písm. e) - V uvedeném ustanovení je normována tzv. bezdlužnost takto: „(1) Provozovatelem Národního CERT může být pouze právnická osoba, která e) nemá v České republice v evidenci daní zachycen splatný daňový nedoplatek a nemá v České republice splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění a na pojistném nebo na penále na sociální zabezpečení nebo příspěvku na státní politiku zaměstnanosti“, Požadujeme, aby byla v návrhu zákona respektována terminologie souladná s daňovým řádem, zejména v případě, má-li určitý subjekt nedoplatek (nikoli „splatný“ nedoplatek) podle § 153 daňového řádu. Slovní spojení „splatný daňový nedoplatek“ není věcně správné, jelikož podle § 153 daňového řádu je „nedoplatek částka daně, u které uplynul již den splatnosti“ a která nebyla uhrazena. Požadavek bezdlužnosti je standardně omezován na nedoplatky evidované orgány Finanční a Celní správy České republiky spolu s paralelním požadavkem absence nedoplatku na veřejných pojistných. Z navrženého ustanovení však není jisté, zda není úmyslem předkladatele podchytit také veškeré	Akceptováno - nyní § 45 Dotčené ustanovení bylo změněno požadovaným způsobem: „Provozovatelem Národního CERT může být pouze právnická osoba, která nemá v České republice evidován nedoplatek, s výjimkou nedoplatku, u kterého je povoleno posečkání jeho úhrady nebo rozložení jeho úhrady na splátky, 1. u orgánů Finanční správy České republiky 2. u orgánů Celní správy České republiky 3. na pojistném a na penále na veřejné zdravotní pojištění a 4. na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti.“ Připomínkové místo s vypořádáním souhlasí.

		nedoplatky na daních v procesním smyslu (viz použitá formulace týkající se pouze nedoplatků „v evidenci daní“). To úzce souvisí se skutečností, že v takto navrženém ustanovení by absentovalo určení, u kterého orgánu jsou dané nedoplatky evidovány – není tedy jasné, jakým způsobem by byla např. prověřována absence nedoplatků na místních poplatcích u všech obcí v České republice, kterých je cca 6000. Z navrženého ustanovení toto není patrné a žadatel by tak nebyl fakticky schopen prokázat všechny požadavky na doložení bezdlužnosti. V tomto ohledu je tento požadavek nesprávný i s ohledem na to, že potvrzení o bezdlužnosti, je podle navrženého § 42 odst. 2 písm. b) požadováno pouze od orgánů Finanční správy České republiky a Celní správy České republiky, které ve svých evidencích nevedou všechny daňové nedoplatky. Požadavek bezdlužnosti se tak nepřekrývá s požadavkem tuto bezdlužnost doložit. Jakkoliv tedy platí, že i když věcné parametry podmínky bezdlužnosti jsou na rozhodnutí gestora příslušné úpravy, legislativní formulace by měla být v rámci právního řádu pokud možno vždy pojata jednotně a neměla by být vnitřně rozporná, resp. klást fakticky nesplnitelné požadavky. Navrhuje se proto využít např. následující textaci, která je standardně napříč právním řádem využívána v souvislosti se statutem bezdlužnost určitého subjektu: „e) nemá evidován nedoplatek (s výjimkou nedoplatku, u kterého je povoleno posečkání jeho úhrady nebo rozložení jeho úhrady na splátky), 1. u orgánů Finanční správy České republiky, 2. u orgánů Celní správy České republiky, 3. na pojistném a na penále na veřejné zdravotní pojištění, a 4. na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti.“. Je třeba poznamenat, že nedoplatky evidované u orgánů Finanční a Celní správy České republiky zahrnují veškeré nedoplatky na peněžitých plněních, která tyto orgány spravují v daňovém procesním režimu. Kromě peněžitých plnění označených jako daně, poplatky či cla se jedná např. i o odvody za porušení	

		rozpočtové kázně či pokuty a jiná peněžitá plnění, jejichž placení je zajišťováno orgány Celní správy České republiky v režimu tzv. dělené správy.	
625. Ministerstvo financí	Z	V ustanovení § 42 odst. 2 písm. b) je stanoveno: „(2) Zájemce prokazuje splnění podmínek předložením b) potvrzení příslušných orgánů Finanční správy České republiky, Celní správy České republiky, České správy sociálního zabezpečení a příslušné pojišťovny v případě odstavce 1 písm. e), která nesmí být starší než 30 dnů“. Samostatnou otázkou je, zda je potřeba ukládat žadateli povinnost daňovou bezdlužnost u finančního nebo celního úřadu prokazovat za situace, kdy si takový zákonný požadavek může orgán veřejné moci ověřit přímo u příslušného finančního nebo celního úřadu na základě prolomení daňové mlčenlivosti podle § 53 odst. 1 písm. l) daňového řádu (a nepotřebuje tedy v této věci zproštění mlčenlivosti či přímo dodání potvrzení žadatelem). Tento obecný průlom do daňové mlčenlivosti tak odstraňuje formální bariéru pro sdělení údajů ve vztahu k bezdlužnosti daňového subjektu mezi orgány veřejné moci při zachování autonomie vůle daňového subjektu, nicméně pouze v případě, že zvláštní úprava rigidně nepožaduje prokázání bezdlužnosti výlučně po daňovém subjektu. Tento postup je však s ohledem na výše uvedené nedůvodný a pro daňový subjekt zatěžující, a to přinejmenším v případě potvrzení bezdlužnosti týkající se nedoplatek u Finanční a Celní správy České republiky. Tento postup je také nedůvodný za situace, kdy jej lze zajistit postupem, který nebude v takové míře zatěžovat i orgány veřejné moci (tj. zejména elektronicky). Současně se tento postup uplatní i při kontrole, zda je průběžně plněna povinnost, aby podmínka bezdlužnosti (resp. další podmínky) byly splňovány po celou dobu, kdy má dotčený subjekt status provozovatele Národního CERT. MF doporučuje nastavit mechanismus tohoto ověřování cestou přímého ověřování u finančního nebo celního úřadu, popřípadě nastavením	Akceptováno Připomínkové místo s vypořádáním souhlasí.

		periodicity prokazování bezdlužnosti ze strany daného subjektu v ostatních případech, kde uvedené ověření přímo u správce daně není možné, a to s ohledem na to, že plnění podmínky bezdlužnosti je požadováno kontinuálně.	
626. Ministerstvo financí	Z	V ustanovení § 48 odst. 1 písm. d) až f), je normována tzv. bezdlužnost takto: „(1) Žadatel má základní způsobilost, pokud „d) nemá v České republice v evidenci daní zachycen splatný daňový nedoplatek, e) nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění, f) nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti“. Ve zdůvodnění nesouhlasu s návrhem textu daného ustanovení odkazujeme na zdůvodnění k § 42 odst. 1 písm. e). Nad rámec výše uvedeného je pak nutno doplnit, že není zřejmé, proč jsou sledovány nedoplatky na pojistném nebo na penále na veřejné zdravotní pojištění a na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti v zemi sídla žadatele, a nejsou sledovány nedoplatky na dani, poplatek nebo jiném peněžitém plnění. V této souvislosti je pak nutno upozornit na skutečnost, že uvedená peněžitá plnění by v souvislosti se zahraničním neměla být vymezena takto výslovně, ale mělo by být uvedeno, že sledovány budou nedoplatky na peněžitých plněních, která jsou těmto peněžitým plněním obdobná (s ohledem na možnou odlišnou zahraniční terminologii).	Akceptováno - nyní § 51 § 51 odst. 1 písm. d) až f) upraven následovně, nově pod odst. 1 písm. d) dotčeného §: " d) nemá v České republice evidován nedoplatek, s výjimkou nedoplatku, u kterého je povoleno posečkání jeho úhrady nebo rozložení jeho úhrady na splátky, 1. u orgánů Finanční správy České republiky 2. u orgánů Celní správy České republiky 3. na pojistném a na penále na veřejné zdravotní pojištění a 4. na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti," Připomínkové místo s vypořádáním souhlasí.
627. Ministerstvo financí	Z	V ustanovení § 48 odst. 2 písm. b) až e) takto: „(2) Žadatel prokazuje splnění podmínek základní způsobilosti podle odstavce 1 předložením „b) potvrzení příslušného finančního úřadu ve vztahu k odstavci 1 písm. d), které nesmí být starší než 30 kalendářních dnů přede dnem podání žádosti, c) písemného čestného prohlášení ve vztahu ke spotřební dani ve vztahu k odstavci 1 písm. d), d) písemného čestného prohlášení ve vztahu k odstavci 1 písm. e) a e) potvrzení příslušné	Akceptováno V návaznosti na úpravu bezdlužnosti došlo i k úpravě jejího prokazování a to následovně v § 51 odst. 3 písm. a): " předložením potvrzení příslušné pojišťovny v případě odstavce 1 písm. d) bod 3 a příslušné okresní

		okresní správy sociálního zabezpečení ve vztahu k odstavci 1 písm. f), které nesmí být starší než 30 kalendářních dnů přede dnem podání žádosti.“ Ve zdůvodnění nesouhlasu s návrhem textu daného ustanovení odkazujeme na zdůvodnění k § 42 odst. 2 písm. b). Nad rámec výše uvedeného je pak nutno doplnit následující. Navržené ustanovení řeší doložení nedoplatků evidovaných finančním úřadem, resp. nedoplatků na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti (formou potvrzení) a nedoplatků na spotřební dani a na veřejném zdravotním pojištění (formou čestného prohlášení). Není zde ovšem jasné, proč je s informacemi od Finanční a Celní správy České republiky, resp. na různých pojistných nakládáno odlišně (a proč je z nedoplatků evidovaných orgány Celní správy České republiky řešena jen oblast spotřebních daní). Vzhledem k výše uvedenému se tato ustanovení navíc zdaleka nepřekrývají s požadavkem bezdlužnosti, jak je formulován v prvním odstavci dotčených paragrafů návrhu, neboť bezdlužnost ohledně řady testovaných nedoplatků by nebyla doložena dokonce ani pouhým čestným prohlášením (viz např. zúžení nedoplatků v působnosti orgánů Celní správy České republiky pouze na spotřební daně). Nástroj v podobě čestného prohlášení je navíc obecně nepříliš šťastný, neboť doložení neexistence nedoplatku ve formě čestného prohlášení téměř není možné ověřit (byť z čistě formálního hlediska lze takové řešení akceptovat), tj. tento nástroj by měl být využíván pouze tam, kde nelze zvolit jiné řešení (typicky u zahraničních nedoplatků).	správy sociálního zabezpečení v případě odstavce 1 písm. d) bod 4, která nesmí být starší než 30 dnů,”, Připomínkové místo s vypořádáním souhlasí.
628. Ministerstvo financí	Z	V § 46 Autorizace subjektů posuzování shody podle aktu o kybernetické bezpečnosti. Není v zákoně popsán proces, kdy subjekt ztratí autorizaci shody podle aktu o kybernetické bezpečnosti a Úřad mu tuto autorizaci odejme. Neexistuje popis mechanismus, po jak dlouhé době může subjekt žádat o novou autorizaci posuzování shody	Neakceptováno - nyní § 49 Toto ustanovení nebylo do zákona zahrnuto, protože procesy vycházejí z evropské právní úpravy, resp. náležitosti k procesu autorizace by měly být upraveny v jednotlivých certifikačních schématech, resp. v prováděcích aktech. Toto připomínkové ustanovení

		podle aktu o kybernetické bezpečnosti. MF navrhuje doplnit příslušný § o možnost znovu získání autorizace.	vychází navíc z již přijatého ustanovení v současném zákoně o kybernetické bezpečnosti. Při jeho přípravě byl proces analogicky upraven i s ohledem na § 11 zákona č. 22/1997Sb., kde je upravena autorizace prováděná ÚNMZ a kde taktéž neupravují délku platnosti autorizace. Připomínkové místo s vypořádáním souhlasí.
629. Ministerstvo financí	Z	V §48 není zřejmé, jaký druh osob může žádat o registraci členství v Komunitě. V zákoně chybí rozlišení mezi FO podnikající a FO. MF navrhuje doplnit příslušný § o FO podnikající a nastavení věkové hranice minimálně na 21 let.	Vysvětleno - nyní § 51 Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center, nerozlišuje, zda se jedná o OSVČ nebo PO, pouze podmiňuje členství v Komunitě tím, že subjekt musí být usazen v členském státu, v našem případě v ČR a musí mít požadované know-how příslušné oblasti podle čl. 8 odst. 3. Jelikož základní podmínky pro vznik členství stanovuje přímo aplikovatelné nařízení, není tyto možné měnit, ani jinak regulovat věkovou hranici pro OSVČ. Nařízení umožňuje sice členskému státu formulovat své "bezpečnostní důvody", věková hranice OSVČ však pod ně nespadá. Znění § 51 OSVČ nevylučuje, neboť stanoví, že člen Komunity může být mimo jiné ten, kdo má sídlo v České republice, to naopak jednoznačně zahrnuje jak OSVČ tak PO. Připomínkové místo s vypořádáním souhlasí.
630. Ministerstvo financí	Z	V § 48 odst. 2 navrhujeme písmeno c) formulovat takto: Žadatel prokazuje splnění podmínek základní způsobilosti podle odstavce 1 předložením „c) potvrzení příslušného celního úřadu ve vztahu k odstavci 1 písm. d), které nesmí být starší než 30 kalendářních dnů přede dnem podání žádosti.“. Tato připomínka je zásadní.	Akceptováno jinak - nyní § 51 S ohledem na úpravu bezdlužnosti (viz vypořádání připomínek 3.18 a 3.19) bude Úřad jako správní orgán, žádat potvrzení k prokázání daňové bezdlužnosti

	Odůvodnění: Předložený návrh zákona stanovuje podmínky, které by měly být plněny žadatelem o registraci v Komunitě. Pokud žadatel podmínky nesplní, nebude mu umožněno členství v Komunitě. Splnění podmínek má být v daňové oblasti prokazováno potvrzením od finančního úřadu a dále čestným prohlášením ve vztahu ke spotřební dani. Koncept, kdy by byla neexistence splatných daňových nedoplatků prokazována čestným prohlášením, považujeme obecně za nežádoucí (viz i konstrukce v § 42 odst. 2 písm. b) návrhu zákona, kdy splnění podmínek je prokazováno potvrzením). Za prvé by mělo platit, že nedoplatky evidované u orgánů Finanční správy a Celní správy se prokazují stejným způsobem, není-li dán racionální důvod pro odlišný postup. Za druhé v čestném prohlášení žadatel může, ať již vědomě či z nedbalosti, uvést nesprávně, resp. v rozporu se skutečností, že nemá nedoplatek na spotřební dani či příslušenství. Za třetí není namístě omezit prokazování splnění podmínek pouze ve vztahu ke spotřebním daním, neboť orgány Celní správy spravují v režimu daňového řádu více veřejnoprávních pohledávek. Má-li být zákonnou podmínkou základní způsobilosti žadatele o registraci členství v Komunitě to, že žadatel nemá v České republice v evidenci daní zachycen splatný daňový nedoplatek, pak by splnění této podmínky mělo být systematicky taky ověřováno, resp. potvrzení neexistence daňových nedoplatků by ve vztahu k Celní správě nemělo být navázáno jen na spotřební daně. Lze uvést, že v režimu daňového řádu v rámci dělené správy jsou vymáhány např. i pokuty, které jsou uloženy dozorovým orgánem v případě spáchání přestupku podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů; tj. i tyto pokuty jsou evidovány v evidenci daní jako splatný daňový nedoplatek. Pro úplnost uvádíme, že námi navrhované znění je již obsaženo např. v zákoně o kybernetické bezpečnosti (§ 18 odst. 3 písm. b) a odst. 4), zákoně o spotřebních	podle odst. 51 písm. d) bod 1 a 2. od příslušného orgánu Finanční a Celní správy České republiky na základě prolomení daňové mlčenlivosti podle § 53 odst. 1 písm. l) zákona č. 280/2009 Sb., daňový řád ve znění pozdějších předpisů. Připomínkové místo s vypořádáním souhlasí.

		daních (§ 43f odst. 2) nebo zákoně o pohonných hmotách a čerpacích stanicích pohonných hmot (§ 6h odst. 3).	
631. Ministerstvo financí	Z	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: - § 2 písm. k) – stanovení kritérií, pravidel a postupů pro definici významné změny by mělo být pevně určeno a navázáno na stupnici pro hodnocení rizik uvedené v příloze č. 2, tabulce č. 3 navrhované vyhlášky.	Neakceptováno Významné změny lze určovat více různými způsoby, což ukazují zkušenosti z prováděných kontrol. Nechceme povinné subjekty omezovat pouze na jedno možné řešení. Performativnost je u tohoto ustanovení velmi žádoucí a praktická - což znamená, že je povinné osobě dán prostor k tvorbě vlastních vhodných pravidel, v tomto případě pravidel pro určení významné změny obecně definující požadovaný cílový stav. V praxi je vícero vhodných a fungujících variant řešení, navázání na samotné řízení rizik je pouze jedno z možných řešení. Cílem tohoto ustanovení je, aby byly identifikovány takové změny, které jsou podstatné z hlediska zajištění kybernetické bezpečnosti (resp. ty, které mohou bezpečnost pozitivně nebo negativně ovlivnit), a aby na ně byla soustředěna adekvátní pozornost. Z praktického úhlu pohledu, účelem určení významné změny je skutečnost, že se v organizaci plánuje něco, co není běžné, resp. nikoliv triviální, a očekává se od této skutečnosti pozitivní efekt. Avšak v případě, že se něco v průběhu realizace činností vedoucí k předmětné změně nezdaří, správně nastavené řízení změn eliminuje možné negativní dopady z toho plynoucí. Současně je vhodné zmínit, že v případě, kdy některý z požadavků není možné splnit např. z důvodu jeho nerelevantnosti či přijetí jiného adekvátního opatření (např. na základě provedené analýzy rizik), je možné zdůvodnit jeho vyloučení v prohlášení o aplikovatelnosti či jinou průkaznou

			formou a dané opatření ve vybraném případě neaplikovat. Připomínkové místo s vypořádáním souhlasí.
632. Ministerstvo financí	Z	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: - § 5 odst. 1 písm. d) a m) – dostupnost zdrojů (personálních a finančních) potřebných pro zajištění systému řízení bezpečnosti informací jako celku je ve veřejné správě odvislá od výše přidělených rozpočtových prostředků ze státního rozpočtu; není tedy možné určit ultimátní odpovědnost, resp. povinnost pro vrcholné vedení za zajištění dostupnosti zdrojů, resp. není v jeho možnostech toto zajistit.	Neakceptováno Smysl této povinnosti není ultimativní. Plnění této povinnosti je myšleno obecně. Jedná se o závazek, aby vedení usilovalo o získání/zajištění potřebných zdrojů, jako v jakékoli jiné oblasti, např. provoz, platy, investice atd. Nikdy nenastane situace, kdy budou prostředky na všechno, proto vedení určuje priority. Zároveň je mířeno na lidské kapacity, aby byly zajištěny role, které se budou kybernetickou bezpečností zabývat, a aby měli na problematiku odpovídající čas (např. 1/5 úvazek manažera kybernetické bezpečnosti pro velkou organizaci nemusí být dostatečný). Nejedná se o absolutní zajištění všech zdrojů, ale maximální snahu a postupné zlepšování. Nejenom v soukromoprávních organizacích, ale i veřejnoprávních, toto ustanovení zakotvuje požadavky na to, aby si vedení uvědomilo závazek a svou vůdčí roli určující směřování systému řízení informační bezpečnosti s ohledem na strategické směřování organizace. Dále je nutné podotknout, že individuální odpovědnost vrcholného vedení, která může v extrémním případě skončit pozastavením výkonu řídicí funkce (§ 63 nZKB), nelze podat vůči osobě vykonávající veřejnou funkci vymezenou funkčním nebo časovým obdobím a obsazovanou na základě přímé nebo nepřímé volby nebo jmenování podle zvláštních právních předpisů. Připomínkové místo s vypořádáním souhlasí.

633. Ministerstvo financí	Z	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: - § 6 odst. 2 – definovat jasné určení povinností spojených s návrhem a rozvojem architektury bezpečnosti regulované služby pro architekta KB; doplnit do návrhu vyhlášky, obdobně jako u role MKB, písm. b) odpovídá za stanovení, dokumentování, údržbu a neustálý rozvoj vhodné architektury bezpečnosti regulované služby podle současné dobré praxe – tato klíčová činnost je uvedena v tab. č. 3 Architekt kybernetické bezpečnosti v Příloze č. 6, která je však pouze doporučujícího charakteru.	Vysvětleno V současné době jsou prováděcí vyhlášky pro režim vyšších a nižších povinností ve fázi rozpracovanosti a nejsou součástí tohoto připomínkového řízení, to proběhne samostatně na začátku příštího roku. Připomínka nám přijde věcná, ale z naší strany je nutné se na ní podívat komplexně a správně ji vyhodnotit, zda nám Vámi navrhované řešení dává smysl, nebo zda nezvolíme trochu odlišnou systematiku pro určení povinností u všech bezpečnostních rolí. V současné chvíli ještě není finální rozhodnutí, i když jsou povinnosti AKB upraveny v příloze k vyhlášce pro režim vyšších povinností, máte pravdu, že jsou doporučujícího charakteru. Na optimálním řešení stále pracujeme, proto nejsme schopni v současné chvíli Vámi navržený způsob akceptovat. Každopádně i když tuto připomínku nebudete uplatňovat v rámci dalšího mezirezortního připomínkového řízení pro vyhlášky, budeme jí evidovat a věříme, že najdeme optimální řešení, na kterém bude panovat vzájemná shoda. Připomínkové místo s vypořádáním souhlasí.
634. Ministerstvo financí	Z	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: - § 17 odst. 5 a 6 – s ohledem na očekávaný nárůst počtu regulovaných služeb je určený interval 5 let na provedení auditu v celém rozsahu vyhlášky velmi krátký; doplnit do ustanovení možnost vzorkování.	Vysvětleno V současné době jsou prováděcí vyhlášky pro režim vyšších a nižších povinností ve fázi rozpracovanosti a nejsou součástí tohoto připomínkového řízení, to proběhne samostatně na začátku příštího roku. Tzv. metoda vzorkování je zcela běžná auditní metoda, která je vhodná jako auditní postup v případech, kdy není praktické ani finančně efektivní prověřit během auditu celou organizaci. Správný a odůvodněný výběr vzorků pro samotný audit má

			auditorům poskytnout informace (ujištění), že požadovaných cílů auditu může být nebo bude dosaženo. Je však důležité zvolit odpovídající výběr vzorků, aby na konci audit poskytl dostatečnou jistotu, že systém řízení informační bezpečnosti je v souladu se zákonnými požadavky. Připomínkové místo s vypořádáním souhlasí.
635. Ministerstvo financí	Z	Shrnutí závěrečné zprávy RIA, box 3.1 + Důvodová zpráva, části 7.1.1 a 7.1.6: MF chápe, že z uvedených důvodů není možné vyčíslit dopady na státní rozpočet v podobě absolutního čísla, které by bylo dostatečně přesné, nicméně MF požaduje doplnit odhad alespoň řádově (stamilióny, desítky miliard apod.), přičemž lze vyjít z dílčích údajů kapitol 7.1.2 až 7.1.5 důvodové zprávy, a číselně také uvedený rozptyl předpokládaných nákladů, jestliže z obdržených vyplněných dotazníků vyplynul jako extrémní. Pouhá verbální informace je nedostatečná. Mimo to na příjmové straně kapitoly 378 - Národní úřad pro kybernetickou a informační bezpečnost by mělo být zmíněno inkaso z pokut ze spáchaných přestupků podle navrhovaného § 58.	Akceptováno jinak Důvodová zpráva a RIA byla doplněna o požadované údaje stran rozptylu zjištěných dat stejně jako o upřesnění příjmů státního rozpočtu. I zde je však třeba poznamenat, že se nejedná o výdaje, které by bylo nutné vynaložit v rámci jednoho roku nutného pro implementaci povinností zákona o kybernetické bezpečnosti. Vždy je tu možnost tyto náklady rozložit do jednotlivých let v závislosti na prioritizaci daných aktiv a finančních možností organizací. Co se týče pokut jako příjmů rozpočtu Úřadu, toto ustanovení bylo z textu návrhu odstraněno, tyto jsou tedy i nadále příjmem státního rozpočtu. Bohužel ani z dostupných dat se nedomníváme, že by bylo možné vyhovět požadavku na celkový odhad nákladů na zavedení celého zákona, takový odhad bude vždy řádově chybný a nevypovídající (odpověď by proto teoreticky mohla být i v duchu připomínky - stamilióny až desítky miliard). Připomínkové místo s vypořádáním souhlasí.
636. Ministerstvo financí	Z	Shrnutí závěrečné zprávy RIA, box 3.1 + Důvodová zpráva, část 7.1.6: Jakékoliv zvyšování počtu úřednických míst (minimálně 39 pro NÚKIB a dalších 12 až 13 pro další úřady či orgány) a tím růst rozpočtových prostředků je v současné situaci, kdy je nutné skutečně	Neakceptováno Otázka zajištění dané agendy je řešena ve vypořádání připomínky viz výše. Nad to je možno uvést, že

		konsolidovat veřejné finance, nežádoucí a v rozporu s programovým prohlášením současné vlády. Navíc to poněkud koliduje s uvedeným principem maximální automatizace a samoobslužnosti platformy NÚKIB vedoucí k redukci administrativní zátěže.	princip maximální automatizace a samoobslužnosti platformy NÚKIB vedoucí k redukci administrativní zátěže s ničím nekoliduje, zavedení těchto procesů jen utlumují výši nutných požadavků, které by bylo potřeba nově vyčlenit, pokud by tento princip zaveden nebyl. Reakce připomínkového místa Na připomínce nadále trváme, neboť materiál v tomto ohledu není v souladu s programovým prohlášením vlády. Tento vzniklý rozpor tak lze odstranit jen politicky na úrovni vládních činitelů. A pokud by se takto zvyšování příslušných výdajů dle navrhovaného materiálu prosadilo, předpokládáme a doufáme, že alokace zdrojů na kybernetickou bezpečnost bude kompletně spadat mezi výdaje na obranu státu ve výši 2 % HDP podle § 2 odst. 1 písm. b) zákona č. 177/2023 Sb., o financování obrany České republiky. Po schůzce Byla navržena úprava materiálu (předkládací zpráva, RIA, odůvodnění) ve smyslu uplatněné připomínky. Návrh úprav byl ze strany připomínkového místa odsouhlasen. Připomínkové místo s vypořádáním souhlasí.
637. Ministerstvo financí	D	K Důvodové zprávě část 7. 1. 6 Shrnutí dopadů na státní rozpočet a ostatní veřejné rozpočty a Závěrečné zprávě RIA – MF doporučuje dopady do personální a platové oblasti, které by měly být nad rámec současných limitů stanovených pro NÚKIB (respektive nad rámec limitů stanovených pro další dotčené rozpočtové kapitoly) hradit právě v nynějších limitech kapitol. MF doporučuje pokrýt výhradně v rámci stanovených limitů počtu míst a objemu prostředků na platy,	Neakceptováno Viz vypořádání obdobné připomínky výše. V souladu s výše uvedeným je potřeba tak jako tak provést aktualizaci schválené koncepce NÚKIB, a tyto oblasti náležitě upravit. Není možné vykonávat ani utlumit v této situaci (jak s ohledem na válečný konflikt a potřebu zvyšování bezpečnosti ve všech oblastech, tak

		např. na úkor agend, které se přirozeně utlumují, tj. bez nároku na jejich jakékoliv navýšení. Případně ať s ohledem na rozpočtovou situaci MF doporučuje předkladateli přehodnotit výběr varianty řešení V na jinou méně ekonomicky náročnou variantu řešení.	s ohledem na nárůst agendy spojený s směrnicí NIS2) agendu NÚKIB, případně ji vykonávat stávajícím způsobem, a je potřeba tyto kapacity navýšit. Pokud by k tomu nedošlo, není možné zajišťovat bezpečnost v poptávané kvalitě, pokud vůbec. Je také potřeba mít na paměti, že NÚKIB jako úřad, který vznikl teprve v roce 2017 a vykonává velkou šíři vysoce aktuální a potřebné agendy (kybernetická bezpečnost, bezpečnost utajovaných systémů, kryptografie,...), která se rozvíjí, než aby stagnovala nebo se utlumovala, je na hraně kapacit již nyní. Přehodnocení varianty č. V odpovídá nejvhodnějšímu způsobu řešení požadavku Bezpečnostní rady státu a z toho důvodu je také předkládána. Připomínkové místo s vypořádáním souhlasí.
638. Ministerstvo financí	D	V části 7.2 důvodové zprávy (7.2. Dopady na územní samosprávné celky) se uvádí, že náklady na zabezpečení kybernetické bezpečnosti obcí s rozšířenou působností (kterých je 205) budou cca 800 000 Kč a 1 500 000 Kč vůči jednomu zabezpečovanému systému. Ze strany těchto ORP lze očekávat vysokou nevoli, pokud tyto obce budou muset předmětné náklady hradit z vlastních zdrojů. Jakkoli MF chápe nutnost ošetřit kybernetickou bezpečnost i na místních úrovních, MF dává ke zvážení, zda by náklady na aktualizaci zabezpečovaných systémů neměl v případě ORP financovat stát. Je tedy nutno specifikovat finanční dopady na veřejné rozpočty a zdroj jejich úhrady.	Neakceptováno Úvodem je nutné podotknout, že všechny ORP budou po diskusích v rámci Úřadu zařazeny v režimu nižších povinností. Vámi zmiňované náklady (800 000 - 1 500 000 Kč) vychází z výpočtů, které zahrnovaly požadavky na vyšší režim povinností - demonstrativní výpočet nákladů v bodech 7.1.2-7.1.6 důvodové zprávy hovoří o nákladech správců kritické informační infrastruktury a významných informačních systémů, což je ekvivalent nově zaváděného režimu vyšších povinností. Oproti tomu budou náklady na zajišťování kybernetické bezpečnosti v režimu nižších povinností mnohem nižší. Žádná ORP nebude začínat se zajišťováním kyberbezpečnosti na "zelené louce". Aníž se to tak může jevit, některé požadavky kladené na režim nižších povinností má již zavedena většina dotčených organizací a mnoho projektů je v realizaci. K tomu slouží např. i financování z výzev IROP.

		Výdaje na bezpečnostní opatření nebudou jednorázové, ale budou rozloženy v čase (i několika let), jak vyhlášky umožňují. Připravovaný nZKB ukládá povinnost plnit, nikoliv direktivně splnit, všechna bezpečnostní opatření. Tzn. že ORP si zavede plán plnění těchto bezpečnostních opatření, který bude postupně realizovat dle svých možností a potřeb dané organizace. Reakce připomínkového místa - Rozpor S navrženým vypořádáním nesouhlasíme, přičemž uvádíme: 1. Pokládáme za nezbytné, aby NÚKIB vypracoval aktualizovanou „Koncepci rozvoje NÚKIB“, která by měla být schválena vládou stejně jako v případě nyní již neaktuální předchozí verze. V ní by měly být zapracovány i veškeré nezbytné potřeby úřadu spojené s aktuálně předkládanými legislativními materiály strategického charakteru. 2. Dále upozorňujeme na skutečnost, že předmětný návrh zákona je dotčeným kapitolám znám již řadu měsíců (byl zpracován i věcný záměr zákona), přičemž měly možnost s MF projednat v rámci přípravy SR 2024 a SDV 2025-26 veškeré své nadpožadavky. Nyní je již návrh SR projednáván ve vládě. Do návrhu zákona proto požadujeme uvést, že veškeré výdaje kapitol vyvolaných touto právní úpravou budou vykryty v rámci výdajových limitů schváleného zákona o SR na tyto roky bez navyšujících personálních a finančních požadavků. Na připomínkách uplatněných v rámci MPŘ trváme a s návrhem vypořádání ze strany předkladatele materiálu nesouhlasíme.

			Jako doporučující připomínka vypořádáno.
639. Ministerstvo financí	D	Shrnutí závěrečné zprávy RIA, boxy 3.1 a 3.3 + Důvodová zpráva, části 7.1.1 a 7.3: Není jasné, proč v rámci dopadů na veřejné rozpočty je mezi neznámé a proměnlivé indikátory zařazen také soulad se zněním stávajícího zákona o kybernetické bezpečnosti (č. 181/2014 Sb.).	Vysvětleno Soulad se stávajícím zněním kybernetické bezpečnosti je proměnlivý ukazatel v případě, že subjekt regulovaný podle navrhované právní úpravy je také povinným subjektem podle úpravy stávající. Tento model se uplatní u všech ministerstev, ústředních správních úřadů a dalších institucí, které jsou v současné chvíli regulovány, a které budou nově spadat do režimu vyšších povinností. Každý z těchto subjektů má v souladu se stávající právní úpravou jinak nastavený rozsah zavádění bezpečnostních opatření, zvolil jiná opatření a může být v jiné fázi zavádění, případně může, ale nemusí, mít problémy s průběžným udržováním daných bezpečnostních opatření. To vše jsou proměnlivé ukazatele vztahující se k této připomínce. Připomínkové místo s vypořádáním souhlasí.
640. Ministerstvo financí	D	MF doporučuje v návrhu zákona sjednotit formátování (např. odstavce by měly být formátově jednotné) a uvést materiál do souladu s legislativními pravidly vlády (např. rozdělit paragrafy, kde je více nežli 6 odstavců). Dále je nutné upravit výkaznictví, jelikož vykazovat jako transpoziční ustanovení, která jsou nad rámec práva Evropské unie, je v rozporu s legislativními pravidly vlády a odpovídajícím metodickým pokynům (např. § 29 návrhu zákona).	Akceptováno Připomínkové místo s vypořádáním souhlasí.
641. Ministerstvo financí	D	V §2 MF navrhuje doplnit pojem „posuzování shody“ jako nové písm. „h) posuzování shody je procesem zhodnocení, zda byly splněny stanovené požadavky týkající se produktu, služby nebo procesu IKT“ a to ve vazbě na navrhovaný § 46 a násl. a Nařízení Evropského	Neakceptováno V tuto chvíli nepovažujeme za nutné rozšiřovat definiční ustanovení o tuto definici, její výklad

		parlamentu a rady (EU) 2019/881 čl. 77 ve vazbě na Nařízení evropského parlamentu a rady (ES) 765/2008, čl. 2, odst. 10) a odst. 12), resp. zákona č. 22/1997 Sb., o technických požadavcích na výrobky o změně a doplnění některých zákonů.	nepovažujeme za problematický a s ohledem právě na uváděné předpisy, které ji definují, ani jako potřebný. Připomínkové místo s vypořádáním souhlasí.
642. Ministerstvo financí	D	K §4 – MF upozorňuje, že podle čl. 79 odst. 3 může správní úřad vydat právní předpis jen v mezích zákona, ovšem zde MF považuje stanovení mezí za nedostatečné. Doporučuje se zpřesnit. Není jasný vztah mezi zmocněním uvedeným v odstavci 1 a v odstavci 2 - stanoví tedy prováděcí předpis kritéria pro identifikace služby jen u vybraných odvětví uvedených v odstavci 2 nebo u všech služeb? Doporučuje se vyjasnit, formulovat jednoznačněji.	Akceptováno Došlo k úpravě relevantních ustanovení a dalšímu přiblížení současnému znění např. § 22a zákona o kybernetické bezpečnosti Připomínkové místo s vypořádáním souhlasí.
643. Ministerstvo financí	D	K § 17 odst. 4 Vzhledem k tomu, že podle Legislativních pravidel vlády by se v právních předpisech neměly používat zkratky složené z velkých písmen, doporučuje se jej při prvním použití označit jako "Portál Národního úřadu pro kybernetickou a informační bezpečnosti" a zavést pro tento pojem vhodnou legislativní zkratku (nabízí se "Portál Úřadu"). Obdobná připomínka platí i pro zkratku CSURT.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
644. Ministerstvo financí	D	K §35 - Povinnosti subjektů poskytujících služby registrace jmen domén Ze znění textu paragrafu není zcela zřejmé, že se jedná o údaje Subjektu poskytující služby registrace jmen internetových domén. MF navrhuje úpravu textu ve znění: „(1) Subjekt poskytující služby registrace jmen internetových domén hlásí Úřadu bez zbytečného odkladu, nejpozději však do 30 dnů ode dne, kdy začal poskytovat službu registrace jmen internetových domén, své údaje v rozsahu a způsobem stanoveným prováděcím právním předpisem“	Neakceptováno - nyní § 36 Údaje, které má subjekt hlásit, jsou uvedeny v textu zákona, a nikoliv vyhlášky, z důvodu přehlednosti pro tyto subjekty, na které se vztahují právě jenom povinnosti uvedené v § 36 a § 37. Vzhledem ke skutečnosti, že se uvedená ustanovení vztahují pouze na subjekty uvedené v hlavě III, nelze očekávat, že by si tyto subjekty dovodily povinnost hlásit údaje jiných subjektů. Připomínkové místo s vypořádáním souhlasí.

645. Ministerstvo financí	D	V §36 v odstavci 1 se doporučuje nahradit slovo "zejména" slovem "alespoň", aby právní úprava jednoznačně stanovila minimální rozsah údajů, které mají být obsaženy v databázi.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
646. Ministerstvo financí	D	Doporučujeme pojem "státní správa" v Hlavě V nahradit pojmem "veřejná správa". Pojem veřejná správa je definován v zákoně č. 365/2000 Sb., zákon o informačních systémech veřejné správy - §27 odst. 1)a) a je součástí tohoto návrhu zákona viz. §4 odst. 2a) a § 27 a). Upozorňuje se, že legislativa EU nerozlišuje pojem státní a veřejná správa a pro tuto oblast používá pojem "veřejná správa". Termín veřejná správa je kompatibilní s Nařízením evropského parlamentu a rady (EU) č. 549/2013 s kapitolou Vládní instituce (S13), ve znění odst. 2.111, 2.112 a)-d), 2.113 a)-d), 2.114, 2.115, 2.116, 2.117 a)b).	Akceptováno Připomínkové místo s vypořádáním souhlasí.
647. Ministerstvo financí	D	K §40 odst. 1, písm. g) Opatření k řešení stavu kybernetického nebezpečí. Je zde reálné riziko, že při vyhlášení stavu kybernetického nebezpečí nebudou v rámci ČR dostatečné personální a finanční kapacity na splnění nařízení k provedení skenu zranitelností nebo penetračního testu. Jelikož se jedná o expertní činnost, kterou realizuje jen omezený počet ekonomických subjektů je toto riziko reálné. Ze současné praxe je jasné, že Úřad i nedisponuje takovým počtem odborníků, kteří by ve stavu kybernetického nebezpečí zajistili zmiňované činnosti. Navrhuje se, aby v zákoně bylo popsáno, že tyto činnosti budou realizovány na pokyn Úřadu postupně nebo adresně, nebo v zákoně omezit rozsah nařízení provedení skenu zranitelností nebo penetračního testu na jednotlivé regulované osoby.	Vysvětleno - nyní § 41 V případě, že dojde k nařízení provedení skenu zranitelnosti nebo penetračního testování, byla identifikována potřeba zapojení zaměstnanců nebo odpovědných osob adresáta takového nařízení. Z toho důvodu je také v návrhu zákona vyžadována součinnost osob, kterým bude tento nástroj nařízen, neboť tím bude celý proces zjednodušen a zároveň nebudou nadměrně zatěžovány kapacity Úřadu a mělo by se snížit riziko, že dojde k poškození aktiv. Rozsah je nutný za součinnosti odpovědné osoby adresáta vymezit ad hoc po vzájemné konzultaci a odhadu dopadů penetračního testování nebo skenu zranitelností. Reakce připomínkového místa V §41 písm. g) je stále nařízení a ne poskytnutí součinnosti. Vypořádání neodpovídá znění textu Materiálu. „g) <i>nařídit orgánům a osobám provedení</i>

			<i>skenu zranitelností nebo provedení identifikace a ověření zranitelností prostřednictvím simulace reálného útoku (dále jen „penetrační test“),“</i> Nesplnění je nadále sankcionováno jako přestupek dle §60 odst. 8 písm. d). Na připomínkách uplatněných v rámci MPŘ trváme a s návrhem vypořádání ze strany předkladatele materiálu nesouhlasíme. Jako doporučující připomínka vypořádáno.
648. Ministerstvo financí	D	V §41 MF dává se ke zvážení, zda by neměl být fakt, že je Národní úřad pro kybernetickou a informační bezpečnost ústředním orgánem státní správy uveden v § 2 zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky. Dále se doporučuje nahradit slova „ústředním správním úřadem“ slovy „ústředním orgánem státní správy“.	Akceptováno - nyní § 44 Připomínkové místo s vypořádáním souhlasí.
649. Ministerstvo financí	D	K §41 odst. 5, písm. g). Dává se na zvážení odstranění nejistoty při realizaci činností Vládního CERT, který je součástí Úřadu. Úřad nemůže (za současné legislativy) realizovat žádná ofensivní akce v rámci řešení kybernetických útoků. Pro odstranění nejistoty MF navrhuje změnit text na: „a) zajišťuje řešení, koordinaci, analýzu a preventivní opatření vůči“	Vysvětleno - nyní § 44 Činnosti Vládního CERT související s řešením kybernetických bezpečnostních incidentů, zranitelností a dalších mohou mít kromě podoby zcela pasivního příjmu informací od povinných osob v omezeném rozsahu též aktivní charakter, například v souvislosti s vyhledáváním zranitelností. Přestože se tedy nejedná o aktivní zásahy proti útočníkovi (např. ve smyslu § 16g zákona č. 289/2005 Sb., o vojenském zpravodajství), považujeme vzhledem k možným podobám realizace této činnosti termín "působení" za nejvíce přiléhavý. Nahrazení slova "působení" za "opatření" by mohlo být naopak matoucí, neboť v zákoně je tento pojem používán pro další instituty (bezpečnostní opatření, protiopatření, nápravná opatření).

			Připomínkové místo s vypořádáním souhlasí.
650. Ministerstvo financí	D	U §41 dává se ke zvážení, aby problematika utajovaných informací (viz § 1 odst. 3 – „Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi“) byla upravena zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, a to s ohledem na současný ucelený systém právních předpisů vztahujících se k ochraně utajovaných informací. Tento sjednocený systém je řešen v rámci jednoho zákona resp. další prováděcích předpisů v rámci jednotlivých druhů zajištění ochrany utajovaných informací. V tomto ohledu MF nepovažuje za žádoucí upravovat dalším způsobem oblast utajovaných informací v novém právním předpise, nýbrž navrhuje se vytvořit samostatnou kapitolu: „Národní úřad pro kybernetickou bezpečnost“ (dále jen „NÚKIB“) v rámci zákona č. 412/2005 Sb., který by upravoval jednotlivé aspekty ochrany utajovaných informací ve vztahu k NÚKIB. Další možnou variantou by mohlo být zcela zrušení stávajícího znění ustanovení §1 odst. 3, který je dle názoru MF v rozporu se zněním některých ustanovení, zejména však s ustanovením § 41 odst. 4 písm. c), dle kterého Úřad vykonává státní správu v oblasti bezpečnosti informačních a komunikačních systémů nakládajících s utajovanými informacemi a v oblasti kryptografické ochrany, zajišťuje činnost Národního střediska komunikační bezpečnosti, Národního střediska pro distribuci kryptografického materiálu, Národního střediska pro měření kompromitujícího vyzařování a Národního střediska pro bezpečnost informačních systémů, které jsou jeho součástí.	Vysvětleno - nyní § 44 Úprava je převzata ze znění účinného zákona o kybernetické bezpečnosti, který navazuje na úpravu v zákoně o ochraně utajovaných informací. Máme za to, že navrhovaným (a současně i původním) zněním § 1 odst. 3 nedochází k narušení uceleného systému ochrany utajovaných informací upravené zákonem č. 412/2005 Sb., naopak zcela jasně omezuje působnost návrhu zákona ve vztahu k informačním a komunikačním systémům nakládajícím s utajovanými informacemi a podporuje tak komplexní úpravu provedenou zákonem o ochraně utajovaných informací. Co se týče úpravy zákona o ochraně utajovaných informací, jeho ustanovení § 137a shrnuje pravomoci Národního úřadu pro kybernetickou a informační bezpečnost v oblasti ochrany utajovaných informací, které jsou promítnuty do 44 odst. 1 a na něj pak navazující § 44 odst. 4 písm. c) a d). § 44 návrhu zákona (stejně tak jako § 22 v účinném zákoně o kybernetické bezpečnosti) zakotvuje postavení Národního úřadu pro kybernetickou a informační bezpečnost a vymezuje (resp. shrnuje) jeho pravomoci jako ústředního správního úřadu komplexně na jednom místě. Navržená úprava není v rozporu s úpravou zákona o ochraně utajovaných informací, naopak je s ní zcela v souladu a přímo na ní odkazuje. Z uvedených důvodů ponecháme předmětnou navrženou úpravu beze změn. Připomínkové místo s vypořádáním souhlasí.

651. Ministerstvo financí	D	V § 48 a násl. MF doporučuje změnit toto ustanovení a násl. tak, aby základem bylo členství v Komunitě, které vzniká registrací žadatele o toto členství. Osoba, která je registrována, pak by již nebyla žadatelem, ale členem. Je nesystémové označovat osobu, které vzniklo registrací členství, jako žadatele stejně jako osobu, která o toto členství teprve žádá. To, že jsou posuzovány podmínky registrace na základě žádosti, a i následně kontrolovány, není vhodné označovat jako podmínky žádosti, ale jako podmínky členství nebo podmínky registrace.	Akceptováno jinak – nyní § 51 Nově navrhované znění zákona vztahující se k Národnímu koordinačnímu centru využívá pojem "člen Komunity" jako označení subjektu (žadatele) po jeho registraci jako člena Komunity. Připomínkové místo s vypořádáním souhlasí.
652. Ministerstvo financí	D	V § 48 odst. 1 navrhuje MF (GŘC) písm. d) formulovat takto: Žadatel má základní způsobilost, pokud „d) nemá v České republice evidován nedoplatek s výjimkou nedoplatku, u kterého je povoleno posečkání jeho úhrady nebo rozložení jeho úhrady na splátky“. Odůvodnění: S ohledem na sjednocení textace napříč jednotlivými právními předpisy navrhujeme přeformulovat stávající text uvedený v písmenu d), podle kterého žadatel má základní způsobilost, pokud nemá v České republice v evidenci daní zachycen splatný daňový nedoplatek. Jeví se žádoucí doplnit, že žadatel může mít nedoplatek, u kterého je povoleno tzv. posečkání ve smyslu § 156 daňového řádu. Tato konstrukce je použita např. v zákoně o spotřebních daních (§ 43f odst. 1), zákoně o hazardních hrách (§ 91 odst. 2 písm. a), zákoně o povinném značení lihu (§ 56 odst. 1) nebo zákoně o pobytu cizinců na území České republiky (§ 178 e odst. 1) apod. Obdobná připomínka je vznesena i k § 42 odst. 1 písm. e) návrhu zákona o kybernetické bezpečnosti.	Akceptováno - nyní § 51 § 51 odst. 1 písm. d) až f) upraven následovně, nově pod odst. 1 písm. d) dotčeného §: " d) nemá v České republice evidován nedoplatek (s výjimkou nedoplatku, u kterého je povoleno posečkání jeho úhrady nebo rozložení jeho úhrady na splátky), 1. u orgánů Finanční správy České republiky, 2. u orgánů Celní správy České republiky, 3. na pojistném a na penále na veřejné zdravotní pojištění, a 4. na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti," Připomínkové místo s vypořádáním souhlasí.
653. Ministerstvo financí	D	V § 48 odst. 4 MF upozorňuje, že v tuzemské evidenci skutečných majitelů nejsou zapsány osoby, které jsou zapsány v evidenci skutečných majitelů v jiném členském státě, a tudíž podmínka v odst. 4 efektivně vyřazuje všechny společnosti usazené mimo Českou	Akceptováno - nyní § 51 V § 51 doplněn nový odstavec, který zní: " V případě, že skutečným majitelem člena Komunity je osoba usazená na území členských států Evropské unie a

		republiku. Dává se ke zvážení, zda se jedná o žádoucí stav. Dává se ke zvážení, zda nezařadit do podmínek, aby daná osoba nepodléhala ani mezinárodním sankcím, včetně těch unijním, jelikož se jedná o naprostou většinu sankcionovaných osob.	členských států Evropského sdružení volného obchodu, předloží člen Komunity k prokázání způsobilosti výpis ze zahraniční evidence obdobné evidenci skutečných majitelů, který nesmí být starší než 30 kalendářních dnů před dnem podání žádosti." Dále došlo k úpravě § 51 odst. 1 písm. b) a § 51 odst. 5 (původně odst. 4) písm. c), kdy došlo k rozšíření požadavků na způsobilost žadatele a to tak, že vůči němu (a jeho skutečnému majiteli) Česká republika neuplatňuje mezinárodní sankce podle přímo použitelného předpisu Evropské unie nebo podle právního předpisu upravujícího provádění mezinárodních sankcí. Připomínkové místo s vypořádáním souhlasí.
654. Ministerstvo financí	D	K §55 MF doporučuje název upravit na "Zmocňovací ustanovení" a zařadit ho až do závěrečných ustanovení. Současně se doporučuje v odstavci 1 upravit úvodní část odstavce 1 takto "Úřad stanoví vyhláškou" a zrušit jeho označení číslem a odstavec 2 vypustit.	Akceptováno jinak § 55 byl celý zrušen. Připomínkové místo s vypořádáním souhlasí.

655. Ministerstvo financí	D	Z dikce navrženého § 56 není jasné, zda se týká i kontroly povinností podle § 29 a § 63 odst. 4, které se týkají poskytování informací o třetích osobách, ve vztahu k orgánům a osobám, které mají povinnosti mlčenlivosti. V případě, kdy by měly být tyto povinnosti kontrolovány i u osob, které mají povinnost mlčenlivosti, by došlo k absurdní situaci, kdy by osoba, vůči níž se povinnost mlčenlivosti uplatňuje, kontrolovala poskytování údajů, které mohou podléhat mlčenlivosti, což bez seznámení se se všemi údaji (tj. i těmi podléhajícími mlčenlivosti) efektivně nelze. Požaduje se buď úprava legislativního textu ve smyslu výše uvedeného, nebo přinejmenším úprava důvodové zprávy tak, aby bylo jednoznačně uvedeno, že na orgány veřejné moci a osoby s povinností mlčenlivosti se kontrolní pravomoci Úřadu nevztahují.	Akceptováno Odstavec 5 § 30 stanovuje, že poskytnutí informací podle tohoto ustanovení není porušením mlčenlivosti podle jiného právního předpisu, nicméně u této konkrétní povinnosti nepředpokládáme potřebu kontroly na místě - v daném ustanovení je jasně stanovena lhůta, její nedodržení, resp. soustavná nečinnost ze strany povinného subjektu, jsou skutečnosti, které není třeba kontrolovat na místě a seznamovat se s informacemi podléhajícími mlčenlivosti. Obdobné platí u § 65 odst. 4 - kontrola nemůže být "zneužívána" pro získávání informací, na které by Úřad neměl nárok, nicméně obě řešená ustanovení obsahují formulaci v tom smyslu, že poskytnutí relevantních informací není porušením mlčenlivosti. Výše uvedené (o nemožnosti zneužívat kontrolu pro obcházení mlčenlivosti) bude každopádně doplněno do důvodové zprávy k § 58 návrhu zákona. Připomínkové místo s vypořádáním souhlasí.
656. Ministerstvo financí	D	Doporučuje se změnit nadpis § 62, jelikož neodpovídá obsahu ustanovení.	Akceptováno - nyní § 64 Název ustanovení § 64 změněn na "Zajištění účelu a průběhu řízení", přičemž původní odstavec 4, který zní "Exekuce rozhodnutí Úřadu ukládajícího povinnost předat nebo jinak naložit s informacemi a daty se řídí ustanoveními správního řádu upravujícími exekuci odebráním movité věci.", je přesunutý k § 26, ke kterému se vztahuje. Připomínkové místo s vypořádáním souhlasí.
657. Ministerstvo financí	D	K oblasti tzv. dělené správy pouze MF (GŘC) upozorňuje, že návrh zákona o kybernetické bezpečnosti obsahuje oblast ukládání pokut	Akceptováno jinak

		obdobně jako stávající zákon č. 181/2014 Sb., kdy dané pokuty celní úřady vymáhají (§ 58-59 a § 62 odst. 3 ve vztahu ke kontrolnímu řádu). Nově je však stanovena i oblast ukládání pořádkových pokut (§ 62 odst. 1) a donucovacích pokut (§ 62 odst. 2), které jsou upraveny ve vztahu ke správnímu řádu, a tyto pokuty si bude Národní úřad pro kybernetickou a informační bezpečnost vybírat a vymáhat sám (donucovací pokuta je již jedním ze způsobů exekuce). S ohledem na působnost Celní správy v oblasti dělené správy MF (GŘC) předpokládá, že řešení této problematiky bude upraveno v rámci komplexního sjednocení úpravy správního řádu a daňového řádu.	Ve vztahu k výběru pokut za přestupky dojde na základě připomínky ke sjednocení mechanismu výběru pokut podle návrhu zákona s obecnou praxí ve správním trestání, kdy pokud jsou pokuty příjmem státního rozpočtu, jsou standardně vybírány celními úřady (aktuálně návrh v § 59 odst. 1 počítá s tím, že pokuty vybírá NÚKIB). Ve vztahu k výběru donucovacích a pořádkových pokut zůstává v platnosti obecná úprava správního řádu (pokuty vybírá orgán, který je uložil, a jsou také jeho příjmem), návrh zákona upravuje speciálně pouze výši maximálních pokut, které lze uložit. Připomínkové místo s vypořádáním souhlasí.
658. Ministerstvo financí	D	U označení odstavců § 71 je třeba doplnit půlkulatou závorku i před číslo odstavce. V zájmu první jistoty se doporučuje slova "dosavadních právních předpisů" nahradit označením právních předpisů, o které se jedná (předpokládáme, že půjde o zákon č. 181/2014 Sb. V odstavci 1 je třeba u prvního výskytu zákona č. 181/2014 Sb. uvést jeho název, protože je citován poprvé.	Akceptováno jinak Připomínkové místo s vypořádáním souhlasí.
659. Ministerstvo financí	D	K §72 MF upozorňuje, že v souladu s čl. 52 Legislativních pravidel vlády je třeba zrušit i všechny zákony, kterými byl novelizován zákon č. 181/2014 Sb.. Tato připomínka platí i pro rušené vyhlášky, pokud byly novelizovány. Zrušované vyhlášky je třeba za sebou řadit v časové posloupnosti od nejstarší k nejnovější.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
660. Hospodářská komora ČR	D	Hospodářská komora ČR (dále jen „HK ČR“) se domnívá, že se předkladatel návrhu ZKB dostatečně nezabýval otázkou realizovatelnosti a dopadů navrhovaných opatření, protože rozsah a dopad povinností, ukládaných předloženým materiálem v důsledku zavedení mechanismu není proporcionální a zásadně přesahuje rámec působnosti předkladatele. Důsledkem mechanismu je zásadní dopad	Neakceptováno Ve vztahu k poskytovatelům sítí či službám elektronických komunikací NÚKIB považuje za nutné chránit veškeré funkce veřejné komunikační sítě, které jsou považovány za kritické. Tyto kritické funkce nemusí být nutně vztaženy pouze na jádro sítě, jelikož

	do ústavním pořádkem zaručeného práva podnikat, který se silně promítne jak v ekonomické, tak geopolitické rovině. Připomínky předkládané níže k mechanismu prověřování bezpečnosti dodavatelského řetězce lze v obecné rovině rozdělit do 3 hlavních bodů: Omezení rozsahu regulace na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni Předkladatel opakovaně uvedl, že mechanismus se má vztahovat pouze na tu nejkritičtější část strategické infrastruktury. V návrhu ZKB však předkladatel vymezil rozsah mechanismu formou vyhlášky o nepominutelných funkcích, která mj. pro oblast telekomunikací obsahuje jak ty nejkritičtější části sítě (jako je jádro sítě), tak i v obecné rovině méně kritické části sítě (např. rádiová přístupová síť) nebo aktiva, která nemají přímý vliv na nedostupnost regulovaných služeb (jako je např. fakturační systém). V návrhu ZKB také zcela chybí odůvodnění, proč jsou kritické části stanoveného rozsahu aktiv definovány tak široce. V předkládaných připomínkách k návrhu ZKB níže HK ČR kritické části strategické infrastruktury transparentně rozdělila dle hrozeb a míry dopadu jejich realizace. Nejvýznamnější hrozbou je výpadek regulované služby. Rozsah mechanismu je tedy omezen na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro oblast telekomunikací se bude jednat zejména o jádro sítě, případně části přenosové sítě. Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je tedy vhodné, aby byla dána možnost státu okamžitým zásahem zakázat vybraného dodavatele, u kterého identifikuje významnou hrozbu. Pro zbylé části aktiv strategicky významné služby, které nemohou ze své podstaty způsobit nedostupnost služby na kritické úrovni, je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik	mnohdy zabezpečují a udržují chod poskytování služeb koncovým uživatelům, a to zejména v rámci rádiové přístupové sítě. Například řízení či monitorovací funkce rádiových stanic představují prostředek, pomocí kterého se koncoví uživatelé připojují právě ke službám poskytovaným jádrem sítě. V případě jejich kompromitace tak může být narušeno či zcela porušeno poskytování služeb koncovým uživatelům. Je pravdou, že jádro sítě je nejvýznamnější z hlediska bezpečnosti a integrity sítě a dostupnosti poskytovaných služeb, ale bez zabezpečené rádiové přístupové sítě pozbývá funkční jádro smysl, jelikož nemůže dojít k propojení koncových zařízení s jádrem, což souvisí s nemožností zajistit dostupnost. Obdobný přístup ke kritičnosti sítí, nehledě na jejich umístění v rámci architektury sítě, zvolilo také Dánsko, dále pak v rámci EU Belgie či Finsko. Kritické části sítě jsou omezeny rozsahem zahrnutých aktiv a rozsahem bezpečnostně významných dodávek. Byť by se striktně jazykovým výkladem dalo dovodit, že je možné do kritického rozsahu sítě zahrnout pouze aktiva s dopadem "kritická", nelze tak učinit. Co se týče ochrany aktiv stanoveného rozsahu, u kterých poskytovatel tyto ohodnotil úrovní vysoká (v rámci připomínky se jedná o část "vysoká nebo"), tak zde, na základě předešlých zkušeností a poznání (vyplývajících zejména z kontrolní činnosti NÚKIB), NÚKIB konstatuje, že tato aktiva jsou velmi důležitá až kritická pro fungování strategicky významných služeb. Aktiva ohodnocena jako vysoká mají podstatné dopady na primární aktiva, a tím pádem na chod celé strategicky významné služby. Ochrana pouze kritických aktiv by nebyla v plném rozsahu

		minimalizoval rizika, která v rámci opatření obecné povahy identifikoval předkladatel. Předkladatel by jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by nově byla upravena zvlášť v bezpečnostní dokumentaci, přičemž poskytovateli strategicky významné služby by byla uložena povinnost ji každoročně aktualizovat. Tento systém nazývá HK ČR tzv. kaskádou bezpečnostních povinností, kdy pro nejkritičtější část strategické infrastruktury bude povinnost řídit se případným omezením či zákazem uvedeným v opatření obecné povahy, a pro ty méně kritické části strategické infrastruktury bude nově dána výslovná povinnost zohlednit rizika identifikovaná státem a implementovat odpovídající bezpečnostní opatření.	schopna pokrýt bezpečnost strategicky významné služby v doménách důvěrnost, integrita i dostupnost. Připomínka vypořádána.
661. Hospodářská komora ČR	D	Zapojení vlády a sektorového regulátora do Mechanismu a) zapojení vlády Zákazem či omezením plnění dodavatele dochází k významnému zásahu do svobody podnikání mnoha subjektů na trhu. Zákaz i omezení plnění dodavatele může mít významné ekonomické, ale i geopolitické dopady. Obdobné dopady již stát v minulosti hodnotil v rámci právní úpravy prověřování zahraničních investic. V rámci procesu prověřování zahraničních investic dochází obdobně jako v případě mechanismu k prověřování osoby investora na základě strategických kritérií. Stejně jako v případě mechanismu může také dojít k zákazu investice. V případě prověřování zahraničních investic je zákaz investice podmíněn usnesením vlády. Stejně by tomu mělo být i v případě mechanismu, zejména s ohledem na skutečnost, že plošný zákaz či omezení plnění dodavatele může mít mnohem větší dopad na trh než zákaz doposud neuskutečněné investice. b) zapojení sektorového regulátora HK ČR respektuje roli předkladatele v rámci procesu posouzení rizikovitosti dodavatele, kterou by společně s vládou měl mít. V rámci	Zapojení vlády do procesu prověřování: Neakceptováno. Do procesu je zapojena Bezpečnostní rada státu, která je stálým pracovním orgánem vlády pro koordinaci problematiky bezpečnosti České republiky a přípravu návrhů opatření k jejímu zajišťování, ve které jsou členové vlády zastoupeni. V případě potřeby může samozřejmě problém eskalovat až na vládní úroveň. S tím také plyne procesní stránky věci, kdy Bezpečnostní rada státu může návrh opatření obecné povahy v případě, že je jí předložen, neprojednat, přerušit jeho projednávání, vrátit jej k přepracování, případně s ním vyjádřit nesouhlas. Jakékoliv rozhodnutí je pro Úřad samozřejmě závazné. Zapojení sektorového regulátora: Neakceptováno v navržené podobě. Úřad při vydávání opatření obecné povahy spolupracuje se všemi orgány státní správy, které jsou relevantní pro

		určení lhůty pro implementaci případného omezení či zákazu plnění dodavatele je však role sektorového regulátora klíčová. Případné omezení či zákaz totiž může mít významný dopad na schopnost povinných osob plnit své zákonné povinnosti vyplývající ze zvláštních právních předpisů (v případě telekomunikací jsou to například výstavbové povinnosti vyplývající ze zákona o elektronických komunikacích). Je tedy naprosto zásadní, aby daný sektorový regulátor (v případě telekomunikací ČTÚ), měl možnost se k implementaci omezení či zákazu vyjádřit a předkladatel musel k jeho stanovisku přihlídnout.	získání všech informací potřebných k tomu, aby byla dosažena maximální kvalita výsledného opatření obecné povahy, která se skládá z mnoha faktorů, například zvýšení bezpečnosti, dopady na poskytovatele strategicky významných služeb, dopady na hospodářskou soutěž, dopady na mezinárodní dohody, lhůta pro zohlednění opatření, dopady na další zákonné povinnosti poskytovatelů strategicky významných služeb a mnoho dalších. Toto v návrhu zákona ošetřeno v § 30 a nadto to vyplývá z obecných principů dobré správy. Připomínka vypořádána.
662. Hospodářská komora ČR	D	Kompenzace Obdobně, jako tomu je v případě zákona o vojenském zpravodajství, navrhuje HK ČR do zákona zapracovat ustanovení o náhradě účelně vynaložených nákladů, které v návrhu ZKB zcela absentuje, je však z hlediska dotčených subjektů zásadní. Konkrétní aspekty náhrady účelně vynaložených nákladů jsou popsány níže v návrhu nového ustanovení § 30a návrhu ZKB.	Neakceptováno K dané připomínce uvádíme, že navrhovaný zákon považujeme za ústavně konformní, kvůli čemuž není důvod přidávat ustanovení o náhradě škod. Vzhledem k charakteru navrhované právní úpravy, převážně v oblasti mechanismu bezpečnosti dodavatelského řetězce, která se snaží vyjít vstříc povinným osobám například v otázkách životních cyklů technologií nebo zamezení možné závislosti na jedné technologii skrz systém výjimek, není nutné, aby možnost kompenzací byla upravena přímo v zákoně. Kompenzací se v obdobných případech lze domáhat na základě již existujících zákonných prostředků, které předmětným ustanovením § 31 nejsou jakkoliv dotčeny. Zároveň platí, že pro vydání omezení či zákazu formou opatření obecné povahy budou posuzovány veškeré okolnosti a reálné dopady na trh a podnikatelské prostředí. Z toho důvodu by NÚKIB posuzoval jak životnost jednotlivých technologií, tak

			například možnosti jednotlivých povinných subjektů či postavení dodavatele na českém trhu apod. Dalším důvodem, proč považujeme zákon za ústavně konformní, je podíl Bezpečnostní rady státu na návrhu opatření obecného povahy, kdy se mají možnost k návrhu vyjádřit jednotliví členové Bezpečnostní rady státu, aby bylo dané riziko a jeho dopady posouzeny relevantním orgánem. Připomínka vypořádána.
663. Hospodářská komora ČR	D	Začlenění klíčových ustanovení přímo do zákona HK ČR navrhuje zapracování kritérií pro identifikaci regulované služby (§ 4), způsobu stanovení režimu poskytovatele regulované služby (§ 6 odst. 3), bezpečnostních opatření odpovídajících režimu poskytovatele regulované služby a míru a způsob jejich zavedení a provádění (§14 odst. 2 a 4), a kritérií pro identifikaci strategicky významné služby (§ 27 odst. 1) přímo zákonem. Zákonný legislativní proces poskytuje adresátům právní úpravy adekvátní míru stability regulatorního prostředí i právní jistoty, která je nezbytná pro veškeré soukromé hospodářské aktivity. Zákonná úprava nadto ve smyslu Ústavy České republiky představuje projev vůle lidu skrze jeho řádně zvolené zástupce – vykonavatele zákonodárné moci. Tento způsob úpravy je vhodný pro řešení zásadních otázek regulace, mezi které bez jakékoliv pochybnosti patří i okruh regulovaných subjektů a stanovení jejich zásadních povinností. Naproti tomu úprava obsažená v předkládaném materiálu předpokládá, že otázka okruhu regulovaných subjektů – zejména poskytovatelů regulované služby a poskytovatelů strategicky významné služby – bude řešena pouhým prováděcím právním předpisem. Předkladatelem navrhovaný postup vnáší do otázky okruhu regulovaných subjektů a jejich klíčových povinností prvek volatility a nejistoty, která má z podstaty věci negativní dopad na hospodářskou činnost ve státě. Není navíc jasné, čím je	Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech [§ 3 a § 2 písm. d)], tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby [§ 3, ve spojení s § 2 písm. i) a k) a § 22a]. Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon [§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)], a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá [§ 3 a § 2 písm. b)]. Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i

		odůvodněna zejména potřeba dynamicky a bez užití řádného zákonodárského procesu měnit okruh regulovaných subjektů.	strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Připomínka vypořádána.
664. Hospodářská komora ČR	D	Ačkoli HK ČR vítá návrh zákona jako takový a jako včasnou implementaci Směrnice NIS 2, některá navržená ustanovení zákona mají potenciálně negativní dopad na digitální transformaci klíčových odvětví ekonomiky i státní správy. Zejména pak odvětví uvedená v § 27 návrhu (energetika, doprava a digitální infrastruktura a služby včetně telekomunikačních služeb) by na základě právní nejistoty spojené s povinnostmi strategicky významných služeb mohla ustupovat od digitalizace. Předkladatel počítá s vydáním metodického pokynu o rozsahu dostupnosti strategicky významné služby – provedení ale může být technicky nemožné (například spuštění pokročilých softwarových řešení, která mohou být součástí i kritické části, nemusí být v jiném data centru vůbec možná) nebo mohou ohrožovat obchodní tajemství („zálohové“ systémy mohou provozovatele data center a cloudových řešení nutit ke sdílení obchodních tajemství, nebo k vyhýbání se využití nejlepších možných prostředků digitalizace i v rámci základních řešení). Návrh zákona dále obsahuje nesoulad s transponovanou směrnicí NIS2 (viz konkrétní zásadní připomínky), který může mít negativní vliv na tržní prostředí.	Vysvětleno Není jasné, co konkrétně je předmětem této připomínky, resp. jakým způsobem by ji Úřad měl případně akceptovat; konkrétní připomínky jsou odpovídajícím způsobem vypořádány a důvodová zpráva k ustanovení o zajištění dostupnosti strategicky významných služeb (SVS) bylo upravena dle připomínek HKČR. Význam a smysl institutu zajištění dostupnosti SVS z území ČR je odpovídajícím způsobem zdůvodněn a vysvětlen v relevantních částech důvodové zprávy, a to včetně vymezení relevantních odvětví. Zajištění dostupnosti SVS nebrzdí digitalizaci a nikterak nebrání využívání nejnovějších služeb či aktiv poskytovaných nebo nacházejících se mimo území ČR. Jde pouze o to, aby poskytovatel SVS mohl tuto službu poskytovat ve stanoveném čase a kvalitě z území České republiky - přičemž tyto parametry si poskytovatel nastavuje sám. Návrh neříká, že musí být SVS poskytována výhradně z území ČR v totožné kvalitě jako při běžném provozu (při využití zahraničních prostředků a služeb). Připomínka vypořádána.
665. Hospodářská komora ČR	D	HK ČR oceňuje akceptování řady připomínek z veřejné konzultace a významné věcné úpravy návrhu zákona. Nadále však trvá na tom, aby většina povinností byla stanovena přímo v zákoně nikoli prostřednictvím prováděcích vyhlášek. Stejně tak trvá výhrada k	Vysvětleno Máme za to, že tato zastřešující připomínka má svůj obsah v níže uvedených konkrétních připomínkách a z tohoto důvodu jsou odpovědi a vypořádání

		nedostatečnému definování některých pojmů, u nichž bude přetrvávat aplikační nejistota. Rovněž trvají výhrady k pravidlům hlášení kybernetických bezpečnostních incidentů (§ 16 a násl.). Není totiž zřejmé, zda je možné hlásit pouze významné incidenty nebo zda je nutné hlásit incidenty všechny. Lze se tudíž obávat významné administrativní náročnosti při aplikaci navržených pravidel. Metodická podpora NÚKIB bude zcela zásadní. U neimplementační části zákona týkající se mechanismu prověřování bezpečnosti dodavatelského řetězce zásadní koncepční výhrady přetrvávají, přestože došlo k věcnému posunu oproti verzi zaslané k veřejné konzultaci. Zůstávají například nezodpovězené otázky v oblasti řešení vlastnické struktury dotčených dodavatelů nereflektující zejména existenci soukromoprávních smluvních vztahů mezi poskytovateli regulovaných služeb a dodavateli (včetně možného uplatnění náhrady škod, sankcí atd.).	jednotlivých částí uvedeny u příslušných detailních připomínek. Připomínka vypořádána.
666. Hospodářská komora ČR	D	Návrh zákona sice obsahuje důvodovou zprávu a závěrečnou zprávu RIA, ta ale neobsahuje měření administrativní zátěže podnikatelů dle platné metodiky Ministerstva průmyslu a obchodu z července 2017. Tato metodika je přitom závaznou pro zpracování RIA tak, jak to uvádí na svých stránkách Úřad vlády ČR. Metodika obsahuje vzorovou tabulku pro výpočet administrativní zátěže v právním předpise, kterou předkladatel zjevně nepoužil, aniž by zdůvodnil, proč. Stejně tak neodůvodnil, proč nepoužil výše zmíněnou metodiku. Má-li právní předpis dopadnout na přibližně šest tisíc subjektů z podnikatelské i nepodnikatelské sféry, není možné dopad na ně shrnout větou, že „není z pohledu regulátora možné vyčíslit dopady na rozpočty v podobě absolutního čísla, které by bylo dostatečně přesné. Z obdržených vyplněných dotazníků vyplýval extrémní rozptyl těchto předpokládaných nákladů.“ Předkladatel si mohl v průběhu zpracovávání návrhu zákona provést vlastní reprezentativní průzkum mezi potenciálními subjekty, případně si objednat studii od externího dodavatele, která by pomohla vyčíslit náklady a tak by byla	Neakceptováno Hodnocení dopadů obsahuje hodnocení nákladů z několika různých zdrojů. Rozhodně není hodnocení dopadů shrnuto jednou větou, jak se snaží připomínkové místo naznačit. Veškeré zdroje, metodiky i důvody pro nemožnost stanovení konkrétního výpočtu, který připomínkové místo požaduje, jsou uvedeny napříč hodnocením dopadů, zejm. v kapitole 3.1, resp. ve všech odkazovaných metodikách, ze kterých je výpočet složen. Nad to bylo úřadem provedeno ještě další šetření. Tato metodika nevznikala „na zelené louce“, ale vycházela z metodik dříve prováděných průzkumů NÚKIB a Ministerstva vnitra, které zjišťovaly potřebu finančních zdrojů na kybernetickou bezpečnost pro státní úřady, ministerstva a Úřad vlády ČR. V přípravné fázi byla podoba celého výzkumu včetně teoretických

		zásadním vodítkem pro to, jak záměr předkladatele implementovat směrnici a do zákona vložit národní úpravu bezpečnosti dodavatelského řetězce řešit a jakým způsobem. Místo toho bohužel provedl „dotazníkové šetření“ adresované – jak píše v závěrečné zprávě RIA – orgánům a osobám podle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti. To jsou ale v drtivé většině subjekty veřejné správy. NIS 2 přitom dopadne ve většině na subjekty ze soukromé sféry. Pokud úřad uvádí, že „z obdržených vyplněných dotazníků vyplýval extrémní rozptyl těchto předpokládaných nákladů“, pak je to důvod k provedení analýzy jiným způsobem, nikoli pouze k prostému konstatování toho, co se stalo. HK ČR si dovoluje si upozornit, že například studie think tanku CETA pro Asociaci provozovatelů mobilních sítí odhaduje, že náklady jen v mobilní síti – pokud bude potřeba vyměnit dodavatele v celé části sítě – se mohou vyšplhat až k 17,8 miliardám korun. Není tak možné v Důvodové zprávě říci, že „výši finančních dopadů není možné předem stanovit“. Naopak, je potřeba vytvořit takový analytický podklad, který tyto náklady odhadne. (Shrnutí studie CETA je zde: https://apms.cz/narodni-bezpecnost-chytre-za-stovky-milionu-tupe-za-18-mld/). Už jen tato částka ukazuje, že dopad nového ZKB může být na podnikatelské prostředí extrémně významný a není možné jej v důvodové zprávě nechat nevyčíslený.	východisek konzultována na jednáních se Svazem průmyslu a dopravy ČR, Svazem měst a obcí a Ministerstvem vnitra ČR. Členové výše zmíněných organizací a státní úřady měli možnost se k celému výzkumu s předstihem dostatečně vyjádřit, což v několika případech rovněž udělali. Četné připomínky byly do podoby dotazníkového šetření implementovány. Nicméně ve fázi provádění samotného průzkumu, zaslalo výsledky jen velmi malé procento subjektů oslovených prostřednictvím výše zmíněných organizací. Použitá metodika byla maximálně zaměřena na novou podobu připravované regulace, zohledňovala jak náklady na jednotlivá bezpečnostní opatření, tak otázku personálií a ve všech podstatných rysech se shoduje s metodikou Ministerstva průmyslu a obchodu, na kterou připomínka odkazuje. Uvedené hodnocení dopadů je dostatečné. Co se týká odkazované studie CETA, která je reprezentována pouze dvoustránkovým shrnutím, na které připomínkové místo odkazuje, je třeba uvést, že Úřad opakovaně žádal o poskytnutí podkladů k této studii, jakož i metodiky a dalších relevantních informací. I přes opakované žádosti nebyly tyto informace poskytnuty. S ohledem na to nelze k této studii přihlížet, neboť chybí podstatné informace o tom, jak a na základě čeho byla tato studie zpracována. Připomínka vypořádána.
667. Hospodářská komora ČR	D	Předkladatel uvádí, že součástí návrhu zákona je zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce do českého právního řádu v souladu s usnesením Bezpečnostní rady státu ze dne 21. června 2022 č. 41. Usnesení ani zájem státu podobný mechanismus zavést HK ČR nijak nerozporuje. Zcela ale chybí jakýkoli analytický podklad, ze kterého by bylo patrné, z jakých dat předkladatel vychází a v jakém rozsahu je daný problém přítomný v	Neakceptováno V rámci analýzy dopadů NÚKIB pracoval s maximálním množstvím dostupných dat, přičemž kontaktoval vybrané povinné osoby a svazy za účelem provedení dotazníkových šetření. Vzhledem k nemožnosti tyto dopady blíže vyhodnotit a

	České republice, tedy kolik potenciálně rizikových dodavatelů, na které by mechanismus dopadl, je přítomno v jakých částech infrastruktury subjektů, na které má mechanismus dopadnout. Dle zpráv z médií k podobnému kroku přistoupil například německý regulátor a ministerstvo vnitra, které mají na starosti regulaci kybernetické bezpečnosti. Předkladatel přitom v důvodové zprávě tvrdí: „Nezřídka se navíc stává, že identifikovaná hrozba, před níž Úřad vydal varování podle zákona o kybernetické bezpečnosti, není v analýze rizik povinných osob podle ZKB dostatečně, či dokonce jakkoli, reflektována. Přestože byla vodítka tohoto druhu ze strany správců této infrastruktury dlouhodobě požadována, k reflexi 5G Doporučení jeho adresáty po jeho vydání prakticky nedošlo; mnozí správci kritické informační infrastruktury v sektoru elektronických komunikací nadále uzavírají kontrakty na dodávky technologií do bezpečnostně citlivých částí své infrastruktury s dodavateli, kteří po vyhodnocení kritérií 5G Doporučení na první pohled nevychází jako důvěryhodní.“ Tato tvrzení patří k části zdůvodnění toho, proč chce stát vůbec mechanismus zavést. Z tohoto textu z důvodové zprávy vyplývá, že předkladatel má zjevně z vlastní činnosti k dispozici analýzu reflexe Varování analýzu reflexe 5G Doporučení mezi povinnými subjekty. HK ČR požaduje, aby předkladatel doplnil do důvodové zprávy data z těchto analýz. Dále požaduje, aby předkladatel provedl naprosto základní analýzu současného stavu mezi potenciálními budoucími povinnými subjekty mechanismu, ze které vyplýne: - Jaké dodavatele mají potenciální povinné subjekty v aktivech, u nichž ohodnotili dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní vysoká nebo kritická. - Zda mají v praxi nasazenou mitigaci rizik spojených s dodavatelem, a případně jakou.	specifikovat, což je rovněž způsobeno nemožností předvídat konkrétní dopady navrhované regulace, jsou tyto dopady popsány na určité úrovni obecnosti, kterou však NÚKIB považuje za vhodnou vzhledem k požadavkům na psaní dopadů regulace RIA. Nutno dodat, že konkrétní dopady ke konkrétním subjektům ovšem budou řešeny ve spolupráci s relevantními subjekty (dle § 31) během projednání s relevantními orgány státu. V této fázi budou řešeny také dopady možného omezení nebo zákazu na daný okruh povinných osob. Připomínka vypořádána.

		- Zda zohledňují rizika spojená s dodavatelem, která předkladatel identifikoval v tezích prováděcího právního předpisu a která zveřejnil v „5G Doporučení“. HK ČR je přesvědčena, že bez úplně základní analýzy statu quo není možné přistupovat k jakékoli další regulaci, protože předkladatel vůbec nemůže mít informace o tom, jak jsou v současnosti tato rizika potenciálními povinnými subjekty vnímána ve světle jím vydaných opatření a materiálů, a případně mitigována. Pouze na základě podobné analýzy (a dalších analýz, které HK ČR zmiňuje výše) je možné přistoupit k vhodnému zvolení regulačního nástroje, který má dospět k zamýšlenému efektu při zohlednění zásad proporcionality. Nakonec i v legislativních pravidlech vlády se uvádí, že „přípravě každého právního předpisu musí předcházet podrobná analýza právního a skutkového stavu“.	
668. Hospodářská komora ČR	D	Některé subjekty na trhu elektronických komunikací jsou zároveň držiteli kmitočtových přidělů z aukcí kmitočtů z let 2017 a 2021. Podmínky spojené s přidělem kmitočtů představují například závazek velkoobchodní nabídky, závazek prioritního BB-PPDR, závazek národního roamingu pro PPDR, závazek pronájmu rádiových kmitočtů pro účely průmyslu 4.0, závazky týkající se pokrytí a podobně. HK ČR požaduje doplnit do důvodové zprávy ve spolupráci s ČTÚ předpokládaný vliv mechanismu na plnění těchto závazků.	Neakceptováno NÚKIB v rámci analýzy dopadů pracoval s maximálním množstvím dostupných dat, kvůli čemuž kontaktoval vybrané povinné osoby a svazy za účelem provedení dotazníkových šetření. Vzhledem k nemožnosti tyto dopady blíže vyhodnotit a specifikovat, což je rovněž způsobeno nemožností předvídat konkrétní dopady navrhované regulace, jsou tyto dopady popsány na určité úrovni obecnosti, kterou však NÚKIB považuje za vhodnou vzhledem k požadavkům na psaní dopadů regulace RIA. Konkrétní dopady ke konkrétním subjektům ovšem budou řešeny ve spolupráci s relevantními subjekty (dle § 31) během projednání s relevantními orgány státu. V této fázi budou řešeny také dopady možného omezení nebo zákazu na daný okruh povinných osob Co se týče plnění závazků, tak takové plnění je nutně spojeno se strategicky významnými službami, což je rovněž popsáno dokumentem RIA. Aukční podmínky

			NÚKIB neznemožní, takže by dotčené subjekty měly být nadále schopny plnit. Připomínka vypořádána.
669. Hospodářská komora ČR	Z	Připomínka k § 1 HK ČR požaduje do § 1 návrhu doplnit nové odstavce 4) a 5) takto: „(4) Aniž je dotčen mechanismus součinnosti podle § 60 a povinnosti k jmenování zástupce podle § 67, tento zákon se nevztahuje na osoby, které mají sídlo v jiném členském státě, s výjimkou: d) poskytovatele veřejně dostupné služby elektronických komunikací ^{x)}, e) osoby zajišťující veřejnou komunikační síť ^{x)} a f) následující subjekty, jejichž hlavní provozovna ve smyslu odstavce 5 se nachází v České republice: 1. subjekt poskytující služby registrace jmen domén a poskytovatel regulované služby, který je poskytovatelem služby systému překladu jmen domén (DNS), 2. poskytovatel správy a provozu registru internetových domén nejvyšší úrovně, 3. poskytovatel služby cloud computingu, 4. poskytovatel služby datového centra, 5. poskytovatel služby sítě pro doručování obsahu (CDN), 6. poskytovatel služby on-line tržiště,	Akceptováno jinak Připomínka vychází z premisy, že regulovány mají být pouze subjekty, které mají v České republice sídlo (se speciálním režimem pro poskytovatele veřejných sítí a služeb elektronických komunikací a vybrané poskytovatele služeb v odvětví digitální infrastruktury, k tomu viz dále), přičemž se odkazuje na znění směrnice NIS 2 a jejího čl. 26 odst. 1. Směrnice NIS 2 ale nehovoří o „sídle“, nýbrž o „usazení“ (angl. establishment), a tyto pojmy je třeba odlišovat. Pojem usazení byl zaveden již směrnicí NIS 1, kde byl vykládán funkčně a předpokládal účinný výkon činnosti regulovaného subjektu prostřednictvím stálých struktur, nezávisle na právní formě takové struktury nebo její závislosti na jiných strukturách umístěných mimo území daného státu. Vycházel přitom z práva na usazení definovaného Smlouvou o fungování EU a zahrnoval jak primární usazení, tedy zřízení nebo přesunutí hlavního centra činnosti na území daného státu, tak i sekundární usazení, tedy zřízení zastoupení, pobočky nebo dceřiné společnosti v jiném členském státě EU za současného zachování původního sídla v jiném členském státě. Směrnice NIS 2 zavedený pojem usazení bez dalšího přejímá. I pro potřeby směrnice NIS 2 (srov. bod 114 preambule) a návrhu zákona tak pojem usazení má být vykládán tak, že jde o místo, kde jsou fakticky vykonávány činnosti regulovaného subjektu prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o

	7. poskytovatel služby internetového vyhledávače, 8. poskytovatel služby platformy sociální sítě, 9. poskytovatel řízené služby (MSP), nebo 10. poskytovatele řízené bezpečnostní služby (MSSP). (5) Pro účely tohoto zákona se má za to, že hlavní provozovna subjektu podle odst. 4 písm. b) v Evropské unii je umístěna v členském státě, v němž jsou převážně přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. Nelze-li takový členský stát určit, nebo nejsou-li tato rozhodnutí přijímána v Evropské unii, má se za to, že hlavní provozovna je v členském státě, v němž daný subjekt provádí činnosti k zajištění kybernetické bezpečnosti. Nelze-li takový členský stát určit, má se za to, že dotčený subjekt má hlavní provozovnu v členském státě, v němž má provozovnu s nejvyšším počtem zaměstnanců v Evropské unii. ^{x)} zákon č. 127/2005 Sb., o elektronických komunikacích “ <u>Odůvodnění:</u> Předložený návrh dle názoru HK ČR nedostatečným způsobem implementuje požadavky čl. 26 odst. 1 a 2 směrnice NIS 2. Ačkoliv předkladatel připomínky k nedostatečné implementaci těchto ustanovení čl. 26 odst. 1 a 2 směrnice NIS 2 v rámci veřejné konzultace odmítl, vzhledem k potenciálním negativním dopadům nesprávné implementace na této připomínce HK ČR trvá a považuje ji za zásadní. Navrhuje proto důslednou implementaci tohoto mechanismu ve smyslu čl. 26 odst. 1 a 2 směrnice NIS 2. V rámci vypořádání připomínek odkazoval předkladatel na ust. § 63 a § 67 návrhu zákona. Odkazovaná ustanovení § 63 a § 67 však implementují jen odstavce 3, 4 a 5 článku 26 směrnice NIS 2 a nijak nereflektují požadavky odst. 1 a 2, které představují tzv. one-stop-shop mechanismus, resp. tedy stanovují že některé subjekty (z povahy	pobočku, odštěpný závod nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem. Kritérium usazení může být v určitých případech splněno i v případě, že se v daném státě fyzicky nacházejí síť a informační systémy používané pro výkon regulované služby. Otázka stálého zařízení totiž není ani judikaturou Soudního dvora EU k výkladu svobody usazování přesně definována, může se tak jednat o kancelář, provozovnu, pobočku apod. Stěžejním je požadavek na fyzickou přítomnost dané osoby na území předmětného státu. V praxi pak bude běžné, že jedna osoba bude usazena ve více státech EU současně. Pro vyjasnění situace a větší zesouladění s čl. 26 odst. 1 směrnice NIS 2 bude do návrhu zákona doplněno ustanovení o osobní působnosti zákona (§ 1). Co se týče odkazu na úpravu v současném zákoně reflektující požadavky směrnice NIS 1, je potřeba jej posuzovat ve světle zbylých ustanovení směrnice. Směrnice NIS 1 nepožadovala po členských státech poskytování vzájemné součinnosti, jediná kooperace, která byla vyžadována, byla konzultace dotčených států při určování provozovatelů základní služby. Nebylo potřeba si nad dotčenými subjekty ponechávat dozorovou pravomoc. To se s příchodem směrnice NIS 2 změnilo a Úřad je nucen zvolit takové řešení, které zajistí, aby vzájemná součinnost byla v praxi realizovatelná. Připomínka navrhuje text „aniž je dotčen mechanismus součinnosti podle § 60...“ (pravděpodobně myšlen § 54 - nyní § 57), taková úprava je však podle názoru Úřadu nedostatečná a neopravňuje Úřad vůči dotčeným subjektům na vyžádání orgánu jiného členského státu aktivovat dozorové pravomoci (vzájemná součinnost není v

	poskytovaných služeb) vždy budou podléhat jen jedné národní úpravě v rámci EU (nikoliv tedy jednotlivým národním úpravám v každém členském státě, kde je taková služba poskytována). Ačkoliv by bylo možné vykládat teritoriální aplikovatelnost zákona prostřednictvím přímé aplikace článku 26 směrnice NIS2, nepovažuje HK ČR takový postup za vhodnou legislativní techniku, jelikož může vyvolávat značnou právní nejistotu u adresátů tohoto zákona. HK ČR se domnívá, že vyjasnění aplikovatelnosti zákona žádným způsobem neomezuje princip součinnosti a zástupce ve smyslu odkazovaných ustanovení, která jsou ostatně přímo předvídána v čl. 26 odst. 3 až 5 směrnice NIS 2, a tudíž evropský zákonodárce předpokládal, že tato ustanovení budou existovat vedle sebe. Pro vyloučení pochybností o tom, že mechanismus součinnosti bude i nadále možné uplatňovat požaduje HK ČR doplnit výslovný odkaz. Zároveň platí, že cílem návrhu zákona je implementovat směrnici NIS 2 (k tomu rovněž srov. § 1 odst. 2 návrhu zákona). Předložený návrh zákona nad rámec prosté implementace však obsahuje další povinnosti, které nemusí mít ve směrnici jednoznačnou oporu – např. prověřování dodavatelského řetězce ve smyslu § 28 a násl. návrhu zákona nebo požadavky na zjištění dostupnosti strategicky významných služeb ve smyslu § 34 návrhu zákona. Ačkoliv směrnice NIS 2 vychází z principu minimální harmonizace (srov. čl. 5) a veškeré povinnosti v tomto zákoně by tak měly být vykládány eurokonformně a v mezích směrnice NIS 2, při aplikaci těchto specifických povinností nemusí být zjevné, že na poskytovatele usazené v jiných členských státech EU, se tyto specifické povinnosti neuplatní, a tedy že nepodléhají působnosti českého zákona o kybernetické bezpečnosti. Jinými slovy nemusí být zjevné, že v souladu s čl. 26 odst. 1 a 2 směrnice NIS 2 podléhají jen právní úpravě členského státu, ve kterém mají hlavní provozovnu. V souladu s čl. 26 odstavce 1 a 2 směrnice NIS2 proto HK ČR považuje za klíčové vyjasnit na úrovni zákona, že český zákon o kybernetické bezpečnosti se neuplatní na vybrané subjekty, které jsou usazeny či mají hlavní provozovnu v jiném členském státě či v něm	zásadě o ničem jiném). Aby byl Úřad schopen vzájemnou součinnost poskytnout (např. dožádat po subjektu informaci, provést u něj kontrolu), musí existovat povinnost, která bude předmětem dozorové činnosti Úřadu. Návrh obsažený v připomínce takovou povinnost, a tedy i možnost Úřadu uplatnit na dožádání dozorové pravomoci, nepřináší. Aby však bylo dosaženo záměru směrnice NIS 2, kterým je jednak <i>one-stop-shop</i> pravidlo, jednak harmonizace povinností, které přeshraničně operující subjekty v digitálním odvětví plní, bude vůči těmto subjektům upraven okruh povinností v oblasti zavádění bezpečnostních opatření a hlášení incidentů tak, že bude odkázáno na prováděcí předpis Komise podle čl. 21 odst. 5 a čl. 23 odst. 11 směrnice NIS 2. Tím bude zajištěno, že ačkoli subjekty mají hlavní provozovnu v jiném členském státě, budou formálně vzato vázány českými národními povinnostmi (za účelem toho, aby nad nimi mohl Úřad na vyžádání vykonat dozorovou činnost), budou jimi vázány jen v rozsahu harmonizujících předpisů, kterými bude subjekt vázán i ve státě, do jehož jurisdikce v souladu s čl. 26 odst. 1 písm. b) směrnice NIS 2 spadá. Zároveň však tato úprava nevylučuje, aby Úřad tam, kde je to otázkou národní bezpečnosti (tedy výlučné pravomoci členských států, do které unijní právo nemůže zasahovat), mohl dotčené subjekty zavázat svým rozhodnutím nebo opatřením obecné povahy i nad rámec povinností vyplývajících z prováděcích aktů Komise. Připomínka vypořádána.

	poskytují své služby, a proto podléhají právnímu řádu tohoto členského státu. HK ČR navrhuje stanovit, že zákon se nevztahuje na poskytovatele usazené v jiném členském státě, ledaže naplňují některou z výjimek stanovených v čl. 26 odst. 1 směrnice NIS 2, jak jsou navrženy implementovat do nového odstavce 4. V souladu s čl. 26 směrnice NIS 2 se český zákon o kybernetické bezpečnosti tak uplatní pouze na:					
	<table><tr><th>Článek 26 odst. 1 směrnice NIS 2</th><th>Článek 18 odst. 1 směrnice NIS 1</th></tr><tr><td>Má se za to, že subjekty spadající do oblasti působnosti této směrnice podléhají pravomoci členského státu, v němž</td><td>Pro účely této směrnice se má za to, že poskytovatel digitálních služeb podléhá pravomoci členského státu, v němž je primárně usazen.</td></tr></table>	Článek 26 odst. 1 směrnice NIS 2	Článek 18 odst. 1 směrnice NIS 1	Má se za to, že subjekty spadající do oblasti působnosti této směrnice podléhají pravomoci členského státu, v němž	Pro účely této směrnice se má za to, že poskytovatel digitálních služeb podléhá pravomoci členského státu, v němž je primárně usazen.	
Článek 26 odst. 1 směrnice NIS 2	Článek 18 odst. 1 směrnice NIS 1					
Má se za to, že subjekty spadající do oblasti působnosti této směrnice podléhají pravomoci členského státu, v němž	Pro účely této směrnice se má za to, že poskytovatel digitálních služeb podléhá pravomoci členského státu, v němž je primárně usazen.					

		jsou usazeny, s výjimkou těchto případů: [....] Má-li poskytovatel digitálních služeb v některém členském státě své sídlo, má se za to, že je v tomto členském státě rovněž primárně usazen. - osoby sídlící v České republice, které naplní definici poskytovatele regulované služby (standardní teritoriální princip již implementovaný v návrhu zákona). - poskytovatele veřejně dostupné služby elektronických komunikací, který v souladu se zákonem o elektronických komunikacích poskytuje služby na území České republiky (čl. 26 odst. 1 písm. a) směrnice NIS 2); - osoby zajišťující veřejnou komunikační síť v souladu se zákonem o elektronických komunikací na území České republiky (čl. 26 odst. 1 písm. a) směrnice NIS 2); a - ty poskytovatele specifikovaných služeb, kteří mají hlavní provozovnu na území České republiky, požaduje HK ČR implementovat v odst. 4 písm. c) bodech 1 až 10 návrhu (čl. 26 odst. 1 písm. b) směrnice NIS 2). Pro úplnost HK ČR uvádí, že obdobným způsobem byla z působnosti dosavadní směrnice „NIS 1“ (směrnice (EU) 2016/1148) vyňata aplikovatelnost na poskytovatele digitálních služeb. Pro srovnání: Článek 18 odst. 1 směrnice NIS 1 byl přitom implementován ve stávajícím znění zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, následovně: „<i>Tento zákon se nevztahuje na poskytovatele digitální služby, který má sídlo v jiném členském státě.</i>“ (srov. § 33 odst. 4 zákona č. 181/2014 Sb.).	
670. Hospodářská komora ČR	Z	Připomínka k § 2	Neakceptováno

		HK ČR ve vazbě na obsah § 28 odst. 3 písm. b) a nebude-li akceptována níže uvedená připomínka požadující vypuštění celého Dílu 5, požaduje, aby byl text § 2 upraven ve smyslu níže uvedeného odůvodnění. <u>Odůvodnění:</u> HK ČR požaduje, aby v § 2 byly definovány všechny pojmy uvedené v § 28 odst. 3 písm. b), především pak bod 3, který není vymezen (definován) nijak. „Informační či komunikační služba“ je přitom extrémně vágní pojem, který je potřeba definovat zcela jasně. Nesplnění požadavků vyplývajících ze zákona s sebou nese vysoké riziko pokut, takže HK ČR předpokládá, že povinné subjekty by v rámci regulační opatrnosti předkladatele informovaly o všech dodavatelích, kteří se mohou být jen dotknout kritické části stanoveného rozsahu, mezi nimiž by při extenzivním výkladu pojmu „informační či komunikační služba“ mohly být třeba poskytovatelé služeb Public Relations (poskytují „komunikační“ služby managementu organizace, který může být „kritickou součástí stanoveného rozsahu“). I při méně extenzivním výkladu pojmu „informační či komunikační služba“ může do těchto služeb spadat například pronájem nenasvíceného vlákna, jejichž riziko narušení bezpečnosti informací může být ohodnoceno na úroveň vysoká nebo kritická, ale nikoli z důvodů kyberútoku, ale fyzického přerušení, což ale vůbec nesouvisí s tím, kdo je dodavatelem onoho vlákna.	Bližší vymezení pojmů § 29 odst. 3 písm. b) není žádoucí pro účel právní úpravy. Informační či komunikační služby je běžně zaužívaným neurčitým pojmem, se kterým pracovalo i předchozí znění zákona a doposud se tento pojem nejevil jako problematický. Informační nebo komunikační službou jsou pak například služby cloud computingu nebo řízené služby. Informování úřadu o všech dodavatelích, kteří se mohou podílet na dodávání služby do kritické části stanoveného rozsahu, ať už sebemenším dílem, je však cílem úpravy proto, aby Úřad měl informace o těchto dodavatelích a mohl vyhodnocovat rizika s nimi související. V případě pochybností s plněním povinnosti hlášení dodavatelů se pak mohou povinné subjekty obracet na Úřad. Obdobných pojmů také užívá například i zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Připomínka vypořádána.
671. Hospodářská komora ČR	Z	Připomínka k § 2 odst. 1 písm. a) HK ČR požaduje upravit text takto: <i>„a) aktivem primární aktiva a podpůrná aktiva relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování nebo likvidace informací a dat v elektronické podobě,“</i> <u>Odůvodnění:</u>	Akceptováno jinak Text byl upraven: <i>„aktivem primární aktiva a podpůrná aktiva relevantní pro zpracování informací a dat v elektronické podobě, a to včetně likvidace“.</i> Připomínka vypořádána.

		Likvidace informací a dat je jednou z klíčových oblastí správy informačních aktiv.	
672. Hospodářská komora ČR	Z	Připomínka k § 2 odst. 1 písm. b) HK ČR požaduje upravit text takto: <i>„b) primárním aktivem informace a služby, přičemž informacemi se rozumí také data, včetně provozních a lokalizačních údajů, a službou se rozumí také procesy,“</i> a současně požaduje v důvodové zprávě vymezit, o jaké procesy se jedná v případě služby. <u>Odůvodnění:</u> Vedle provozních údajů jsou lokalizační údaje důležitým atributem dat a informací. Navíc je zde vazba na zákon o elektronických komunikacích. Jasně vymezení pojmu alespoň v důvodové zprávě pomůže aplikační praxi. Z textu návrhu není jasné, o jaké procesy se jedná, zda např. o procesy vedoucí k zajištění DDI regulované služby.	Akceptováno jinak Na základě četných podnětů se vracíme k původní (současné) definici aktiv („primárním aktivem informace a služby“). Lokalizační údaje budou zmíněny a případně upřesněny v odůvodnění návrhu vyhlášky v souladu s Vaší připomínkou. Připomínka vypořádána.
673. Hospodářská komora ČR	Z	Připomínka k § 2 odst. 2 písm. f) a g) HK ČR požaduje upravit definiční vymezení pojmu „kybernetický bezpečnostní incident“ ve vazbě na vyloučení úmyslného zavinění (např.: <i>kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v rámci aktiv, s výjimkou případů, kdy lze s jistotou vyloučit úmyslné zavinění</i>), a to ve smyslu níže uvedeného odůvodnění. <u>Odůvodnění:</u> HK ČR rozumí, že poskytovatelé v režimu vyšších povinností nemají povinnost hlásit předkladateli tzv. provozní incidenty, které z povahy věci pod působnost předkladatele nespádají a incidenty, u kterých lze s jistotou vyloučit úmyslné zavinění a které nemají pro vyhodnocování ze strany předkladatele a další mapování bezpečnostní	Akceptováno jinak Definice kybernetického bezpečnostního incidentu zůstala v návrhu zachována, došlo nicméně k úpravě formulace § 16 odst. 1 na „Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a nejsou způsobeny vlastní provozní činností.“. Povinnost poskytovatele regulované služby v režimu vyšších povinností se proto nově nevztahuje na kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a zároveň jsou způsobeny vlastní provozní činností.

		situace v kybernetickém prostoru zásadnější význam. Současně je definováno v § 16, odst. 1, že subjekty mají povinnost hlásit pouze incidenty, které vznikly v kyberprostoru. Tato znění vyčleňuje z povinnosti incidenty, které vznikly úmyslným zaviněním a případnou chybou samotného subjektu, např. při plánovaných pracích. Takto vyznívá i důvodová zpráva k návrhu zákona. V tomto smyslu by bylo tedy vhodné upravit formulace samotného pojmu „kybernetický bezpečnostní incident“. NCSC definuje kybernetický incident jako porušení bezpečnosti aktiva (systému) s cílem ovlivnit jeho integritu nebo dostupnost nebo neoprávněný přístup nebo pokus o neoprávněný přístup k aktivu (systému) s cílem porušit jeho důvěrnost. HK ČR doporučujeme využít Metodiku k hlášení kybernetického bezpečnostního incidentu předkladatele: https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni-incidentu_1.1.pdf, která uvádí: Kybernetický bezpečnostní incident není potřeba Úřadu hlásit v případě, kdy došlo v důsledku technického selhání k nedostupnosti části aktiv, lze s jistotou vyloučit úmyslné zavinění (zejména útočníkem). Zároveň HK ČR doporučuje vyloučit ze současné Metodiky podmínku řádného fungování záložních systémů: „...a zároveň řádné zafungování k nim záložních (redundantních, zdvojených) aktiv zabránilo vzniku nedostupnosti systému jako celku.“ Cílem je hlášení incidentů, kde nelze vyloučit úmyslné zavinění bez ohledu na dostupnost.	Zahrnutí úmyslu mezi proměnné určující, zda incident bude hlášen či nikoli, bylo zvažováno a bylo zavrženo z důvodu, že zjišťování úmyslu by kladlo na povinné subjekty neúměrnou zátěž (nadto ve chvíli, kdy je jejich primárním zájmem zvládnutí probíhajícího incidentu a nikoli zjištění, zda incident mohl být zaviněn úmyslně). Pokud jde o doporučení ohledně uvedené metodiky, k obsahu doporučení bude přihlédnuto při tvorbě nové metodiky, která bude založena na návrhu zákona, bude-li přijat. Po vypořádání: Ustanovení bylo v rámci vypořádání připomínek upraveno následovně: „<i>Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a nelze u nich ve lhůtě podle § 17 odst. 1 vyloučit úmyslné zavinění.</i> Připomínka vypořádána.
674. Hospodářská komora ČR	Z	Připomínka k § 2 odst. 2 písm. h) HK ČR požaduje zpřesnit vymezení pojmu „významný dodavatel“ ve smyslu níže uvedeného odůvodnění. <u>Odůvodnění:</u>	Neakceptováno Chápeme Váš požadavek na podrobnější definici významného dodavatele, ale bohužel její zpřesnění přináší více problémů, než její obecné znění, které vychází z performativnosti kybernetické regulace a je tím pádem navázáno na řízení rizik v organizaci.

		Z hlediska aplikační praxe není uvedená definice jednoznačná a bude (podle názoru HK ČR) působit praktické problémy. Je tedy na místě požadovat, aby definiční vymezení významného dodavatele (jako účastníka „právního vztahu, který je významný z hlediska bezpečnosti informací ve stanoveném rozsahu řízení kybernetické bezpečnosti“, bylo výrazně návodnější.	Definice dává povinným subjektům možnost nastavení vlastních kritérií pro jejich určení prostřednictvím politiky řízení dodavatelů, ve které mají povinné osoby stanovit pravidla a principy pro jejich výběr. Žádná organizace není stejná (má odlišné procesy), dopadají na ně rozdílné hrozby a rizika. Po diskuzích s odbornou veřejností jsme se přiklonili k tomu, že definici necháme obecnou. Připomínka vypořádána.
675. Hospodářská komora ČR	Z	Připomínka k § 3 HK ČR požaduje obsah § 3 přeformulovat tak, aby věcně kopíroval směrnici NIS 2 a stávající předpisy, a v souvislosti s tím doplnit důvodovou zprávu o příslušné vysvětlení, které nebude vyústit v rozpor se směrnicí NIS 2. <u>Odůvodnění:</u> Článek 26 směrnice NIS 2 obsahuje zvláštní pravidla pro příslušnost a územní příslušnost. Ve vztahu k poskytovatelům služeb DNS, registrům názvů domén nejvyšší úrovně, subjektům poskytujícím služby registrace názvů domén, poskytovatelům služeb cloud computingu, poskytovatelům služeb datových center, poskytovatelům sítí pro doručování obsahu, poskytovatelům řízených služeb, poskytovatelům řízených bezpečnostních služeb, jakož i poskytovatelům on-line tržišť, on-line vyhledávačů nebo platform služeb sociálních sítí (dále jen "poskytovatelé") stanoví čl. 26 odst. 1 písm. b) směrnice NIS 2 mechanismus jednoho správního místa, podle něhož poskytovatelé spadají do jurisdikce členského státu, v němž mají hlavní provozovnu v EU. Toto pravidlo je třeba vykládat tak, že poskytovatelé podléhají výlučně právu pouze jednoho členského státu a řídí se jím, i když poskytují služby v jiných členských státech. Současně čl. 26 odst. 5 směrnice NIS 2 stanoví povinnosti vzájemné	Akceptováno jinak Pro vyjasnění situace a soulad s čl. 26 odst. 1 směrnice NIS2 bude do návrhu zákona doplněno ustanovení o osobní působnosti zákona. Co se týče odkazu na úpravu v současném zákoně reflektující požadavky směrnice NIS1, je potřeba jej posuzovat ve světle zbylých ustanovení směrnice. Směrnice NIS1 nepožadovala po členských státech poskytování vzájemné součinnosti, jediná kooperace, která byla vyžadována, byla konzultace dotčených států při určování provozovatelů základní služby. Nebylo tedy potřeba si tedy nad dotčenými subjekty ponechávat dozorovou pravomoc. To se s příchodem směrnice NIS2 změnilo a Úřad je nucen zvolit takové řešení, které zajistí, aby vzájemná součinnost byla v praxi realizovatelná. Připomínka neobsahuje žádný návrh řešení této situace, jiná připomínková místa navrhovala nedostatečné úpravy, neboť návrhy neumožňovaly Úřadu vůči dotčeným subjektům na vyžádání orgánu jiného členského státu aktivovat dozorové pravomoci (vzájemná součinnost není v zásadě o ničem jiném). Aby byl Úřad schopen

	pomoci mezi orgány dohledu s pravomocí nad poskytovateli a orgány dohledu v jiných členských státech. HK ČR se domnívá, že návrh zákona plně neprovádí mechanismus jednoho správního místa, jak je stanoven v článku 26 směrnice NIS 2. Konkrétně se jedná o čl. 26 odst. 5 směrnice NIS 2, který se provádí v § 54 návrhu zákona. Podle tohoto ustanovení má Agentura omezenou dozorovou pravomoc nad poskytovateli, kteří mají hlavní provozovnu v jiných členských státech než v České republice (dále jen "poskytovatelé z jiných členských států"). To potvrzuje i důvodová zpráva k § 54 návrhu zákona. Čl. 26 odst. 1 písm. b) směrnice NIS 2 se však do návrhu zákona nenavrhuje implementovat v plném rozsahu. Podle důvodové zprávy k § 3 návrhu zákona se návrh zákona vztahuje na všechny poskytovatele regulovaných služeb usazené v České republice nebo poskytující služby do České republiky, a to včetně poskytovatelů z jiných členských států. Ve vypořádání připomínek ze dne 10. března 2023 předkladatel reagoval na podobně formulovanou připomínku s tím, že tato úprava je v souladu s článkem 26 směrnice NIS 2 a navrhovaná úprava je nezbytná k zajištění toho, aby předkladatel měl požadovanou dozorovou pravomoc při poskytování součinnosti dozorovým orgánům s působností nad poskytovateli z jiných členských států. Takové vypořádání HK ČR nepovažuje za zcela správné, neboť nerozlišuje mezi: a) použitelností věcného předpisu a b) dozorovou pravomocí předkladatele. Konkrétně se jedná o následující: - Návrh zákona se vztahuje na všechny poskytovatele regulovaných služeb usazené v České republice nebo poskytující služby do České republiky, tedy i na poskytovatele z jiných členských států. To znamená, že poskytovatelé z jiných členských států budou muset dodržovat veškerá nařízení podle návrhu zákona a návrhů aktů v přenesené pravomoci. To zároveň znamená, že i kdyby některý z poskytovatelů z jiných členských států jednal v souladu s hmotněprávní úpravou	vzájemnou součinnost poskytnout (např. požádat po subjektu informaci, provést u něj kontrolu), musí existovat povinnost, která bude předmětem dozorové činnosti Úřadu. Aby však bylo dosaženo záměru směrnice NIS2, kterým je jednak one-stop-shop pravidlo, jednak harmonizace povinností, které přeshraničně operující subjekty v digitálním odvětví plní, bude vůči těmto subjektům upraven okruh povinností v oblasti zavádění bezpečnostních opatření a hlášení incidentů tak, že bude odkázáno na prováděcí předpis Komise podle čl. 21 odst. 5 a čl. 23 odst. 11 směrnice NIS2. Tím bude zajištěno, že ačkoli subjekty mající hlavní provozovnu v jiném členském státě budou formálně vzato vázány českými národními povinnostmi (za účelem toho, aby nad nimi mohl Úřad na vyžádání vykonat dozorovou činnost), budou jimi vázány jen v rozsahu harmonizujících předpisů, kterými bude vázán i ve státě, do jehož jurisdikce v souladu s čl. 26 odst. 1 písm. b) směrnice NIS2 spadá. Zároveň však tato úprava nevylučuje, aby Úřad tam, kde je to otázkou národní bezpečnosti (tedy výlučné pravomoci členských států, do které unijní právo nemůže zasahovat), mohl dotčené subjekty zavázat svým rozhodnutím nebo opatřením obecné povahy i nad rámec povinností vyplývajících z prováděcích aktů Komise. Připomínka vypořádána.

		členského státu, v němž má hlavní provozovnu, ale nikoliv v souladu s hmotněprávní úpravou v České republice, jednalo by se o porušení českého práva. - I když by takový poskytovatel z jiného členského státu pravděpodobně nebyl sankcionován vzhledem k omezené dozorové pravomoci předkladatele, stále by jednal protiprávně, což by mohlo představovat významný problém zejména pro poskytovatele služeb větším společnostem a státním orgánům v České republice, kteří obvykle vyžadují plné dodržování všech právních povinností. Na základě výše uvedených skutečností považuje HK ČR navrhované řešení za nevhodné a návrh zákona za rozporný se zamýšleným účelem směrnice NIS 2. Jak bylo uvedeno výše, navrhované řešení by vyžadovalo, aby subjekty splnily všechny platné povinnosti podle návrhu zákona a návrhů aktů v přenesené pravomoci. HK ČR rovněž poznamenává, že navrhované řešení představuje podstatné rozšíření působnosti české právní úpravy kybernetické bezpečnosti. Ustanovení § 33 odst. 4 stávajícího zákona o kybernetické bezpečnosti výslovně stanoví, že se zákon o kybernetické bezpečnosti nevztahuje na poskytovatele digitálních služeb usazené v jiném členském státě.	
676. Hospodářská komora ČR	Z	Připomínka k § 4 odst. 1 a odst. 2 HK ČR požaduje upravit text § 4 v odst. 1 a 2 takto: <i>„(1) Kritéria pro identifikaci regulované služby jsou tvořena kritériem služby a kritériem poskytovatele regulované služby. Kritéria pro identifikaci regulované služby stanoví ~~prováděcí právní předpis vláda nařízením.~~</i> <i>(2) ~~Prováděcí právní předpis~~ Nařízení vlády stanoví kritéria pro identifikaci regulované služby v těchto odvětvích“</i> <u>Odůvodnění:</u>	Neakceptováno Právní forma nařízení vlády není pro danou regulaci odpovídající. Stanovení okruhu povinných osob, jejich režimu a dalších ustanovení pro něž je vydáván prováděcí právní předpis je analogicky nejpodobnější současnému nastavení vyhlášky č. 4372017 Sb., o kritériích pro stanovení provozovatelů základní služby, což je spolu s § 22a současného zákona o kybernetické bezpečnosti způsob stanovení osobní působnosti transpozičních ustanovení předchozí směrnice NIS1. Stejným způsobem je tedy

		Původní znění umožňuje předkladateli, aby na základě vlastního uvážení rozhodoval o okruhu jím regulovaných subjektů, přičemž zákon nevylučuje, aby tento okruh byl rozšířen na libovolný subjekt v rámci vyjmenovaných odvětví. Taková míra koncentrace pravomocí v rukou jednotlivého orgánu veřejné správy je v demokratickém a právním státě nepřijatelná. Navrhovaná změna má za cíl přenést pravomoc určování rozsahu působnosti zákona o kybernetické bezpečnosti na Vládu ČR obdobně jako v případě nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které v současnosti určuje prvky infrastruktury, na něž dopadá nejpřísnější režim regulace dle zákona o kybernetické bezpečnosti.	přístupováno k transpozici směrnice NIS2 - podstata věci se i přes rozdílnost směrnic v tomto případě nijak nemění. Stanovení okruhu povinných osob prostřednictvím prováděcího právního předpisu na základě a v mezích zákona (jak vyplývá z čl. 79 odst. 3 Ústavy) je v působnosti Úřadu. Z tohoto důvodu také není využito nařízení vlády, které má být využito jen v situacích, kdy se věc týká působnosti více než dvou orgánů nebo je dán naléhavý obecný zájem, což v tomto případě provedení běžného ustanovení zákona není. Stejně jako v případě dříve zaslaných podnětů v rámci neoficiálního připomínkového řízení je potřeba opět upozornit, že domněnka navrhovatele, že je Úřadu dána pravomoc „na základě vlastního uvážení rozhodoval o okruhu jím regulovaných subjektů, přičemž zákon nevylučuje, aby tento okruh byl rozšířen na libovolný subjekt v rámci vyjmenovaných odvětví“ je mylná, protože přijímání každého právního předpisu je podmíněno řádně provedeným legislativním procesem, který umožňuje zapojení široké skupiny připomínkových míst, stejně jako v tomto případě. Připomínka vypořádána.
677. Hospodářská komora ČR	Z	Připomínka k § 6 odst. 3 HK ČR požaduje, aby byl text § 6 odst. 3 upraven takto: <i>„(3) Režim poskytovatele regulované služby je stanoven ~~prováděcím právním předpisem~~ v příloze tohoto zákona. Je-li orgán nebo osoba poskytující regulovanou službu určen rozhodnutím Úřadu podle § 5, je vždy poskytovatelem regulované služby v režimu vyšších povinností.“</i> <u>Odůvodnění:</u>	Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech (§ 3 a § 2 písm. d)), tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby (§ 3, ve spojení s § 2 písm. i) a k) a § 22a). Obdobný způsob stanovení

		Požadavek reflektuje aplikaci principu právní a regulační jistoty.	povinných osob obsahuje také současný krizový zákon (§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)), a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá (§ 3 a § 2 písm. b)). Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona o kybernetické bezpečnosti. Připomínka vypořádána.
678. Hospodářská komora ČR	Z	Připomínka k § 9 odst. 1 HK ČR požaduje výslovně stanovit, že se za změnu považuje i výmaz, resp. ukončení regulované služby. Alternativně HK ČR navrhuje nastavení podmínek a lhůty v § 11. <u>Odůvodnění:</u> Ustanovení § 9 odst. 1 nestanovuje, jak provést změnu registrace poskytovatele regulované služby směrem k podání oznámení výmazu (ukončení) regulované služby. Obecně § 9 řeší pouze registraci dalších služeb a změny režimu, avšak nezabývá se možností oznámení změn ve formě ukončení regulované služby. Navazující § 11 sice stanovuje postup výmazu z evidence poskytovatelů regulovaných služeb z pohledu předkladatele materiálu, ale nestanovuje proces	Akceptováno jinak Výmaz z evidence regulovaných služeb není změnou registrace a subjekty záměrně samy nemohou přes portál službu z evidence smazat. Úprava výmazu je stanovena v samostatném ustanovení. Na základě této, ale i dalších souvisejících připomínek, došlo k tomu, že bude umožněn výmaz z evidence na žádost poskytovatele regulované služby. Do výmazu regulované služby z evidence však platí fikce, že se na službu zapsanou v evidenci vždy hledí jako na regulovanou službu. Poskytovatel regulované služby tudíž musí plnit vůči této službě všechny povinnosti plynoucí mu ze zákona. Připomínka vypořádána.

		(postup) podání oznámení změn z pohledu poskytovatele, pokud již nejsou plněna příslušná kritéria. Cílem je umožnit, aby činnost, která odpadne, mohla být formálně ihned zrušena a poskytovateli nevznikaly další náklady.	
679. Hospodářská komora ČR	Z	Připomínka k § 10 odst. 2 HK ČR požaduje, aby byl text § 10 odst. 2 upraven takto: <i>„(2) Poskytovatel regulované služby zapsaný v evidenci poskytovatelů regulovaných služeb je povinen plnit všechny povinnosti plynoucí mu ze zákona vůči zapsaným regulovaným službám nejpozději od uplynutí šesti měsíců od okamžiku doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb až do okamžiku doručení vyrozumění o výmazu z evidence poskytovatelů regulovaných služeb podle § 11.“</i> <u>Odůvodnění:</u> Je třeba přijmout dostatečnou lhůtu k tomu, aby byl subjekt vůbec schopen plnit požadované povinnosti vyplývající ze zákona tak, aby obstál při případné kontrole. Z tezí vyhlášek vyplývá, že některé povinnosti budou poskytovatelé regulovaných služeb v režimu vyšších povinností muset realizovat pomocí zaměstnanců či kontraktorů s konkrétními znalostmi a dovednostmi, které nemusí být v dané organizaci dosud vůbec přítomny. Navíc musí dojít k revizi smluv s dodavateli a k další řadě plnění, které zajistí compliance. U menších poskytovatelů služeb elektronických komunikací může být velká komplikace vůbec nalézt vhodné lidi – pokud se předpokládá, že po datu účinnosti zákona bude podobné subjekty poptávat velká část nově regulovaných subjektů, nemusí se na ně vůbec dostat. Je potřeba si uvědomit, že předkladatel bude regulovat nově až 2000 subjektů v odvětví elektronických komunikací, z nichž řada jsou mikropodniky v odlehlých venkovských oblastech.	Vysvětleno Den doručení písemného vyrozumění o zápisu do evidence regulovaných služeb je rozhodným datem, se kterým celý zákon pracuje i na jiných místech a počítá se od něj běh některých lhůt. Například jedna z hlavních povinností zavádět bezpečnostní opatření má na zavedení podle § 14 odst. 3 návrhu zákona lhůtu v délce jednoho roku a začíná běžet od tohoto rozhodného data. Neplatí tedy, že by tato povinnost začala platit ihned po doručení vyrozumění o zápisu do evidence. Toto ustanovení pouze říká, že od vyrozumění zápisu do evidence platí, že daná služba je regulovanou službou a poskytovatel regulované služby vůči ní musí plnit své povinnosti. Jednotlivé povinnosti pak vyplývají z dalších ustanovení a mají své samostatné lhůty. Připomínka vypořádána.
680. Hospodářská komora ČR	Z	Připomínka k § 12	Vysvětleno

		HK ČR požaduje upravit text § 12 ve smyslu níže uvedeného odůvodnění. <u>Odůvodnění:</u> Je na místě z požadovaných údajů vynechat ty údaje, které má předkladatel dostupné v základních registrech (tady je i vazba na prováděcí vyhlášku – například informace o vlastnické struktuře viz požadavek § 3 Vyhlášky o portálu NÚKIB). Portál NÚKIB by měl být napojen na základní registry, tudíž by registrační a doplňující údaje měly být z velké části, ne-li všechny, na těchto registrech dostupné.	Počítáme s tím, že dojde k napojení na základní registry a k čerpání maximálního množství údajů z nich, tak aby docházelo k minimální administrativní zátěži regulovaných organizací. Nicméně náležitosti formulářů musí být ve vyhlášce specifikovány tak či tak (vyplývá to z judikatury Ústavního soudu, která je zmíněna v důvodové zprávě). Takto je navíc transparentní, které údaje NÚKIB ze základních registrů získává a dále zpracovává. Výčet potřebných údajů je nezbytné ve vyhlášce v této podobě zachovat také pokud by se Portál Úřadu nepodařilo napojit na základní registry k okamžiku účinnosti návrhu zákona. Připomínka vypořádána.
681. Hospodářská komora ČR	Z	Připomínka k § 13 odst. 3 HK ČR požaduje upravit text § 13 odst. 3 takto: <i>„(3) O provedení identifikace a určení organizačních částí a aktiv podle odstavce 1 vede poskytovatel regulované služby dokumentovaný záznam, a to včetně evidence primárních aktiv, která byla ze stanoveného rozsahu vyjmuta, a odůvodnění jejich vyjmutí.“</i> <u>Odůvodnění:</u> Důvodová zpráva v prvním odstavci uvádí, že subjekty, které již nyní postupují podle platného a účinného zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti v procesu stanovování rozsahu řízení, budou mít situaci výrazně ulehčenou, jelikož nový postup pouze zpřesňuje již zavedenou praxi. Tuto tezi však vyvrací nová povinnost, kterou poskytovatelům ukládá právě § 13 v odst. 3, kde se nad rámec popsaného a standardního procesu jednotlivých kroků identifikace nastavuje povinnost naprosto opačná, a to popsání a zdokumentování argumentace, proč daná aktiva nebyla zařazena.	Neakceptováno Stanovený rozsah se vztahuje na aktiva související s regulovanou službou (nikoliv na všechna identifikovaná primární aktiva - pokud všechna nesouvisí s regulovanou službou). Je pracováno s typovými aktivy, nikoliv s každou službou/informací jako takovou zvlášť. Jde o základní identifikaci služeb, které organizace poskytuje (za jakým účelem je vytvořena a co jsou její zásadní služby). Primární aktiva, která nesouvisí s regulovanou službou není potřeba hodnotit (nZKB to nepožaduje). Nepovažujeme tuto změnu při identifikaci aktiv za nepřiměřenou. Je pravda, že v tomto ustanovení se projevují zkušenosti Úřadu z kontrolní činnosti, kdy správně stanovit rozsah ISMS organizací způsobuje značné problémy. Oproti platné právní úpravě došlo k otočení způsobu identifikace primárních aktiv, na které se nyní pohlíží z pohledu celé organizace a určují

		V požadavcích návrhu nového zákona a prováděcích právních předpisů je však stanovena povinnost jasně popsat i předchozí kroky, které k zařazení aktiva vedou. Pro dokumentaci a doložení argumentů, proč dané aktivum nebylo zařazeno, tedy dostačuje interpretace popisu aktiva v předchozích krocích celého procesu. Popis nad rámec tohoto přináší administrativní zátěž subjektům a nepřináší přidanou hodnotu předkladateli.	se ty, které souvisejí s regulovanou službou. Nesouhlasíme s tím, že pro zajištění kybernetické bezpečnosti současné znění předmětného ustanovení nebude mít vliv, a že se jedná o nepřiměřený zásah do práv povinných subjektů. Naopak, naší snahou je zmírnění požadavku NIS2 zavádět opatření na celou organizaci v tom smyslu, že se prvně podívám na celou organizaci ale opatření zavádím na těch aktivech, které se přímo dotýkají poskytování regulované služby. Připomínka vypořádána.
682. Hospodářská komora ČR	Z	Připomínka k § 14 odst. 1 HK ČR požaduje upravit text takto: <i>„(1) Bezpečnostními opatřeními se rozumí úkony, jejichž cílem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv. ~~Bezpečnostními opatřeními jsou organizační a technická opatření.~~“</i> <u>Odůvodnění:</u> Dle § 14 jsou bezpečnostními opatřeními organizační a technická opatření. HK ČR vnímá argumentaci předkladatele, že pro režim vyšších povinností jsou nastavena přísnější pravidla, zároveň není jasné, proč nelze – minimálně fakultativně – nastavit organizační a technická opatření i pro služby v režimu nižších povinností. V případě holdingu může totiž dojít k situaci, kdy některé společnosti spadnou do režimu vyšších a jiné do režimu nižších povinností. Zpravidla se však pro celý holding zpracovává jednotná řídicí dokumentace a bude poměrně náročně vést dvojkolejnou dokumentaci – organizační a technická opatření pro vyšší režim a bezpečnostní opatření pro režim nižší. Ideální by bylo zachovat možnost stejného rozdělení pro oba režimy, ale věcný rozsah upravit dle typu režimu.	Neakceptováno Jednotlivá ustanovení návrhu vyhlášky pro režim nižších povinností kombinují oba typy bezpečnostních opatření, z toho důvodu nebylo účelné je rozdělovat na organizační a technická. Toto řešení nemění podstatu bezpečnostních opatření, dále bylo cílem regulátora zpracovat přehledný a srozumitelný předpis, kdy bude na první pohled jasné, jaká všechna bezpečnostní opatření se váží k dané oblasti (např. BCM, obsahuje jak organizační, tak technická bezpečnostní opatření) - všechna BO ke BCM jsou tak přehledně uvedena v jednom ustanovení. Je jedno, jak budou mít dokumentaci označenou, podstata opatření zůstává stejná, pro plnění zákonných povinností není důležité, zda jsou jednotlivá BO definována v interní dokumentaci jako technická nebo organizační, ale je důležité, zda jsou fakticky zaváděna. Pro lepší pochopení byl upraven § 15 odst. 2 aby bylo jasné, že BO pro režim nižších povinností jsou organizačního a technického typu, i když nejsou rozdělena samostatně, jako je tomu v režimu vyšších povinností, z důvodů uvedených výše. Praktičnosti

			nastavení jednotného přístupu v rámci holdingu rozumíme a nevidíme to v tom v budoucnu aplikační problém. Rádi bychom i k této problematice vydali samostatnou metodiku, která bude porovnávat jaké ustanovení vyhlášky z režimu vyšších povinností lze podřadit pod ustanovení vyhlášky pro režim nižších povinností, tak aby bylo možné jednotné řízení ISMS pro lepší efektivnost a hospodárnost procesů v rámci holdingu. Připomínka vypořádána.
683. Hospodářská komora ČR	Z	Připomínka k § 15 odst. 2 písm. c) HK ČR požaduje upravit text takto: „c) řízení aktiv a rizik,“ <u>Odůvodnění:</u> Řízení rizik je možné pouze tehdy, jsou-li identifikována aktiva. Teprve po identifikaci aktiv lze definovat rizika. Teze prováděcích právních předpisů k navrhované právní úpravě řízení aktiv vůbec v nižším režimu neupravují. Naopak vyhláška o bezpečnostních opatřeních poskytovatele služby v režimu vyšších povinností v § 8 výslovně stanoví řízení aktiv a v § 9 řízení rizik. Původní návrh právní úpravy, který NÚKIB předložil k veřejné konzultaci (dokument 1a str. 10 – odst. 3 písm. v) „řízení aktiv“ obsahoval. Pokud tedy nedojde k doplnění samostatného bodu týkajícího se řízení aktiv, navrhuje HK ČR spojení řízení aktiv a řízení rizik do jednoho bodu.	Akceptováno Upraveno na: „c) řízení aktiv, d) řízení rizik,“. Připomínka vypořádána.
684. Hospodářská komora ČR	Z	Připomínka k § 16 HK ČR požaduje znění návrhu zákona přizpůsobit znění a záměru NIS 2 a zachovat povinnosti pro subjekty, které odpovídají označení “essential” a “important” ve smyslu NIS 2. Jiná úprava by mohla být v rozporu s NIS 2 a vytvořit nerovnoměrné zatížení subjektů. <u>Odůvodnění:</u>	Neakceptováno Nová úprava podle NIS2 reflektuje snahu EU o zajištění vysoké společné úrovně kybernetické bezpečnosti napříč celou EU, proto jsou mezi povinné osoby ve vysoce kritickém odvětví nad rámec stávající právní úpravy zahrnuti mj. i poskytovatelé služeb

	Článek 23 směrnice NIS2 stanoví ohlašovací povinnosti základních a významných subjektů. Podle tohoto ustanovení musí základní a důležité subjekty hlásit každou událost, která má významný dopad na poskytování jejich služeb. Návrh zákona implementuje článek 23 směrnice NIS 2 ve svém § 16. V porovnání se směrnicí NIS 2 stanoví § 16 návrhu zákona pro základní subjekty přísnější pravidla než pro významné subjekty. Podle tohoto ustanovení musí významné subjekty hlásit každou událost bez ohledu na její dopad na poskytování svých služeb. Předkladatel v této souvislosti odkazuje na článek 5 směrnice NIS 2, který členským státům umožňuje přijmout nebo zachovat ustanovení zajišťující vyšší úroveň kybernetické bezpečnosti, pokud jsou tato ustanovení v souladu s právem EU. To potvrzuje i důvodová zpráva k § 16 návrhu zákona. Předkladatel odůvodňuje tuto úpravu odkazem na stávající zákon o kybernetické bezpečnosti a uvádí, že takový přístup se v současné době uplatňuje. To HK ČR nepokládá za zcela vypovídající. Ustanovení § 8 zákona o kybernetické bezpečnosti rozlišuje oznamovací povinnosti většiny regulovaných subjektů a dále pak poskytovatelů digitálních služeb. Poskytovatelé digitálních služeb hlásí pouze takový incident, který má významný dopad na poskytování jejich služeb. Na základě výše uvedeného a s ohledem na nové rozlišení podstatných a významných subjektů by se na poskytovatele cloudových služeb mohla vztahovat mnohem přísnější pravidla ve srovnání se současným stavem, neboť by mohli být považováni rovněž za podstatné subjekty.	cloud computingu. Do režimu vyšších povinností, se kterým je vázána povinnost hlásit všechny kybernetické bezpečnostní incidenty, budou poskytovatelé služeb cloud computingu spadat pouze v případě, že jsou velkým podnikem, nebo poskytovatelem státního cloud computingu podle zákona o informačních systémech veřejné správy. Navrhovaná právní úprava vychází ze základní zásady, na níž je založena NIS2, totiž že subjekty spadající do oblasti působnosti právní úpravy by měly být zařazeny do dvou kategorií, s přihlédnutím k míře kritické důležitosti, pokud jde o odvětví nebo druh služby, kterou poskytují, a také k jejich velikosti (viz recitál 15 uvedené směrnice). Jinak řečeno, stane-li se osoba poskytovatelem regulované služby ve vyšším povinnostním režimu, znamená to, že odvětvím, v němž poskytuje službu, respektive kombinací tohoto odvětví a vlastní velikosti dosahuje hranice vysoké míry kritické důležitosti pro České republiky. Kritérium poskytování státního cloud computingu vychází z požadavku na zabezpečení digitální infrastruktury státu. Podle ustanovení § 6m odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy je pro zajištění provozu informačního systému veřejné správy zařazeného do kritické bezpečnostní úrovně pomocí služeb cloud computingu nutné využít služeb státního poskytovatele cloud computingu. Poskytovatel státního cloud computingu bude tedy zřejmě zajišťovat provoz určité části pro stát kritických systémů, z toho důvodu by na něj měly být kladeny minimálně obdobné požadavky na zajištění kybernetické bezpečnosti, jaké jsou kladeny na systémy, k zajištění jejichž provozu jsou jeho služby využívány. Z důvodu kumulace zajišťování provozu více kritických systémů orgánů veřejné správy nestačí

			spoléhat na přenesení povinností v rámci řízení dodavatelů. Z výše uvedeného vyplývá nutnost zařadit tyto poskytovatele do režimu vyšších povinností. Požadavek na hlášení všech kybernetických bezpečnostních incidentů bez ohledu na to, zda mají významný dopad, reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob. Připomínka vypořádána.
685. Hospodářská komora ČR	Z	Připomínka k § 17 odst. 3 a 5 HK ČR požaduje doplnit náležitosti závěrečné zprávy buď přímo do textu zákona (nebo alternativně do § 3 Vyhlášky o Portálu NÚKIB), tzn. upravit text § 17 odst. 3 a 5 ve smyslu níže uvedeného odůvodnění. <u>Odůvodnění:</u> Připomínkované ustanovení ukládá poskytovatelům regulované služby povinnost do 30 dní od oznámení incidentu nebo předložení zprávy o aktuálním stavu zvládání kybernetického bezpečnostního incidentu předložit závěrečnou zprávu, jejíž náležitosti mají být dle odst. 5 stanoveny prováděcím předpisem.	Akceptováno Ustanovení § 17 odst. 5 návrhu zákona obsahuje zmocňovací ustanovení pro vydání prováděcího předpisu, který stanoví mj. obsahové náležitosti hlášení incidentu. Tímto předpisem je vyhláška o Portálu Úřadu a požadavcích na vybrané úkony, která v § 3 odst. 1 stanovuje obsahové náležitosti formuláře pro hlášení incidentů, přičemž z odst. 3 písm. d) tohoto ustanovení vyplývá, že jde přes daný formulář vytvořit i závěrečnou zprávu. Náležitosti v § 3 odst. 1 vyhlášky přitom dle našeho názoru odpovídají požadavkům čl. 23 odst. 4 písm. d) NIS2. Závěrečná zpráva bude v podstatě agregovat, upřesňovat a doplňovat informace

		Vyhláška o Portálu NÚKIB se ale v § 3, který popisuje obsahové náležitosti úkonů spojených s hlášením kybernetických bezpečnostních incidentů, nevěnuje konkrétním náležitostem závěrečné zprávy, nýbrž pouze popisu obsahu formuláře pro hlášení incidentů, z něhož vyplývá, že slouží primárně k oznamování incidentů podle § 17 odst. 1 písm. a) nebo c) podávání průběžné zprávy o podstatných změnách stavu zvládnutí kybernetického bezpečnostního incidentu podle § 17 odst. 3 písm. b) zákona. HK ČR proto požaduje doplnit obsahové náležitosti závěrečné zprávy tak, aby se předešlo nejistotě regulovaných osob ohledně způsobu plnění povinností podle § 17 odst. 1 písm. b) a c), obzvláště vzhledem k tomu, že za jejich porušení hrozí dle § 58 odst. 1 písm. h) ve spojení s odst. 15 písm. a) pokuta ve výši až 250 000 000 Kč nebo do výše 2 % čistého celosvětového ročního obrátu.	nahlášené v předcházejících fázích procesu hlášení. Pro jistotu adresátů byl doplněn odst. 3 specificky hovořící o obsahu závěrečné zprávy. Připomínka vypořádána.
686. Hospodářská komora ČR	Z	Připomínka k § 19 odst. 1 HK ČR požaduje upravit text § 19 odst. 1 takto: <i>„(1) Pokud to poskytovatel regulované služby považuje za vhodné, oznámí bez zbytečného odkladu uživatelům regulované služby kybernetický bezpečnostní incident s významným dopadem, který by mohl negativně ovlivnit poskytování této služby. Úřad je po konzultaci s dotčeným poskytovatelem regulované služby oprávněn uložit poskytovateli regulované služby, který je dotčen kybernetickým bezpečnostním incidentem s významným dopadem, povinnost informovat uživatele regulované služby o tomto incidentu. V rozhodnutí o uložení této povinnosti stanoví Úřad rozsah informační povinnosti. Zveřejnění informace nesmí ohrozit bezpečnost nebo provoz regulované služby a povinné osoby.“</i> <u>Odůvodnění:</u> V případě, že předkladatel uloží takovou povinnost bez předchozí konzultace, může dojít k poskytnutí informací, které takový incident	Akceptováno jinak - nyní § 20 Úřad při rozhodování o zveřejnění informací o kybernetickém bezpečnostním incidentu vezme v rámci správního uvážení do úvahy potřebu zachování rovnováhy mezi zájmem uživatelů regulované služby na informacích o hrozbách a incidentech, a možným poškozením pověsti či obchodních zájmů poskytovatele regulované služby, který incident ohlašuje. Reflektovány budou také skutečnosti, které Úřad zjistil v průběhu konzultace s tímto poskytovatelem, a to takovým způsobem, aby zveřejněním nedošlo k ohrožení bezpečnosti nebo provozu regulované služby. Připomínka vypořádána.

		mohou prohloubit, případně i vyvolat další incidenty s využitím informací získaných zveřejněním zranitelností. Rozsah informační povinnosti není nijak upřesněn/omezen. Předkladatel tak může vyzvat ke zveřejnění informací bez znalosti celkového kontextu incidentu. Přílišná transparentnost může v některých případech ohrozit bezpečnost regulovaných služeb a kritické infrastruktury.	
687. Hospodářská komora ČR	Z	Připomínka k § 19 odst. 2 HK ČR požaduje upravit text § 19 odst. 2 takto: <i>„(2) Poskytovatel regulované služby, který se dozví o významné kybernetické hrozbě ovlivňující jím poskytovanou regulovanou službu, je povinen bez zbytečného odkladu informovat Úřad, který vhodným a srozumitelným způsobem informuje o této hrozbě uživatele regulované služby, který může být ovlivněn významnou kybernetickou hrozbou, o takových krocích, které může uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší. V případě, že je to možné a vhodné, informuje poskytovatel regulované služby uživatele také o této významné kybernetické hrozbě.“</i> Případně variantně požaduje HK ČR alespoň ujištění o tom, že informace předávané poskytovatelem jsou generické informace podávané subjektům čelícím významné kybernetické hrozbě. <u>Odůvodnění:</u> Z navrhovaného znění zákona není patrné, o jakých hrozbách by měl poskytovatel regulované služby uživatele informovat a zároveň je povinnost stanovena nezávisle na vědomosti poskytovatele o existenci hrozby. Povinnost je přitom spojena s nejvyšší možnou pokutou dle § 58 odst. 1 písm. k) ve spojení s odst. 15 písm. a). HK ČR proto navrhuje jasně definovat, že poskytovatel je povinen informovat pouze o hrozbách, o kterých se dozví a které ovlivňují jím poskytovanou regulovanou službu. Dle navrhovaného znění by totiž	Neakceptováno – nyní § 20 O hrozbách, o kterých se poskytovatel regulované služby nedozví a nemohl dozvědět, není z podstaty věci možné kohokoliv informovat a toto jednání sankcionovat. Vztahovat informační povinnost na uživatele kterékoliv regulované služby se zároveň jeví jako výrazně extenzivní výklad, který úmyslem zákonodárce není a nevyplývá z textu zákona ani důvodové zprávy. Jelikož je cílem tohoto ustanovení předat informace uživateli regulované služby, který může být ovlivněn, nejvíce se informování širokého spektra subjektů skrze Úřad jako optimální řešení, neboť je primárně kladen důraz na rychlost takového informování, která nebude zatížena o další článek v řetězu a zároveň také postup poskytovatele regulované služby podle § 20 návrhu zákona nevylučuje další informování Úřadem, například skrze varování podle § 23 návrhu zákona. Nadto je také důležité, aby byli informováni dotčení uživatelé, k nimž bude mít pravděpodobně přístup skrze evidenci sám poskytovatel regulované služby. V případě nutnosti individualizace o způsobu předcházení hrozbě je také důležitá znalost systému poskytovatele regulované služby, kterou by měl nejvíce disponovat sám poskytovatel regulované služby.

		bylo možné sankcionovat jakéhokoli poskytovatele za jakoukoli významnou hrozbu nezávisle na tom, jestli se hrozba dotýká jím poskytované regulované služby a jestli o hrozbě poskytovatel věděl nebo vědět měl. Informace o významné kybernetické hrozbě by měl poskytovatel regulované služby předávat předkladateli, který agregovaně předá informaci širokému spektru subjektů, aby tak nedocházelo k přílišnému zahlcení kapacit řešitelských týmů poskytovatele regulované služby při nutnosti podávání individualizované informace o způsobu předcházení takové hrozbě jednotlivým subjektům. Tyto kapacity pak může poskytovatel využít pro řešení případné hrozby a dalším úkonům potřebným k udržení nejvyšší úrovně kybernetické ochrany.	Připomínka vypořádána.
688. Hospodářská komora ČR	Z	Připomínka k celému Dílu 3 Vztah poskytovatele regulované služby a jeho dodavatelů HK ČR požaduje doplnit příslušná ustanovení zavazující určeného dodavatele k součinnosti při plnění zákonných požadavků poté, co byl prokazatelně informován, že se stává osobou zajišťující bezpečnostně významnou dodávku strategické služby, a to ve smyslu níže uvedeného odůvodnění. <u>Odůvodnění:</u> Dodavatel by měl mít v zákoně výslovně stanovenou povinnost spolupracovat. V praxi totiž bez součinnosti dodavatele, pokud tomuto není povinnost součinnosti textem právního předpisu výslovně uložena, nemusí být poskytovatel regulované služby schopen plnit zákonné požadavky.	Neakceptováno Uložení zákonné povinnosti dodavatelům bezpečnostně významné dodávky poskytovat součinnost poskytovateli strategicky významné služby Úřad považuje za neproporcionální řešení. Navrhované řešení by neúměrně zatížilo Úřad, potažmo stát, přičemž vymáhání plnění takto stanovené povinnosti by bylo velmi problematické. V potaz je také nutno vzít skutečnost, že aplikací navrhovaného řešení by si Úřad vytvořil příliš extenzivní pravomoci. Úřad si je vědom, že pro poskytovatele strategicky významné služby může být za určitých okolností složité získat informace zejména o svých nepřímých dodavatelích. Z tohoto důvodu návrh zákona nestanoví poskytovateli strategické služby povinnost zjistit informace o dodavatelích bezpečnostně významných dodávek, ale stanoví povinnost poskytovatele strategicky významné služby tyto informace o dodavatelích bezpečnostně významných dodávek aktivně zjišťovat, a to s

			vynaložením přiměřeného úsilí. Posouzení, zda poskytovatel strategicky významné služby vynaložil přiměřené úsilí, či nikoliv bude vždy záviset na konkrétních skutkových okolnostech. Vzhledem k výše uvedenému je Úřad přesvědčen, že získávání informací o dodavatelích bezpečnostně významných dodávek mají být v gesci poskytovatelů strategicky významné služby. Povinnosti dodavatelů je nutné smluvně ošetřit v rámci řízení dodavatelů. Připomínka vypořádána.
689. Hospodářská komora ČR	Z	Připomínka k § 21 odst. 1 HK ČR požaduje, aby byl text § 21 odst. 1 upraven takto: <i>„(1) Úřad je po konzultaci s dotčeným poskytovatelem regulované služby z důvodu ochrany vnitřního či veřejného pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn veřejnost informovat o významném kybernetickém bezpečnostním incidentu či o porušování povinností daných tímto zákonem, nebo dotčenému poskytovateli regulované služby rozhodnutím uložit, aby tak učinil sám. Zveřejnění informace nesmí ohrozit bezpečnost nebo provoz regulované služby.“</i> <u>Odůvodnění:</u> Směrnice NIS 2 v článku 23 odst. 7, ze kterého vychází § 21 „Výstraha“, pojednává pouze o „významných“ incidentech, toto zúžení ale v § 21 chybí, HK ČR požaduje jej doplnit. Jinak je oprávnění předkladatele informovat o kyberbezpečnostních incidentech prakticky bezbřehé. Zveřejnění klasifikovaných informací a případného nesouladu s tímto zákonem může vést k narušení bezpečnosti informací a samotného smyslu zákona zajistit bezpečnost regulovaných služeb.	Neakceptováno – nyní § 22 Od použití sousloví „významný incident“ bylo upuštěno, protože má v kontextu zákona o kybernetické bezpečnosti jiný obsah (jedná se o incident, který naplňuje kritéria daná vyhláškou pro určení míry významnosti v kontextu hlášení incidentů ze strany poskytovatelů regulované služby v režimu nižších povinností). Významnost incidentu pak indikuje formulace „z důvodu ochrany vnitřního či veřejného pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu“, která stanoví, že Úřad musí mít pro zveřejnění incidentu některý z těchto závažných důvodů a právě zveřejněním incidentu by bylo možné těmto dopadům předejít, což vymezuje okruh možností, kdy lze zveřejnění incidentu odůvodnit. Úřad v rámci správního uvážení bere do úvahy jak informace získané při konzultaci s daným poskytovatelem regulované služby, tak i míru dopadu výstrahy na daného poskytovatele regulované služby a právě veřejný zájem musí v rámci testu proporcionality převážet nad dopady, které by zveřejnění mohlo mít na danou organizaci. Běžně je incident a informace o něm

			v rozsahu informací, pro které platí i výjimka ze zákona o svobodném přístupu k informacím obsažená v zákoně o kybernetické bezpečnosti, což plyne např. z ustanovení § 38. Jedná se tedy skutečně o prostředek <i>ultima ratio</i> a výjimku z pravidla o neposkytování informací o incidentech a svévoli Úřadu tak zabraňuje množství dalších ustanovení zákona o kybernetické bezpečnosti. Připomínka vypořádána.
690. Hospodářská komora ČR	Z	Připomínka k § 22 odst. 2 HK ČR požaduje, aby byl text § 22 odst. 2 vypuštěn a odst. 3 byl odpovídajícím způsobem přečíslován. <u>Odůvodnění:</u> Varování je instrument, který je v předkládaném návrhu upraven nad rámec směrnice NIS 2. V aktuálním znění zákona je varování (§ 12) upraveno tak, že jeho obsahem není nic ekvivalentního ve vztahu k odstavci 2. Jde tedy o typický gold-plating. V důvodové zprávě není nijak zdůvodněno, proč odstavce 2 předkladatel do § 22 vložil. Navíc pokud může předkladatel „stanovit jinak“, jak poskytovatel regulované služby v režimu vyšších povinností varování zohlední, znamená to významný prostor k širokému zásahu předkladatele do svobody podnikání fakticky dle libosti. Předkladatel v důvodové zprávě správně píše, že „<i>Varování je ve svém důsledku závazné pro poskytovatele regulovaných služeb v režimu vyšších povinností, jelikož ti v rámci svého systému řízení bezpečnosti informací a řízení rizik jsou schopni zohlednit hodnotu dané hrozby či zranitelnosti.</i>“, pro existenci odstavce 2 tedy neexistuje žádný logický důvod. Navrhovaný text dává předkladateli možnost prostřednictvím varování ukládat relativně blíže neurčenému okruhu osob povinnosti, které by adresát úpravy – zde poskytovatel regulované služby – byl bez dalšího povinen plnit. Vzhledem k okruhu adresátů, kteří by byli nuceni takto uložené povinnosti plnit, mohou být takové povinnosti	Vysvětleno - nyní § 23 Úřad nikdy neměl v úmyslu rozšiřovat okruh subjektů, kterých se varování týká, nad zákonem stanovenou úroveň, tedy ani globálně, ani vůči poskytovatelům regulovaných služeb v režimu nižších povinností. Úřad toto ustanovení zahrnul pouze proto, aby v případech, kdy je zejména hrozba relevantní pouze pro některé odvětví, mohl navázat varování vůči naopak úžeji vymezenému počtu subjektů. Rozšířit varování na subjekty mimo zákon o kybernetické bezpečnosti pouhým rozhodnutím Úřadu by nebylo legální a rozšíření na poskytovatele regulované služby v režimu nižších povinností je neúčelné, jelikož tito neprovádějí povinně analýzu rizik, do které by mohli tuto změnu hodnoty hrozby či zranitelnosti implementovat. Tedy tato varianta není rovněž z pozice Úřadu relevantní. Toto je také příslušně doplněno do důvodové zprávy, aby o úmyslu Úřadu s použitím tohoto ustanovení nebylo pochyb. Co se týká jiného právního předpisu, který může subjekty zavázat k aplikaci varování, to vychází z faktu, že vzrůstá trend sektorové regulace, která zahrnuje mimo regulaci sektorovou i regulaci kybernetické bezpečnosti. Při její implementaci ze

		ukládány přinejmenším formou opatření obecné povahy na základě zákonného zmocnění. Opatření obecné povahy je přitom ze zákona spojeno s procesními náležitostmi a prostředky procesní obrany, které v případě varování dle předloženého návrhu chybí. HK ČR má za to, že v předložené podobě je návrh co do otázky závazné povahy varování neústavní. HK ČR chápe potřebu předkladatele rychle a bez nadbytečných procedurálních formalit reagovat na vyvíjející se charakteristiky kybernetického prostředí a vhodným způsobem varovat soukromý sektor, nemůže se tak však dít formou ukládání závazných povinností.	strany sektorových regulátorů zaznívá, že by těmto regulátorům připadalo účelné ve svých předpisech zavázat některé subjekty, u kterých to systém řízení bezpečnosti umožňuje (jde o řízení prostřednictvím rizik) a jsou zároveň postaveni mimo dosah zákona o kybernetické bezpečnosti k tomu, aby se tyto organizace řídily varováními vydanými Úřadem. Z tohoto důvodu je tu ponechán prostor pro jiný právní předpis stejné právní síly, tedy zákon, k tomu, aby zavázal další povinné osoby k dodržování varování. Co se týče zařazení ustanovení, které není jen odrazem směrnice NIS2, je třeba poznamenat, že varování jako takové je institutem, který je obsahem zákona již od jeho první verze účinné od roku 2015, kdy ještě žádná legislativa EU neexistovala a odstavec 2 byl do zákona zařazen s ohledem na situace, se kterými se Úřad při jeho vydávání setkal a které z jeho fungování v praxi považuje za vhodné vyjasnit v samotném textu zákona. Připomínka vypořádána.
691. Hospodářská komora ČR	Z	Připomínka k § 23 odst. 5 a 6 HK ČR požaduje text § 23 odst. 5 a 6 upravit takto: <i>„(5) Opatření obecné povahy podle odstavce 4 nabývá účinnosti okamžikem jeho vyvěšení na úřední desce Úřadu; ~~ustanovení § 172 správního řádu se nepoužije.~~ O vydání opatření obecné povahy Úřad rovněž vyrozumí poskytovatele regulované služby, kteří jsou jím dotčeni.</i> <i>~~(6) Dotčený poskytovatel regulované služby či kdokoli, kdo prokáže, že jeho práva, povinnosti nebo zájmy mohou být opatřením obecné povahy přímo dotčeny, může k opatření obecné povahy vydanému podle odstavce 4 uplatnit připomínky ve lhůtě 30 dnů ode dne jeho vyvěšení na úřední desce Úřadu. Úřad může na~~</i>	Neakceptováno Zákon o kybernetické bezpečnosti ani v aktuální podobě neobsahuje jiný, než v současnosti navrhovaný proces vydávání reaktivního protiopatření (dříve reaktivního opatření). Účelem reaktivního protiopatření je co nejrychleji a v případech, které nesnesou odkladu reagovat na vyvstálé riziko. Z tohoto důvodu byl jediný příležitý nástroj obsažený v rámci správního řádu příslušně upraven a návrhová část celého procesu opatření obecné povahy nebyla zavedena jako součást procesu vydávání reaktivního protiopatření, stejně jako nebyla součástí procesu původního reaktivního opatření. Zavedení

		~~základě uplatněných připomínek opatření obecné povahy změnit nebo zrušit.~~“ <u>Odůvodnění:</u> Ustanovení odst. 6 připouští jen podání připomínek proti vydanému opatření obecné povahy, a to ve lhůtě 30 dnů. Připomínky jsou poněkud slabší nástroj ochrany ve vztahu k námitkám, o nichž je orgán vydávající opatření obecné povahy povinen samostatně rozhodnout, zrušením ustanovení se použije postup podle § 172 a násl. správního řádu, kde je možno uplatnit připomínky i námitky. Ve srovnání s připomínkami představují námitky procesně silnější nástroj ochrany práv. Dále je potřeba uvést, že jen postup podle § 172 a násl. správního řádu je zárukou uplatnění práv, povinností nebo zájmu těch, kteří jsou opatřením obecné povahy přímo dotčeni, jelikož ustanovení § 173 odst. 2 správního řádu určuje, že proti opatření obecné povahy nelze podat opravný prostředek, kterým by subjekt mohl dosáhnout nápravy. Proti opatření obecné povahy nelze podat odvolání ani rozklad (na rozdíl od správního rozhodnutí).	navrhovaného by tedy bylo v přímém rozporu s účelem tohoto ustanovení, které je již ověřeným institutem, který byl ze strany Úřadu již několikrát úspěšně použit. Připomínka vypořádána.
692. Hospodářská komora ČR	Z	Připomínka k § 24 odst. 2 HK ČR požaduje (alespoň) v důvodové zprávě upřesnit kritéria pro posouzení možnosti/nemožnosti zohlednění bezpečnostních požadavků. <u>Odůvodnění:</u> Jedná se o nový institut, proto by bylo vhodné koncipovat důvodovou zprávu podrobněji. Zejména jde o to, zda je poskytovatel regulované služby povinen splnit povinnosti i v případě značných nákladů.	Neakceptováno - nyní § 25 Dotčené ustanovení není v regulaci kybernetické bezpečnosti ničím novým, naopak jde o ustanovení přejaté z aktuálně účinného § 4 odst. 4 zákona č. 181/2014 Sb., které doznalo pouze mírných formulačních změn tak, aby nedocházelo k výkladovým nejasnostem. Stejně jako za současného zákona č. 181/2014 Sb. tedy bude platit, že poskytovatel regulované služby bude povinen zohlednit požadavky vyplývající z bezpečnostních opatření při výběru svých dodavatelů, stejně jako bude i do budoucna platit současná povinnost povinných osob zohledňovat požadavky vyplývající z

		bezpečnostních opatřeních ve smlouvách se svými dodavateli. Oproti aktuálně účinné úpravě bylo doplněno „tam, kde je to možné“. Toto doplnění míří zejména na situace, kde nové požadavky vyplývající z bezpečnostních opatření vstupují do již existujících smluvních vztahů. V takovém případě je poskytovatel regulované služby povinen učinit vše pro to, aby již uzavřené smlouvy uvedl do souladu s požadavky návrhu zákona (požadavky vyvěrajícími z bezpečnostních opatření). V odůvodněných případech, kdy není možné smlouvu změnit či ukončit (z toho důvodu je použita právě formulace „tam, kde je to možné“), je možné ve smluvním vztahu po nezbytně nutnou dobu pokračovat a požadovanou úroveň kybernetické bezpečnosti zajistit jiným způsobem (zejména zavedením kompenzačních bezpečnostních opatření). Výše nákladů na promítnutí bezpečnostních požadavků do smluv obecně nemůže být důvodem pro neplnění požadavků zákona, v závislosti na konkrétních skutkových okolnostech však může být např. relevantním důvodem pro rozložení plnění jednotlivých povinností do delšího časového úseku, případně pro zavedení jiných kompenzačních opatření, která budou zajišťovat potřebnou úroveň kybernetické bezpečnosti. Od požadavků stanovených v tomto ustanovení je pak potřeba odlišovat mechanismus prověřování bezpečnosti dodavatelského řetězce resp. opatření obecné povahy z něj plynoucí, které může být (v závislosti na jeho obsahu) přímo aplikovatelné a jeho plnění v tu chvíli nebude probíhat v režimu připomínkou dotčeného ustanovení.

			Připomínka vypořádána.
693. Hospodářská komora ČR	Z	Připomínka k § 25 odst. 1 HK ČR požaduje přeformulovat nebo upřesnit v § 25 odst. 1 slovní spojení „...hrozícího kybernetického bezpečnostního incidentu...“, a to ve smyslu níže uvedeného odůvodnění, a současně text § 25 odst. 1 upravit takto: <i>„(1) Úřad může v případě hrozícího kybernetického bezpečnostního incidentu na podnět poskytovatele regulované služby v režimu vyšších povinností, který marně vyzval významného dodavatele ke splnění smluvního závazku předat informace a data, rozhodnutím uložit významnému dodavateli povinnost předat poskytovateli regulované služby v režimu vyšších povinností informace a data související s provozem aktiv sloužících k poskytování regulované služby. Pokud významný dodavatel informacemi nebo daty souvisejícími s provozem aktiv sloužících k poskytování regulované služby nedisponuje nebo vzhledem ke skutkovým okolnostem není účelné po něm požadovat jejich opatření a vydání, může Úřad povinnost podle předchozí věty uložit i jinému orgánu nebo osobě, která požadovanými informacemi a daty disponuje. Úřad může v rozhodnutí určit formát, rozsah, způsob a lhůtu předání a stanovit povinnost po provedení předání tyto informace a data a jejich kopie bezpečně zlikvidovat. Rozhodnutí Úřadu o uložení povinnosti ohledně formátu, rozsahu, způsobu a lhůty předání informací podle předchozí věty nesmí jít nad rámec smluvních závazků jiného orgánu nebo osoby, jíž je povinnost ukládána.“</i> <u>Odůvodnění:</u> Z díkce návrhu zákona není zřejmé, jakou metrikou bude vyhodnocována míra hrozby incidentu, která se nelehko kvantifikuje, pokud takový incident ještě nenastal. Není zřejmé, kdo určí, že se jedná o hrozící incident, a tedy oprávněnost žádosti. Není postaveno najisto, zda se jedná podle definice o Událost, není zřejmé, o jaká data	Akceptováno jinak – nyní § 26 Definice hrozícího kybernetického bezpečnostního incidentu byla upřesněna. Úřad bude při zvažování dopadu incidentu brát v rámci správního uvážení v potaz vždy konkrétní okolnosti každého případu. V každém případě se bude jednat o informace a data související s provozem aktiv sloužících k poskytování regulované služby. Toto ustanovení míří na krajní situace, kdy by hrozící či probíhající kybernetický bezpečnostní incident mohl mít závažný vliv na poskytování regulované služby s dopadem na zachování základních funkcí státu, hospodářských činností, bezpečnosti, veřejného zdraví, majetku nebo životního prostředí. V takovém případě převládá zájem státu na odvrácení incidentu s takto významným dopadem nad soukromoprávní dohodou o předání dat. Povinnost zanechat do smlouvy specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání povinnou osobou je součástí bezpečnostních opatření, která bude poskytovatel regulované služby v režimu vyšších povinností povinen zavádět. Vzhledem k tomu, že příslušná ujednání by měla být součástí smluvního vztahu mezi poskytovatelem regulované služby a významným dodavatelem, měl by institut předání dat sloužit jako <i>ultima ratio</i> až poté, co selžou jednání mezi dotčenými stranami. Do situace, kdy je smlouva jasně ujednána, vyhovuje oběma stranám a významný dodavatel se jejím plnění nebrání, Úřad nikdy zasahovat nebude.

		a informace se jedná, pokud incident ještě nenastal. Bez vyjasnění může docházet ke zneužití a nepřesným interpretacím. Ohledně formátu, rozsahu, způsobu a lhůty pro předání dat či informací je nutno respektovat smluvní ujednání.	Přípomínka vypořádána.
694. Hospodářská komora ČR	Z	Přípomínka k Dílu 5 Mechanismus prověřování bezpečnosti dodavatelského řetězce HK ČR požaduje, aby byl celý Díl 5 ze zákona vypuštěn a ze zákona odstraněny odkazy na ustanovení Dílu 5, případně alternativně, aby schvalování mechanismu prověřování bezpečnosti dodavatelského řetězce mělo formu zvláštního zákonného předpisu mimo implementaci NIS 2. <u>Odůvodnění:</u> Mechanismus prověřování bezpečnosti dodavatelského řetězce s NIS 2 nijak zásadně věcně nesouvisí a není nutné ho schvalovat současně. Navíc na evropské úrovni se zjevně připravuje podobná právní úprava v podobě Telecoms Act, který avizoval v rozhovoru pro deník Les Echos evropský komisař pro vnitřní trh Thierry Breton (https://www.lesechos.fr/tech-medias/hightech/thierry-breton-la-commission-soutient-les-etats-membres-qui-bannissent-huawei-1952702). Je tak potřeba pečlivě zvážit (i s ohledem na další připomínky HK ČR), zda je vhodná forma prověřování dodavatelů čistě národní úprava a zda není vhodné postupovat na úrovni celé EU. Zároveň samotná směrnice NIS 2 předpokládá celoevropské hodnocení dodavatelů v článku 22 „Koordinované posouzení bezpečnostních rizik kritických dodavatelských řetězců na unijní úrovni“. Ten předpokládá, že Skupina pro spolupráci může ve spolupráci s Komisí a agenturou ENISA provést koordinované posouzení bezpečnostních rizik dodavatelských řetězců u specifických kritických služeb IKT, systémů IKT nebo produktů IKT, přičemž zohlední technické, případně netechnické rizikové faktory.	Neakceptováno Problematika prověřování rizikových dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České republice pro stát i soukromé subjekty. Úkol připravit návrh zákona upravující bezpečnost dodavatelského řetězce byl Národnímu úřadu pro kybernetickou a informační bezpečnost uložen usnesením Bezpečnostní rady státu ze dne 21. června 2022 č. 41. Z důvodu vzájemné propojenosti s úpravami v rámci transpozice směrnice NIS2 bylo rozhodnuto o spojení obou zmiňovaných problematik do jednoho právního předpisu. Z těchto důvodů nepovažujeme za vhodné, aby byl návrh zákona rozdělen, jak připomínkové místo požaduje. Koordinované posouzení je nástroj, se kterým sice směrnice NIS2 počítá, ale dále ho nerozpracovává. Nadto NÚKIB zdůrazňuje, že otázka národní bezpečnosti (do které prověřování dodavatelského řetězce ve strategicky významných službách bezpochyby spadá) zůstává ve výlučné pravomoci jednotlivých členských států. Nic tedy nebrání tomu,

	Dle našeho přesvědčení je vhodné postupovat v tomto ohledu na evropské a nikoli národní úrovni. Předkladatel sám v důvodové zprávě uvádí (na straně 69), že kritéria jsou fakticky totožná, jaká navrhuje v mechanismu prověřování bezpečnosti dodavatelského řetězce. Navíc tvrdí, že v podobě § 23 má k dispozici nástroj (reaktivní protiopatření), kterým může povinným osobám nařídit zohlednění výsledků koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců: <i>„Reaktivní protiopatření je zároveň v této podobě i nástrojem odrážejícím požadavek, který směrnice NIS 2 na členské státy klade ve svém článku 21 odst. 3. Ten stanovuje členským státům povinnost disponovat nástrojem, prostřednictvím kterého zajistí, aby povinné osoby, tedy poskytovatelé regulovaných služeb museli zohlednit výsledky koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců podle čl. 22 směrnice NIS 2.“</i> Pokud má předkladatel k dispozici evropskou úpravu posouzení bezpečnostních rizik kritických dodavatelských řetězců fakticky se stejnými kritérii, jaké plánuje do národní úpravy, a nástroj, kterým dokáže donutit povinné osoby, aby zohlednily výsledky tohoto posouzení, pak je na místě otázka, k čemu je mechanismus na národní úrovni vlastně potřeba. Pro případ, že by požadavek HK ČR na vypuštění celého Dílu 5 nebyl akceptován, požaduje HK ČR: - detailní odůvodnění v důvodové zprávě a závěrečné zprávě RIA, proč se stát nerozhodl jít v tomto případě kroky, které předpokládá směrnice NIS 2. Ta v článku 22 kodifikuje přesně to, čeho chce stát dosáhnout vlastním mechanismem – tedy posouzení bezpečnosti rizik dodavatelských řetězců u specifických kritických služeb ICT, systémů ICT nebo produktů ICT, a to se zohledněním technických, případně netechnických faktorů. V souladu se zásadou proporcionality by měl předkladatel zdůvodnit, z jakého důvodu není toto ustanovení dostatečné a nevede k cíli, kterého chce stát	aby do budoucna byla problematika dodavatelských řetězců řešena jak na evropské, tak na národní úrovni. Připomínka vypořádána.

		dosáhnout. Je zcela legitimní otázka, zda článek není dostatečnou implementací mechanismu, jehož přípravu zadala předkladateli Bezpečnostní rada státu ještě před tím, než bylo známé finální znění směrnice NIS 2, zvláště když předkladatel sám v důvodové zprávě tvrdí, že v podobě § 23 návrhu má k dispozici nástroj (reaktivní protiopatření), kterým může povinným osobám nařídít zohlednění výsledků koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců; - koordinované posouzení rizik dodavatelských řetězců na evropské úrovni by dle pohledu HK ČR odstranilo mnoho nejasností, které jsou bohužel přítomné v současném návrhu. Protože dle článku 22 specifické služby, systémy a produkty ICT určí Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA, nedojde k závažnému narušení jednotného trhu, kdy dnes reálně hrozí, že operátoři v jedné zemi (a v jedné podnikatelské skupině) budou moci využívat větší množství dodavatelů, než v zemi jiné. Tím se operátoři v zemi, kde stát úředně omezí množství dostupných dodavatelů, dostanou do konkurenční nevýhody, protože se jim logicky zvýší náklady – tím se stanou méně atraktivní pro potenciální investory a sníží se valuace jejich společností, což bude mít vliv na případný exit majitelů nebo na získání strategických investorů. Předkladatel by měl tyto aspekty zhodnotit podrobně v analýze RIA, kde zcela absentují; - HK ČR upozorňuje, že existuje „Metodická pomůcka pro prevenci nadbytečné regulatorní zátěže při implementaci práva EU“ dostupná na stránkách Úřadu vlády ČR. Podle kapitoly II „Předcházení nadbytečné regulatorní zátěži při neminimalistické implementaci“ by měl předkladatel vždy posoudit, zda zvolená varianta implementace nepředstavuje nadbytečnou regulatorní zátěž a posouzení provést při hodnocení dopadů regulace. HK ČR požaduje, aby předkladatel dle této metodické pomůcky vyhodnotil, proč	

		zvolil mechanismus prověřování dodavatelského řetězce jako národní variantu a nikoli společný postup v rámci EU a jeho uplatnění na regulované subjekty v ČR pomocí § 23 návrhu; - případné omezení dodavatelů významně ovlivní investiční kapacitu a schopnosti především menších a středních firem investovat do rozvoje svých sítí. Pokud budou NÚKIB nějací dodavatelé omezeni nebo zakázáni, pochopitelně to sníží úroveň konkurence a zvýší ceny. Tento faktor musí NÚKIB zhodnotit v RIA v oddílu týkajícího se sociálních dopadů; - předkladatel by měl také zhodnotit vliv na malé a střední podniky v RIA tak, jak to předpokládají příslušná pravidla.	
695. Hospodářská komora ČR	Z	Připomínka k § 28 HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text § 28 upraven ve smyslu níže uvedeného odůvodnění a § 28 odst. 1 upraven takto: <i>„(1) Úřad shromažďuje a vyhodnocuje informace a data spojené s orgánem či osobou, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikivosti dodavatele. Úřad využívá data výhradně za účelem vyhodnocování rizikivosti dodavatelů.“</i> <u>Odůvodnění:</u> V kritériích rizikivosti dodavatele nejsou nijak zohledněna kritéria technické a organizační povahy zajišťování kybernetické bezpečnosti. Zahrnutí technických kritérií do hodnocení důvěryhodnosti dodavatelů byla přitom doporučena samotným předkladatelem v Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice z února 2022. Technické a organizační zajištění kybernetické bezpečnosti může být přitom vhodnou mitigací rizik vyplývajících ze „strategického“ posouzení dodavatele – minimálně by měl předkladatel a další orgány brát tato technická a	Neakceptováno - nyní § 29 NÚKIB se na základě četných připomínek rozhodl, že kritéria rizikivosti dodavatele ve formě prováděcího právního předpisu nevydá. Zpětně však uvádíme, že návrh vyhlášky cílil na strategická, nikoliv technická, kritéria záměrně. NÚKIB pevně věří, že je ve schopnostech státu a jeho organizačních složek, v tomto případě též NÚKIB, posuzovat rizika ve strategické rovině, tedy na základě strategických kritérií, ke kterým mohou jednotlivé orgány státu disponovat relevantními informacemi. Obdobně se tak děje i v jiných státech, včetně Spojených států amerických, Německa, Dánska či Estonska. Strategická kritéria jsou pro posouzení rizikivosti dodavatele nezbytná. Posuzování technických či organizačních kritérií by tedy mělo být primárně na jednotlivých poskytovatelích strategicky významné služby, kteří v těchto otázkách disponují širokými znalostmi, jež dokáží aplikovat na své potřeby. Stát, potažmo NÚKIB, by měl zasáhnout až v případě posuzování

		organizační opatření v úvahu při rozhodování o rizikosti dodavatele. HK ČR tak požaduje doplnit do kritérií rizikosti dodavatele technická a organizační kritéria a výslovně uvést do § 4 prováděcí vyhlášky (nebo přímo do zákona), že technická a organizační kritéria musí být brána v úvahu při vyhodnocování rizikosti dodavatele a jako mitigační opatření. Navrhované znění explicitně neomezuje účel sběru informací, účel žádostí ani charakter sbíraných a vyžadovaných informací. Absence těchto omezení vytváří zjevně nezamýšlený prostor pro zneužití institutu sběru údajů a součinnosti k neodůvodněnému shromažďování údajů o právnických i fyzických osobách. Navrhované znění by bylo možné vykládat např. tak, že zakládá povinnost poskytovatele služeb elektronických komunikací poskytnout předkladateli na vyžádání shromažďované provozní a lokalizační údaje, ačkoli takové poskytnutí by ve většině případů bylo neproporcionálním zásahem do ústavně chráněného základního práva na soukromí. HK ČR předepisuje, že navrhovaná úprava má vazbu i na změny v díkci § 29 odst. 3 – podrobnosti viz níže.	rizikosti dodavatele na strategické úrovni, kde stát disponuje informacemi, ke kterým nemohou mít poskytovatelé strategicky významné služby přístup. NÚKIB shromažďuje a vyhodnocuje informace primárně za účelem zajištění fungování mechanismu bezpečnosti dodavatelského řetězce. Z povahy činnosti správních orgánů však nelze vyloučit, že získané informace budou využity i při dalších činnostech NÚKIB nebo jiných orgánů veřejné moci. Bylo by v rozporu se základními zásadami činnosti správních orgánů, pokud by NÚKIB tyto informace nepředal, respektive nevyužil při výkonu ostatních pravomocí. NÚKIB však garantuje, že v žádostech o součinnost podle § 30 odst. 1 až 3 bude postupovat v souladu s principem proporcionality. Tento soulad bude kontrolován i dotazovanými orgány a osobami, které řádně neodůvodněné žádosti nemusí vyhovět. Je vhodné doplnit, že žádosti o součinnost podle § 30 odst. 1 až 3 se nijak neliší od obdobných institutů zákona. Připomínka vypořádána.
696. Hospodářská komora ČR	Z	Připomínka k § 28 odst. 3 písm. a) HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text § 28 odst. 3 písm. a) upraven takto: <i>„a) kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovni vysoké nebo kritická a jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby; ~~kritickou částí~~</i>	Neakceptováno - nyní § 29 NÚKIB považuje za nutné chránit veškeré funkce veřejné komunikační sítě, které jsou považovány za kritické. Tyto kritické funkce nemusí být nutně vztaženy pouze na jádro sítě, jelikož mnohdy zabezpečují a udržují chod poskytování služeb koncovým uživatelům, a to zejména v rámci rádiové přístupové sítě. Například řízení či monitorovací funkce rádiových stanic představují prostředek, pomocí kterého se koncoví uživatelé připojují právě ke službám poskytovaným jádrem sítě. V případě jejich kompromitace tak může být narušeno či zcela

	~~stanoveného rozsahu jsou vždy alespoň aktiva stanoveného rozsahu strategicky významné služby, která zajišťují nepominutelné funkce stanoveného rozsahu stanovené prováděcím právním předpisem,~~“ <u>Odůvodnění:</u> Poskytovatelé strategicky významných služeb, kteří jsou povinnými osobami podle zákona č. 181/2014 Sb., mají klasifikovaná aktiva a u řady těchto aktiv může být dopad narušení bezpečnosti informací ohodnocen úrovní vysoká, aniž by přitom bylo přiměřené u těchto aktiv aplikovat mechanismus prověřování. Přijetí nového zákona přitom nebude odůvodňovat samo o sobě změnu hodnocení dopadu narušení bezpečnosti informací na tato aktiva. Je proto namístě aplikovat tento mechanismus pouze na aktiva s hodnocením dopadu úrovní kritická. Omezení kritické části stanoveného rozsahu pouze na aktiva s hodnocením dopadu úrovní kritická přitom nevytváří riziko nedostatečného zahrnutí klíčových aktiv. Předkladatel sám pojmenoval onu část stanoveného rozsahu, kterou chce prověřovat, jako „kritickou část stanoveného rozsahu“. Přitom aktiva, která mají být předmětem prověřování jejich dodavatelů, jsou taková, u kterých bylo ohodnocené poskytovatelem strategicky významné služby jejich případné ohrožení bezpečnosti informací na úrovni vysoká nebo kritická. Dle přesvědčení HK ČR postačí, když budou předmětem prověřování pouze aktiva, u nichž poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotí dopad narušení bezpečnosti informací na stanovených rozsah strategicky významné služby na úroveň kritická. Zároveň je HK ČR přesvědčena, že identifikace podle prováděcího právního předpisu postačuje k tomu, aby předkladatel dosáhl zamýšleného cíle, tedy že mechanismus bude prověřovat dodavatele aktiv, která jsou kritickou částí stanoveného rozsahu. Je to patrné i z toho, že v tezí vyhlášky jsou nepominutelné funkce stanovené pro síť a služby elektronických komunikací, ale nikoli pro subjekty v	porušeno poskytování služeb koncovým uživatelům. Je pravdou, že jádro sítě je nejvýznamnější z hlediska bezpečnosti a integrity sítě a dostupnosti poskytovaných služeb, ale bez zabezpečené rádiové přístupové sítě pozbývá funkční jádro smysl, jelikož nemůže dojít k propojení koncových zařízení s jádrem, což souvisí s nemožností zajistit dostupnost. Obdobný přístup ke kritičnosti sítí, nehledě na jejich umístění v rámci architektury sítě, zvolilo také Dánsko, dále pak v rámci EU Belgie či Finsko. Co se týče ochrany aktiv stanoveného rozsahu, u kterých poskytovatel tyto ohodnotil úrovní vysoká (v rámci připomínky se jedná o část "vysoká nebo"), tak zde, na základě předešlých zkušeností a zkoumání, NÚKIB konstatuje, že tato aktiva jsou kritická pro fungování strategicky významných služeb. Byť by se striktně jazykovým výkladem dalo dovodit, že je možné do kritického rozsahu sítě zahrnout pouze aktiva s dopadem „kritická“, nelze tak učinit. Co se týče ochrany aktiv stanoveného rozsahu, u kterých poskytovatel tyto ohodnotil úrovní vysoká (v rámci připomínky se jedná o část „vysoká nebo“), tak zde, na základě předešlých zkušeností a poznání (vyplývajících zejména z kontrolní činnosti NÚKIB), NÚKIB konstatuje, že tato aktiva jsou velmi důležitá až kritická pro fungování strategicky významných služeb. Aktiva ohodnocená jako vysoká mají podstatné dopady na primární aktiva, a tím pádem na chod celé strategicky významné služby. Ochrana pouze kritických aktiv by nebyla v plném rozsahu schopna pokrýt bezpečnost strategicky významné služby v doménách dostupnost, důvěrnost i integrity. Připomínka vypořádána.

	ostatních odvětvích stanovených v § 27 odst. 1. HK ČR tak požaduje zrušit zákonné zmocnění předkladatele vydat prováděcí právní předpis stanovující nepominutelné funkce stanoveného rozsahu. Rozsah mechanismu je navíc nutné zaměřit pouze na taková aktiva, u nichž má jejich nedostupnost přímý okamžitý dopad na nedostupnost strategicky významné služby, což je nejvýznamnější hrozba. Předkladatel by měl mít možnost zakázat rizikového dodavatele pro aktiva, jejichž výpadek může způsobit nedostupnost strategicky významné služby. Tento postup je s ohledem na princip proporcionality přiměřený. Navrhované ustanovení ponechává pravomoc předkladatele provádět prověřování rizik spojených s dodavatelem tak, jak přepokládá materiál, odlišně však vymezuje některé pojmy spojené s touto pravomocí. Vzhledem k odlišné koncepci pojmu kritické části stanoveného rozsahu (viz níže), je obsolentním úkonem vydání vyhlášky o nepominutelných funkcích stanoveného rozsahu, jak předpokládá návrh ZKB, proto byla ze znění tohoto návrhu vypuštěna. Pravomoc předkladatele má být realizována, v souladu s návrhem ZKB, prostřednictvím shromažďování a vyhodnocování informací, jež mohou přispět k vyvození závěrů o existenci hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele stanovených prováděcím právním předpisem, a které jsou spojeny s plněním konkrétního dodavatele. Kritéria rizikovosti dodavatele stanoví prováděcí právní předpis – vyhláška, k jejímuž vydání je zmocněn předkladatel v § 55 návrhu ZKB. Jak uvádí předkladatel v důvodové zprávě k návrhu ZKB, cílem mechanismu prověřování bezpečnosti dodavatelského řetězce je umožnit státu identifikovat a vyhodnocovat hrozby spojené jak s orgány nebo osobami, které již jsou dodavateli do infrastruktury poskytovatelů strategicky významné služby, tak s orgány nebo osobami, u nichž se lze domnívat, že by svá plnění do této infrastruktury dodávat mohly, a to s cílem odhalit hrozbu ještě dříve,	

		než bude u strategicky významné služby moci způsobit narušení bezpečnosti informací. S ohledem na velké množství orgánů a osob, které mohou být předmětem prověřování, je stanovena možnost předkladatele prioritizovat činnosti spojené s prověřováním stávajících a potenciálních dodavatelů, tak jak to předpokládá i návrh ZKB, a to s ohledem na možná rizika a dostupné kapacity předkladatele. Odstavec 3 předmětného ustanovení vymezuje pojmy, které navrhovaná právní úprava dále užívá v souvislosti s mechanismem. Pojem „bezpečnostně významná dodávka“, který vymezuje plnění, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů, a „dodavatel bezpečnostně významné dodávky“, který vymezuje okruh orgánů a osob, na jejichž plnění se mohou vztahovat omezení využití v důsledku prověření rizik s nimi spojených, je dle tohoto návrhu shodný se zněním uvedeným v návrhu ZKB, proto se mu text zde nebude věnovat. Změny však v tomto předkládaném návrhu doznal pojem „kritická část stanoveného rozsahu“, který vymezuje aktiva poskytovatele strategicky významné služby, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů. Předkladatel opakovaně deklaroval, že mechanismus se má vztahovat pouze na tu nejkritičtější část strategické infrastruktury. V návrhu ZKB však předkladatel vymezil rozsah mechanismu formou vyhlášky o nepominutelných funkcích, která je výrazně širší, než bylo deklarováno, a například pro oblast telekomunikací obsahuje jak ty nejkritičtější části sítě (jako je jádro sítě – „core“), tak i méně kritické části sítě (jako je např. rádiová přístupová síť) nebo aktiva, která nemají přímý vliv na nedostupnost regulovaných služeb (např. fakturační systém). V návrhu ZKB i důvodové zprávě k němu zcela chybí odůvodnění, proč jsou kritické části stanoveného rozsahu aktiv definovány tak široce. V předkládaném návrhu je stanovena nová úprava kritické části stanoveného rozsahu aktiv tak, aby se jednalo pouze o aktiva	

	ohodnocená povinnými subjekty na úrovni kritická, jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby. Předkládaný návrh vychází z předpokladu, že kritická část stanoveného rozsahu se skládá z podmnožiny aktiv strategicky významných služeb, u kterých si poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu upravujícího bezpečnostní opatření poskytovatele regulované služby v režimu vyšších povinností sám v rámci plnění povinností podle § 13 návrhu ZKB ohodnotí dopad narušení bezpečnosti informací úrovni kritická. Kritické části strategické infrastruktury jsou transparentně rozděleny dle úrovně hrozby a dopadů její případné realizace. Nejvýznamnější hrozbou je výpadek regulované služby – rozsah mechanismu tak byl v návrhu omezen výlučně na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro příklad – pro oblast telekomunikací se jedná zejména o jádro sítě, případně části přenosové sítě. Úprava je formulována obecněji, aby se vztahovala na všechny oblasti, nejen telekomunikace. Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je přiměřené, aby byla dána možnost státu okamžitým zásahem omezit či zakázat vybraného dodavatele, u kterého identifikuje významnou hrozbu. Pro zbylé části aktiv strategicky významné služby, které nemohou ze své podstaty způsobit nedostupnost služby na kritické úrovni, je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika, která v rámci opatření obecné povahy identifikuje předkladatel. Předkladatel by přitom (jako doposud) nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by měla být nově upravena zvláště v bezpečnostní dokumentaci, kterou by poskytovatel strategicky významné služby měl povinnost každoročně aktualizovat (blíže viz odůvodnění § 30 návrhu níže).	

697. Hospodářská komora ČR	Z	Připomínka k § 28 odst. 3 písm. c) HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text § 28 odst. 3 písm. c) upraven takto: <i>„c) dodavatelem bezpečnostně významné dodávky ten, kdo poskytovateli strategicky významné služby poskytne přímo či jako ~~poddodavatel~~ bezpečnostně významnou dodávku.“</i> <u>Odůvodnění:</u> V současné podobě návrhu bude subjektem mechanismu prakticky každý lokální a regionální subjekt, který poskytuje provozovateli „kritické součásti stanoveného rozsahu“ velkoobchodně jakoukoli bezpečnostně významnou dodávku podle § 28 odst. 3 písm. b), což je ale fakticky jakákoli služba, protože předkladatel definuje aktiva natolik široce, že „kritickou částí stanoveného rozsahu“ je podle návrhu fakticky celá síť poskytovatele sítě či služby elektronických komunikací. Důsledkem toho je, že mechanismus nedopadne jen na subjekty, u kterých to předkladatel dle důvodové zprávy předpokládá, ale na stovky dalších subjektů. Předkladatel nebere v úvahu fakt, že sektor elektronických komunikací je extrémně propojen řadou dodavatelsko-odběratelských vztahů. Protože předkladatel definuje mechanismus extrémně široce fakticky jako celou síť, budou regulovanými subjekty i stovky malých a středních regionálních a lokálních operátorů, kteří poskytují velkoobchodní služby velkým národním operátorům. Zjevně jim neposkytují „kritickou“ službu (typicky pronájem vlákna či propoj základnové stanice s nějakým koncentračním bodem), ale přesto budou předmětem tlaku na změnu dodavatele od svých větších obchodních partnerů, protože budou součástí „kritické části stanoveného rozsahu“. To bude mít zásadní vliv na podnikání malých a středních regionálních firem, který není zohledněný v RIA (která má dle obecných zásad pro hodnocení dopadů regulace hodnotit dopad na podnikatelské prostředí „zejména	Neakceptováno - nyní § 29 Z hlediska strategických hrozeb pro kybernetickou bezpečnost státu a strategicky významných služeb je nutno posuzovat jak dodavatele, tak také poddodavatele, jelikož skrz tyto může například dojít k provedení stejného vektoru útoku, vzhledem k tomu, že oba mají obdobné až stejné možnosti a stejný vliv v rámci dodavatelského řetězce jako celku. Je nasnadě zmínit, že z hlediska strategické bezpečnosti státu a strategicky významných služeb plynou tak ze strany dodavatele i poddodavatelů totožná rizika, v rámci bezpečnosti dodavatelského řetězce obdobné možnosti zásahu do bezpečnostně významných dodávek. Z tohoto důvodu je zákonná šíře taková, jak je uvedena v § 29. Připomínka vypořádána.

	s ohledem na osoby samostatně výdělečně činné a malé a střední podniky“). Ostatně i z tohoto důvodu HK ČR požaduje změnit § 28 odst. 3 písm. a) skutečně jen na kritické části sítě, jak je uvedeno v předcházející připomínce. Je třeba blíže specifikovat úroveň dodavatelského řetězce, do které jsou poskytovatelé strategicky významných služeb povinni zjišťovat informace dle § 32 odst. 1 písm. a). V souladu s cílem a účelem předmětné úpravy je přiměřené, aby poskytovatel strategicky významné služby zjišťoval informace nejen o primárním dodavateli, kterým bude často pouze distributor, ale také o přímém výrobcí daného produktu nebo poskytovateli služby ve vztahu, ke kterým je stěžejní prověřit rizikovost. Navrhované znění však lze vykládat i jako povinnost zjišťovat informace i o dodavatelích jednotlivých komponent daného výrobku (polovodičových prvků) nebo dodavatelích dílčích programových prostředků (licencí), pomocí kterých je poskytována služba přímým dodavatelem. Taková povinnost pro poskytovatele strategicky významných služeb by byla nepřiměřená a není opodstatněna bezpečnostními riziky, která jednotlivé komponenty či programové vybavení představují pro kybernetickou bezpečnost regulované služby. Taková hloubka prověřování by naopak byla přiměřená v případě služeb elektronických komunikací, kde by poskytovatelé strategicky významných služeb měli zjišťovat informace o dodavatelích použité infrastruktury, jakožto bezpečnostně významných dodavatelích, přičemž by měli promítnout opatření obecné povahy spočívající v zákazu nebo stanovení podmínek využívání plnění bezpečnostně významného dodavatele i na dodavatele infrastruktury pro využívané služby elektronických komunikací. Vypořádání připomínky z veřejné konzultace se nevyrovnává s různorodou povahou poddodavatelů pospanou výše (dodavatele	

		software vs. komponent). Ze skutečnosti, že hloubka prověřování musí být přiměřená, neplyne možnost některé dodavatele, kteří nemají význam z hlediska kybernetické bezpečnosti, zcela ignorovat. Touto úpravou se tento mechanismus omezí pouze na přímé dodavatele povinných osob, a nikoliv i dalších nepřímých poddodavatelů. Tímto zúžením počtu subjektů, na něž bude dopadat předmětná úprava, dojde k omezení této zásadní administrativní zátěže. Zároveň se předejde situaci, kdy např. povinnosti z předmětné úpravy budou muset plnit také dodavatelé poddodavatelů apod.	
698. Hospodářská komora ČR	Z	Připomínka k § 28 odst. 4 HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text § 28 odst. 4 vypuštěn z důvodů uvedených níže. <u>Odůvodnění:</u> Odůvodnění se částečně shoduje s odůvodněním uvedeným v připomínce k § 28 odst. 3 písm. a) a navíc je nutno zdůraznit, že navrhované znění zakládá právní nejistotu pro poskytovatele strategicky významných služeb i bezpečnostně významné dodavatele, protože kritéria hodnocení rizikovosti se mohou v budoucnu významně a snadno změnit změnou vyhlášky. Navrhované znění v tomto směru pro obsah vyhlášky nestanoví žádné limity. Ponechání této kompetence v rukou moci výkonné, nikoli zákonodárné, by vedlo k nepřiměřené koncentraci pravomocí v rukou jednoho z orgánů veřejné moci, nesouladné s principem dělby moci, která je v demokratickém právním státě nezbytná. Nelze přitom akceptovat vypořádání připomínky z veřejné konzultace, dle kterého je úprava kritérií formou podzákoného právního předpisu běžnou legislativní praxí. Podstata hodnocení bezpečnosti dodavatelského řetězce a dostupná opatření se závažností dopadu blíží opatřením podle zákona č. 34/2021 Sb. o prověřování zahraničních investic, přičemž zde jsou základní parametry hodnocení	Akceptováno jinak - nyní § 29 Odůvodnění připomínky hovoří o nevhodnosti úpravy kritérií hodnocení rizikovosti dodavatele, v tomto ohledu bylo připomínce zcela vyhověno a vyhláška byla zrušena, zmocnění k jejímu vydání vypuštěno. Je nasnadě zmínit, že úprava nepominutelných funkcí ve vyhlášce představuje proporcionální řešení konfliktu mezi uvážením NÚKIB a vymezením funkcí na úrovni zákona. Všechny vyhlášky prochází takovým legislativním procesem, aby k nepřiměřené koncentraci pravomocí nedocházelo. Připomínka vypořádána.

		rovněž stanoveny zákonem. Současně již nyní navrhovaná kritéria jsou svou povahou obecná, lze proto očekávat minimum jejich změn. K jejich vyčlenění do prováděcího právního předpisu tedy není racionální důvod. S ohledem na závažný ekonomický i provozní dopad na poskytovatele regulované služby tedy nelze akceptovat model, kdy by kritéria byla stanovena vyhláškou.	
699. Hospodářská komora ČR	Z	Připomínka k § 29 HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl v § 29 odst. 1 a 2 výčet orgánů, které jsou povinny poskytovat předkladateli informace a součinnost, rozšířen o Český telekomunikační úřad, případně obecné odvětvové regulátory, text § 29 odst. 3 vypuštěn (odst. 4 přečíslován na odst. 3), to vše ve smyslu níže uvedeného odůvodnění. <u>Odůvodnění:</u> Zákon o kybernetické bezpečnosti a související předpisy významně dopadají na poskytovatele regulovaných služeb v oblasti služeb elektronických komunikací. Přesto navrhované znění výslovně nezmiňuje mezi orgány poskytujícími součinnost Český telekomunikační úřad (jakkoli jej lze považovat za „orgán“ podle odst. 3). ČTÚ má přitom ve vztahu k oblasti služeb elektronických komunikací největší odbornost, dohlíží nad bezpečností a integritou komunikačních sítí a ukládá opatření k řešení hrozeb (§ 98 zákona č. 127/2005 Sb., o elektronických komunikacích), díky čemuž disponuje řadou informací významných z hlediska technologií, které je pro zajištění bezpečnosti dodavatelského řetězce třeba zohlednit (zejména z hlediska nepominutelných funkcí stanoveného rozsahu). Navrhované znění explicitně neomezuje okruh dalších orgánů a osob, které jsou povinny poskytnout předkladateli informace a součinnost.	Neakceptováno - nyní § 30 Dle návrhu zákona NÚKIB, v rámci získávání informací, spolupracuje s relevantními orgány státu, přičemž v případě jednotlivých sektorů pak zákon v podobě, jaké je dnes, tuto spolupráci předpokládá s regulátory jednotlivých sektorů, je-li to možné. Toto je zaručeno mimo jiné § 8 odst. 2 zákona č. 500/2004 Sb., správního řádu. Dále je tento postup dán principem dobré správy, kdy NÚKIB pro co nejlepší vyhodnocení situace a možných dopadů počítá s dožádáním informací od relevantních orgánů státu v rámci jednotlivých odvětví. Důvodem, proč jsou v navrhovaném zákoně popsány orgány, které jsou obsaženy v § 30, je ten, že tyto fungují napříč jednotlivými sektory a jejich spolupráce je tak pro správné posouzení rizik, včetně následujícího vyhodnocení pro případné omezení či zákaz, žádoucí. Připomínka vypořádána.

		To vytváří potenciál k zatížení povinných osob mechanismu prověřování dodatečnými povinnostmi k poskytování údajů, typicky v reakci na hlášení podle § 32 odst. 1 písm. b), a tak faktické rozšiřování výčtu údajů podle § 4 odst. 4 Vyhlášky o portálu NÚKIB. Okruh osob a orgánů povinných k součinnosti vůči NÚKIB v této oblasti by měl být stanoven taxativně.	
700. Hospodářská komora ČR	Z	Připomínka k § 30 HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text § 30 upraven takto: „§ 30 <i>Omezení rizik spojených s dodavatelem</i> ~~(1) Úřad vydá opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, zjistí-li na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Lhůtu pro zohlednění podmínek nebo zakazu obsaženého v opatření obecné povahy stanoví Úřad s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby.~~ ~~(2) Návrh opatření obecné povahy podle odstavce 1 Úřad po projednání s ostatními orgány uvedenými v § 29 odst. 1 a 2 a Ministerstvem financí předloží Bezpečnostní radě státu~~ ~~a) pro informaci, jestliže lhůta pro zohlednění podmínek nebo zakazu obsaženého v opatření obecné povahy pro stávající či minulá plnění dodavatele bezpečnostně významné dodávky~~ ~~1. je stanovena podle doby odpisování podle právního předpisu upravujícího zdanění příjmu⁴⁾, jestliže ji tento~~	Neakceptováno – nyní § 31 Do procesu je zapojena Bezpečnostní rada státu, ve které jsou členové vlády zastoupeni. Jedná se o bezpečnostní orgán, který zastupuje bezpečnostní zájmy státu. V případě potřeby může samozřejmě problém eskalovat až na vládní úroveň. S tím také souvisí procesní stránka věci, kdy Bezpečnostní rada státu může návrh opatření obecné povahy v případě, že je jí předložen, neprojednat, přerušit jeho projednávání, vrátit jej k přepracování, případně s ním vyjádřit nesouhlas. Jakékoliv rozhodnutí je pro Úřad samozřejmě závazné. Předmětné ustanovení bylo nicméně v návaznosti na připomínky k němu dále rozpracováno a upraveno. Připomínka vypořádána.

		~~právní předpis ve vztahu k dotčené bezpečnostně významné dodávce stanoví, nebo~~ ~~2. je alespoň 5 let, nebo~~ ~~b) k projednání, jestliže lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy pro stávající či minulá plnění dodavatele bezpečnostně významné dodávky~~ ~~1. není stanovena podle doby odpisování podle právního předpisu upravujícího zdanění příjmu⁴⁾, jestliže ji tento právní předpis ve vztahu k dotčené bezpečnostně významné dodávce stanoví, nebo~~ ~~2. je kratší než 5 let.~~ ~~(3) Po informování členů Bezpečnostní rady státu podle odstavce 2 písmene a) nebo po projednání podle odstavce 2 písm. b) Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu opatření obecné povahy podávali připomínky. Lhůta pro podání připomínek činí 30 dnů, nestanoví-li Úřad jinak. Ustanovení § 172 odst. 1 a 5, § 173 odst. 1 věty první, část věty za středníkem, a § 173 odst. 1 věty druhé správního řádu se pro postup podle tohoto ustanovení nepoužijí.~~ ~~(4) Úřad přezkoumá alespoň jednou za 3 roky trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 1. Zjistí-li Úřad, že tyto skutečnosti pominuly, zruší opatření obecné povahy podle odstavce 1 postupem podle odstavce 1 a 2 obdobně~~ ~~(1) Zjistí-li Úřad na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, předloží věc k projednání Vládě České republiky (dále jen "Vláda"). Před předložením věci Vládě je Úřad povinen vyhotovit odhad nákladů povinných osob spojených se zavedením omezení či zákazu plnění dodavatele, který je nedílnou součástí~~	

		<i>dokumentace předkládané Vládě. Poskytovatel strategicky významné služby je povinen na výzvu poskytnout Úřadu potřebnou součinnost.</i> <i>(2) Vláda přijme do 45 dnů ode dne, kdy jí byla věc předložena k projednání, usnesení o tom, zda plnění dodavatele může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Při posuzování věci Vláda zohlední soulad případného plnění dodavatele s principy demokratického právního státu, dopad na ochranu života a zdraví obyvatel, obranu státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku.</i> <i>(3) V návaznosti na usnesení vlády, že plnění dodavatele představuje významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, vydá Úřad opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu. Při stanovení podmínek dle předchozí věty je Úřad povinen přijmout vždy jen takové podmínky, které budou pro jejich adresáty nejméně zatěžující při zachování účelu odvrácení významného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. K zákazu využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu může Úřad přistoupit jen tehdy, nelze-li významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku odvrátit pouhým stanovením podmínek dle věty první tohoto odstavce.</i> <i>(4) Usnesení vlády je pro Úřad závazné a vydání opatření obecné povahy omezující či zakazující plnění dodavatele bezpečnostně</i>	

		<i>významné dodávky v kritické části stanoveného rozsahu je vydáním usnesení Vlády podmíněno.</i> <i>(5) Zakáže-li nebo omezí-li Úřad opatřením obecné povahy dle odstavce 3 plnění dodavatele, určí zároveň v opatření obecné povahy přiměřenou lhůtu zákazu nebo zohlednění podmínek plnění dodavatele. Lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy stanoví Úřad tak, aby tato lhůta byla pro poskytovatele strategicky významné služby nejméně zatěžující, při zachování účelu odvrácení významného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Úřad vždy musí lhůtu předem konzultovat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele.</i> <i>(6) Před vydáním opatření obecné povahy je Úřad povinen projednat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele, zda návrh opatření obecné povahy a jeho možné dopady neohrozí plnění povinností stanovených a vyplývajících ze zvláštních právních předpisů. Úřad je povinen při vydání opatření obecné povahy stanovisko ústředního orgánu státní správy zohlednit.</i> <i>(7) Jestliže zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle odstavce 3 může ohrozit poskytování strategicky významné služby anebo představuje bezprostřední hrozbu kybernetického bezpečnostního incidentu, který podstatným způsobem ohrožuje poskytování strategicky významné služby, je poskytovatel strategicky významné služby povinen plnit opatření obecné povahy až po pomnutí takové hrozby.</i> <i>(8) Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu opatření obecné povahy</i>	

		podávali připomínky. Lhůta pro podání připomínek činí 30 dnů, nestanoví-li Úřad jinak. Ustanovení § 172 odst. 1 a 5, § 173 odst. 1 věty první, část věty za středníkem, a § 173 odst. 1 věty druhé správního řádu se pro postup podle tohoto ustanovení nepoužijí. (9) V případě vydání opatření obecné povahy odstavce 3 musí poskytovatel strategicky významné služby provést analýzu rizik spojených s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3 pro aktiva strategicky významné služby, která nezařadil do kritické části stanoveného rozsahu podle § 28 odst. 3 písm. a). (10) Na základě analýzy rizik vypracuje poskytovatel strategicky významné služby plán zvládnutí rizik dle odstavce 9, v němž uvede bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3. Plán zvládnutí rizik je poskytovatel strategicky významné služby povinen aktualizovat alespoň jednou za kalendářní rok. (11) Úřad přezkoumá alespoň jednou za 3 roky trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 3. Zjistí-li Úřad, že tyto skutečnosti pominuly, opatření obecné povahy zruší. (12) Opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu lze vydat nejvýše na dobu v délce trvání tří let ode dne konce lhůty pro zohlednění podmínek nebo zákazu obsaženého v daném opatření obecné povahy.“ <u>Odůvodnění:</u> HK ČR je přesvědčena, že není možné, aby do procesu omezování dodavatele, což je fakticky velmi zásadní a závažný zásah do svobody podnikatelského prostředí, byl zapojen pouze předkladatel a ostatní státní orgány, především ty s politickou odpovědností, byly zapojené	

		v procesu pouze okrajově poskytováním součinnosti či poskytováním informací. Problematika mechanismu prověřování bezpečnosti dodavatelského řetězce už jde daleko za hranice kybernetické bezpečnosti, ale směřuje k obecnému prověřování hrozeb pro bezpečnost České republiky, její vnitřní a veřejný pořádek. V samotném návrhu se píše v § 28 odst. 1: “Úřad shromažďuje a vyhodnocuje informace a data spojené s orgánem či osobou, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele“. I kritéria pro hodnocení rizikovosti dodavatelů určená ve vyhláškách se vůbec nezaměřují na kybernetickou bezpečnost, na technologie nebo služby, ale čistě na vyhodnocení právního a politického prostředí země mající vliv na dodavatele a na osobu dodavatele. Pro oblast vnitřního a veřejného pořádku a bezpečnosti České republiky je ústředním orgánem státní správy Ministerstvo vnitra. Problematika prověřování bezpečnosti dodavatelského řetězce se dotýká i pravomocí dalších ústředních orgánů státní správy – zahraničního obchodu, hospodářské soutěže, bezpečnosti a integrity služeb veřejných komunikačních sítí a služeb elektronických komunikací. Omezení dodavatele je vysoce politickým krokem, který může mít zahraničněpolitické i ekonomické dopady, a spolurozhodovat by tak měly orgány s politickým mandátem. Do procesu posuzování dodavatele tak HK ČR požaduje (analogicky k zákonu o prověřování zahraničních investic) zapojit vládu (odstavec 1-4) a sektorové regulátory (odstavec 5-6) Obdobně je tato problematika řešena na Slovensku v rámci § 27a odst. 3 zák. č. 69/2018 Z. z., o kybernetické bezpečnosti. Podle slovenské právní úpravy Národní bezpečnostní úřad Slovenska před vydáním rozhodnutí o omezení dodavatele, produktu, služby nebo procesu vyhotoví analýzu rizik na základě a v součinnosti s ostatními ústředními orgány státní správy, zpravodajskými službami a připraví návrh rozhodnutí. Návrh rozhodnutí potom předloží Bezpečnostní radě Slovenska a vládě. Od stanoviska vlády se potom Národní	

		bezpečnostní úřad nemůže odchýlit. Navrhuje se řešit tuto problematiku v rámci českého návrhu zákona obdobně. Navrhovaný § 30 obsahuje navíc další bezpečnostní opatření, kterými poskytovatel strategicky významné služby musí pro aktiva nezařazená jím do kritické části stanoveného rozsahu provést analýzu rizik. V nich musí zohlednit rizika, která předkladatel uvedl v opatření obecné povahy a vypracovat plán zvládání rizik, jehož součástí jsou i bezpečnostní opatření minimalizující rizika spojená s dodavatelem. Jak je uvedeno ve zprávě o hodnocení dopadů, cílem prověřování rizik spojených s dodavatelem je minimalizace ekonomických dopadů a omezení pouze na kritickou část síťové infrastruktury. Pokud je cílem vymezit pouze kritickou část strategické infrastruktury, mělo by se jednat o aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je tedy vhodné, aby byla možnost státu okamžitým zásahem zakázat vybraného dodavatele, u kterého identifikuje významné hrozby. Pro zbylé části aktiv strategicky významné služby je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika, která v rámci opatření obecné povahy identifikoval regulátor. Regulátor by jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by nově byla upravena zvlášť v bezpečnostní dokumentaci, kterou by poskytovatel měl povinnost ročně aktualizovat. Nově je navrženo zapojení Vlády ČR do procesu vydávání opatření obecné povahy. Je nezbytné, aby v případě vyhodnocování hrozeb měla Vláda možnost posoudit dopady úkonů předkladatele na principy demokratického právního státu, ochranu života a zdraví obyvatel, obrany státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti	

	důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Lhůtu plnění povinností poskytovatele z opatření obecné povahy je navrženo stanovovat na základě délky životního cyklu aktiv bezpečnostně významné dodávky, která je vyjádřena účetními odpisy jednotlivých aktiv. V případě, že je takové lhůta zkrácena, znalec stanoví výši náhrady. Nový návrh ustanovení § 30 návrhu ZKB zakotvuje možnost omezit nebo zakázat využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, a to zjistí-li Úřad postupem podle § 28 odst. 1 návrhu ZKB, že může být významně ohrožena bezpečnost České republiky nebo vnitřní či veřejný pořádek. Jak již bylo uvedeno, oproti návrhu ZKB je do procesu prověřování rizik spojených s dodavatelem zapojena vláda. Zapojení vlády v procesu prověřování rizikovosti dodavatele je zásadně smysluplné a důležité, a to jak z hlediska transparentnosti a objektivity rozhodování, tak vzhledem k závažnosti opatření obecné povahy, které na základě uvedeného ustanovení zákona může být vydáno. Případný zákaz či omezení plnění dodavatele musí vždy být až nejzazším řešením – představuje totiž značný zásah do ústavně zaručených práv a povinností jednotlivých subjektů, i proto musí být podmíněn právě usnesením vlády. Je třeba podotknout, že vláda do jisté míry v současnosti již do posuzování rizikovosti dodavatele (resp. investora) zapojena je, a to dle zákona č. 34/2021 Sb., o prověřování zahraničních investic. Dle zákona o prověřování zahraničních investic jsou přijetím usnesení vlády podmíněna rozhodnutí omezující či zakazující zahraniční investici, a to právě s ohledem na míru zásahu do práv dotčených subjektů v důsledku tohoto omezení či zákazu. Začlenění vlády do procesu prověřování rizikovosti dodavatele má tedy pevné základy již v aktuálně účinné právní úpravě a rozhodnutí o omezení či zákazu plnění dodavatele by mělo být podmíněno usnesením vlády (obdobně jako u zahraničních investic), a to zejména s ohledem na to, že plošný	

	zákaz či omezení plnění dodavatele může mít mnohem větší dopad na trh než zákaz doposud neuskutečněné investice. Řešení otázky dodavatelského řetězce zasahuje do vícero oblastí, nejen do oblasti bezpečnostní. Pouze vláda může posoudit jak geopolitické a ekonomické dopady věci, tak i bezpečnostní aspekty – ostatně takto to činí již dle zákona o prověřování zahraničních investic, kdy vláda posuzuje, zda je případné omezení či zákaz zahraniční investice nutný z důvodu ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku, přičemž při posuzování jsou hodnocena i strategická kritéria, jako je hodnocení investorů z hlediska země jejich původu (např. zda je zahraniční investor ovládán přímo či nepřímo vládou třetí země, či zda již byl zapojen do činností ovlivňujících bezpečnost nebo veřejný pořádek v některém členském státě EU). Právě z důvodu komplexnosti celé problematiky a přesahu do rozličných oblastí není vhodné, aby věc byla konzultována pouze s Bezpečnostní radou státu, jejímž předmětem činnosti je výhradně koordinace problematiky bezpečnosti České republiky, jak navrhuje návrh ZKB. Nadto je třeba uvést, že usnesení vlády jsou závazná zásadně šířeji, než usnesení Bezpečnostní rady státu (usnesení vlády zavazují všechny členy vlády, ministerstva, jiné ústřední orgány státní správy, ostatní správní úřady a další subjekty, pokud tak stanoví zvláštní zákon, zatímco v případě usnesení Bezpečnostní rady státu je závazná pouze jeho ukládací část (jen v oblasti zajišťování bezpečnosti České republiky), a to pouze pro určené členy vlády a vedoucí jiných správních úřadů). Vedle zapojení vlády počítá předkládaná připomínka rovněž s účastí sektorových regulátorů (příslušných ústředních orgánů státní správy), jejichž pozice je v návrhu ZKB značně opomíjena, je však v procesu prověřování zcela zásadní. Právě příslušní sektoroví regulátoři disponují potřebným penzem informací a odborných znalostí o fungování a činnosti daného regulovaného sektoru a jsou schopni posoudit reálné dopady případného omezení či zákazu plnění dodavatele, jakož i přesah do oblasti úpravy zajišťované zvláštními	

		právními předpisy pro daný sektor (např. ohrožení plnění povinností subjektů stanovených těmito zvláštními právními předpisy). V návaznosti na usnesení vlády a konzultaci se sektorovými regulátory, je dáována předkladateli pravomoc vydat konkrétní omezení formou opatření obecné povahy, kterým se budou muset řídit všichni poskytovatelé strategicky významných služeb. Toto opatření obecné povahy však musí být přijato na základě usnesení vlády a zohledňovat stanovisko příslušného sektorového regulátora. S ohledem zákonnou nemožnost procesní obrany proti opatření obecné povahy po uplynutí lhůty jednoho roku od jeho vydání, navrhuje HK ČR limitovat trvání opatření obecné povahy na tři roky s tím, že v případě trvání důvodů, pro které bylo opatření vydáno, bude jeho obsah vydán ve formě nového opatření, které bude moci být opětovně přezkoumáno soudy. Proces prověřování rizikovosti dodavatele je dle obsahu připomínky nastaven následovně: Pokud předkladatel na základě vyhodnocení kritérií rizikovosti dospěje k závěru, že plnění dodavatele může představovat významné ohrožení bezpečnosti anebo vnitřního či vnějšího pořádku České republiky, předloží věc k projednání vládě. Vzhledem k tomu, že možné opatření omezující či zakazující plnění konkrétního dodavatele může mít rozsáhlé dopady nejen na dodavatele samého, ale i na povinné osoby (poskytovatele strategicky významných služeb), jichž se opatření obecné povahy dotýká, bude předkladatel ještě před předložením věci vládě povinen vypracovat odhad nákladů spojených s implementací povinností stanovených v opatření obecné povahy povinnými osobami. Tento podklad je zásadní pro samotnou vládu, aby mohla věc posoudit ve všech souvislostech a učinit informované rozhodnutí s vědomím veškerých hrozících dopadů. Za účelem vypracování odhadu nákladů jsou poskytovatelé strategicky významné služby povinni předkladateli poskytnout potřebnou součinnost.	

		Vláda bude mít následně k dispozici lhůtu 45 dnů k projednání a vydání usnesení o tom, zda plnění dodavatele může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, přičemž při posuzování věci vláda zohledňuje jak možný dopad plnění dodavatele na principy demokratického právního státu, ochranu života a zdraví obyvatel, obranu státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Usnesení vlády bude pro předkladatele vždy závazné a bude jím podmíněno vydání zakazujícího či omezujícího opatření obecné povahy. V návaznosti na usnesení vlády o tom, že plnění dodavatele představuje významné ohrožení, je předkladateli dáвана pravomoc vydat opatření obecné povahy, kterým stanoví podmínky nebo zakáže plnění dodavatele bezpečnostně významné dodávky. Z povahy opatření obecné povahy vyplývá, že jde o opatření, kterým se budou muset řídit všichni poskytovatelé strategicky významných služeb – směřuje však vždy vůči vymezeným plněním daného dodavatele (proti bezpečnostně významné dodávce). Stejně jako v návrhu ZKB, se vydání opatření obecné povahy řídí obecnou právní úpravou obsaženou ve správním řádu, a to s výjimkou ustanovení, která pojmově nejsou příleňavá k problematice prověřování rizikovitosti dodavatele (týkají se typicky nemovitostí a územního rozvoje). Z obecné právní úpravy také vyplývá možnost přezkoumat opatření obecné povahy v přezkumném řízení nebo v soudním řízení správním dle obecné úpravy správního řádu a správního řádu soudního, nelze však proti němu podat opravný prostředek. V rámci omezujícího či zakazujícího opatření obecné povahy předkladatel vždy stanoví i přiměřenou lhůtu pro zohlednění podmínek či zákazu. Pozměněná úprava ukládá, že lhůta musí být vždy stanovena v návaznosti na projednání s příslušnými ústředními orgány státní správy (sektorovými regulátory), do jejichž působnosti náleží strategicky významná služba, do níž směřuje bezpečnostně významné plnění dodavatele, neboť právě sektoroví regulátoři	

	disponují objektivními informacemi, na jejichž základě lze přiměřenou lhůtu stanovit. Je nutné trvat na tom, aby omezení či zákaz stanovený prostřednictvím opatření obecné povahy byly vždy proporcionální a přiměřené a nekolidovaly s právní úpravou obsaženou ve zvláštních právních předpisech. Vzhledem k tomu, že případné omezení či zákaz plnění dodavatele mohou mít významný dopad na schopnost povinných osob plnit své zákonné povinnosti vyplývající ze zvláštních právních předpisů, je za tímto účelem navrhováno, aby předkladatel projednal s příslušnými ústředními orgány státní správy (sektorovými regulátory), do jejichž působnosti náleží strategicky významná služba, do níž směřuje bezpečnostně významné plnění dodavatele, zda návrh opatření obecné povahy a jeho možné dopady neohrozí plnění povinností uvedených ve zvláštních právních předpisech. Například pro oblast telekomunikací jde mj. o výstavbové povinnosti vyplývající ze zákona č. 127/2005 Sb. o elektronických komunikacích. Je tedy zásadní, aby daný sektorový regulátor, v tomto případě Český telekomunikační úřad, měl možnost se k implementaci omezení či zákazu vyjádřit a předkladatel musel k jeho stanovisku přihlédnout. V souladu s návrhem ZKB je i v připomínce pozměněném návrhu zachována povinnost předkladatele pravidelně (nejméně jednou za 3 roky) přezkoumávat trvání skutečností, na jejichž základě bylo vydáno omezení či zákaz, aby byla v případě jejich pominutí bezodkladně zrušena. HK ČR si je vědoma nutnosti zajištění kybernetické bezpečnosti a bezpečnosti informací, a to v celé síti, proto v rámci ustanovení § 30 navrhuje nově zavést taktéž povinnost pro poskytovatele strategicky významné služby provést analýzu rizik spojených s dodavatelem dotčeným opatřením obecné povahy u těch aktiv strategicky významné služby, které poskytovatel strategicky významné služby nezařadil do kritické části stanoveného rozsahu dle § 28 odst. 3 písm. a). Jedná se v podstatě o zavedení jakési kaskády bezpečnostních opatření, kdy pro tu nejkritičtější část strategické infrastruktury, kde	

		hrozí přímý okamžitý dopad na nedostupnost strategicky významné služby, bude uvalena povinnost řídit se případným omezením či zákazem uvedeným v opatření obecné povahy, a pro ty méně kritické části strategické infrastruktury bude nově dána povinnost zohlednit rizika identifikovaná státem a implementovat odpovídající bezpečnostní opatření. Na základě analýzy rizik poskytovatel strategicky významné služby vypracuje plán zvládání rizik, jehož součástí jsou i bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v opatření obecné povahy, který musí pravidelně (alespoň jednou za kalendářní rok) aktualizovat Předkladatel tedy bude moci omezit či zakázat plnění dodavatele v kritické části stanoveného rozsahu tam, kde hrozí nedostupnost strategicky významné služby. Pro zbytek aktiv pak vznikne poskytovatelům strategicky významné služby automaticky povinnost provést analýzu rizik uvedených v opatření obecné povahy i pro aktiva nezařazená do kritické části stanoveného rozsahu a vypracovat strategii zvládání rizik včetně implementace odpovídajících bezpečnostních opatření. HK ČR se domnívá, že takto navržený postup, který vychází z předpokladu účasti vlády na rozhodování (vzhledem k tomu, že se jedná o otázku se zahraničně-politickým přesahem) a konzultacemi se sektorovými regulátory, lze, na rozdíl od postupu stanoveného návrhem ZKB, považovat za proporcionální a vhodný a přiměřený z hlediska dotčených subjektů.	
701. Hospodářská komora ČR	Z	Připomínka k § 30 HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl za text § 30 vložen nový § 31 takto: „§ 31 Náhrada účelně vynaložených nákladů	Neakceptováno – nyní § 31 K dané připomínce uvádíme, že navrhovaný zákon považujeme za ústavně konformní, kvůli čemuž není důvod přidávat ustanovení o náhradě škod. Vzhledem k charakteru navrhované právní úpravy, převážně v oblasti mechanismu bezpečnosti dodavatelského řetězce, která se snaží vyjít vstříc povinným osobám

	(1) <i>V případě, že lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle § 30 odstavce 3 je kratší, než životní cyklus bezpečnostně významné dodávky, nejdéle však 9 let, má každý poskytovatel strategicky významné služby vůči státu právo na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností podle odstavce 3 a to včetně nákladů na náhradu dlouhodobého majetku, který poskytovatel strategicky významné služby v důsledku opatření obecné povahy podle odstavce 3 nemůže dále využívat. Výši účelně vynaložených nákladů podle věty první určí Úřad na základě znaleckého posudku, pro jehož vyhotovení poskytne poskytovatel strategicky významné služby součinnost.</i> (2) <i>Životní cyklus bezpečnostně relevantní dodávky bude znalcem určen na základě účetních odpisů zařízení.</i> (3) <i>Zrušením opatření obecné povahy podle odstavce 11 nezaniká právo na náhradu nákladů podle tohoto odstavce. Ve věci náhrady nákladů podle tohoto odstavce jménem státu jedná Úřad.</i>“ a § 31 až 73 byly přecíslovány na 32 až 74. <u>Odůvodnění:</u> HK ČR je přesvědčena, že není možné, aby do procesu omezování dodavatele, což je fakticky velmi zásadní a závažný zásah do svobody podnikatelského prostředí, byl zapojen pouze předkladatel a ostatní státní orgány, především ty s politickou odpovědností, byly zapojené v procesu pouze okrajově poskytováním součinnosti či poskytováním informací. HK ČR proto navrhuje vložení úpravy náhrady škody, a to podobně, jako je tomu např. v § 16n zákona č. 289/2005 Sb., o vojenském zpravodajství, v němž je přiznána náhrada škody každému, komu škoda nebo nemajetková újma vznikla v souvislosti s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu:	například v otázkách životních cyklů technologií nebo zamezení možné závislosti na jedné technologii skrz systém výjimek, není nutné, aby možnost kompenzací byla upravena přímo v zákoně. Kompenzací se v obdobných případech lze domáhat na základě již existujících zákonných prostředků, které předmětným ustanovením § 31 nejsou jakkoliv dotčeny. Zároveň platí, že pro vydání omezení či zákazu formou opatření obecné povahy budou posuzovány veškeré okolnosti a reálné dopady na trh a podnikatelské prostředí. Z toho důvodu by NÚKIB posuzoval jak životnost jednotlivých technologií, tak například možnosti jednotlivých povinných subjektů či postavení dodavatele na českém trhu apod. Dalším důvodem, proč považujeme zákon za ústavně konformní, je podíl Bezpečnostní rady státu na návrhu opatření obecné povahy, kdy se mají možnost k návrhu vyjádřit jednotliví členové Bezpečnostní rady státu, aby bylo dané riziko a jeho dopady posouzeny relevantním orgánem. Připomínka vypořádána.

	„(1) Každý, komu vznikla škoda nebo nemajetková újma v souvislosti s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu, má právo na jejich náhradu. (2) Fyzické nebo právnické osobě se nahrazuje také škoda nebo nemajetková újma, která jí vznikla v důsledku realizace opatření přijatých Vojenským zpravodajstvím v zájmu provedení aktivního zásahu směřujícího k odstranění kybernetického útoku nebo hrozby v rámci zajišťování obrany státu v kybernetickém prostoru. (3) Povinnost státu k náhradě škody nebo nemajetkové újmy podle odstavců 1 a 2 nevznikne, pokud se jedná o škodu nebo nemajetkovou újmu způsobenou fyzické nebo právnické osobě, která vyvolala útok nebo hrozbu. (4) Za škodu nebo nemajetkovou újmu způsobenou Vojenským zpravodajstvím odpovídá stát. Náhradu škody nebo nemajetkové újmy poskytuje v zastoupení státu Ministerstvo obrany.“ Náhrada škody je upravena v nově navrhovaném ustanovení § 31, podle kterého má poskytovatel strategicky významné služby vůči státu nárok na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností z opatření obecné povahy. Náhrada škody dle předmětného ustanovení je koncipována jako náhrada za nemožnost používání technologie po plnou dobu jejího životního cyklu a konkrétní výše je určována znalcem, a to na základě daňových odpisů, s tím, že by byla určena na základě rozdílu mezi délkou životního cyklu plnění dodavatele a lhůty stanovené předkladatelem pro omezení či odstranění plnění dodavatele. Metoda určení výše náhrady škody dle odpisů se použije právě a jen pro případy náhrady za nemožnost používání dlouhodobého majetku v plném rozsahu. Pokud by tedy např. předkladatel stanovil lhůtu pro odstranění plnění dodavatele v délce 3 roky a životní cyklus plnění dodavatele (technologie) by byl dle daňových odpisů 5 let, mohl by poskytovatel strategicky významné služby požadovat náhradu škody odpovídající 2 zbývajícím rokům odpisů. Pro náhradu dalších účelně	

		vynaložených nákladů vzniklých v důsledku plnění povinností uvedených v opatření obecné povahy se metoda odpisů z povahy věci nevyužije. Pro zajištění větší právní jistoty státu je maximální doba odpisů omezena na 7/9 let, aby nedocházelo k umělému protahování odpisů, pokud dojde ke změně §28 odst. 3 písm. a). V opačném případě je nutné respektovat životnost zařízení okrajových částí sítě, která je zpravidla násobně delší. Pokud bude rozsah regulace nastaven tak, jak je uvedeno v tomto návrhu, lze říci, že kompenzace např. v oblasti telekomunikací nebudou žádné. Ustanovení je však nastaveno tak, že pokud by škoda způsobena byla (například v jiných dotčených sektorech), nebo by došlo k novelizaci zákona a rozšíření rozsahu regulace, existovala by zde zákonná možnost nárokovat náhradu škody, což je zásadně žádoucí z hlediska mitigace případných nákladů povinných osob vzniklých v důsledku reflektování opatření obecné povahy.	
702. Hospodářská komora ČR	Z	Připomínka k § 31 odst. 4 HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byly v § 31 za stávající odst. 4 vložen nový odst. 5 takto: „(5) Veškeré informace týkající se rozhodnutí o povolení výjimky a řízení o povolení výjimky jsou považovány za neveřejné informace.“ <u>Odůvodnění:</u> Vzhledem k citlivosti informací, které jsou v rozhodnutí o povolení výjimky uvedeny, je potřebné zajistit, aby rozhodnutí nebylo veřejně dostupné. S ohledem na potřebu zajištění kybernetické bezpečnosti a ochrany informací, jakož i obchodního tajemství dotčených subjektů, není přípustné, aby bylo rozhodnutí o povolení výjimky veřejně dostupné. Zveřejnění informací o tom, komu a za jakých podmínek byla předkladatelem povolena výjimka, je z hlediska cíle zajištění	Akceptováno jinak - nyní § 32 Již nyní se informace týkající se řízení o povolení výjimky a samotného rozhodnutí považují za informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti podle § 38 nZKB. Zároveň se tyto informace uchovávají mimo spis dle § 66 nZKB. Z těchto důvodů neakceptujeme navrhovanou úpravu, protože by byla nadbytečná. Pro zvýšení jistoty žadatelů, že se k jejich důvěrným informacím nedostanou třetí osoby, došlo k úpravě důvodové zprávy v následujícím znění: „Informace týkající se řízení o povolení výjimky se považují za informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti.“ Dále doplňujeme, že i zákon č. 106/1999 Sb., o svobodném přístupu k informacím, poskytuje ochranu

		kybernetické bezpečnosti, jakož i z hlediska hospodářské soutěže a ochrany údajů zásadně nevhodné a v rozporu se smyslem zákona.	obchodnímu tajemství nebo např. informacím dle § 11 odst. 2 písm. a) zákona č. 106/1999 Sb. Připomínka vypořádána.
703. Hospodářská komora ČR	Z	Připomínka k § 32 odst. 1 HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby bylo slovní spojení „identifikace všech bezpečnostně významných dodávek“ použité v ustanovení § 32 odst. 1 zpřesněno v tom smyslu, že bezpečnostně významnou dodávkou plynoucí z rámcové smlouvy je uzavření rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb jako celku (se specifikací rozsahu rámcové smlouvy), nikoli jednotlivé dílčí plnění (objednávky), a to ve smyslu níže uvedeného odůvodnění. <u>Odůvodnění:</u> V případě, že by každé jednotlivé dílčí plnění (realizovaná objednávka) z rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb, mělo být hlášeno jako samostatná bezpečnostně významná dodávka, byla by na poskytovatele strategicky významné služby kladena neúměrně vysoká administrativní zátěž a stejně tak by byl předkladatel zatížen řadou nadbytečných hlášení bez přidané informační hodnoty. Účel tohoto ustanovení bude naplněn i ve znění navrhované změny, dle které se plnění plynoucí z rámcové smlouvy budou hlásit jako jedna bezpečnostně významná dodávka s určením možného rozsahu plnění. Vypořádání připomínky z veřejné konzultace nereflextuje, že návrh se vztahuje k opakovanému objednávání stejného plnění (zboží) tedy nezměněného bezpečnostního rizika.	Akceptováno jinak - nyní § 33 Souhlasíme, že v případě, kdy se dílčí plnění z rámcové smlouvy nijak nezmění, bylo by nadbytečné každé toto plnění hlásit. Úprava této problematiky na úrovni zákona je však s ohledem na její specifčnost nevhodná. Z těchto důvodů byla upravena DZ k § 33 nZKB následujícím způsobem: „Úřad specifikuje, že vzhledem k účelu ustanovení není v případě rámcových smluv na dodávku určitého výrobku nebo služby žádoucí, aby byla opakovaně hlášena jednotlivá dílčí plnění. Postačí hlášení rámcové smlouvy jako celku. Výjimkou jsou však situace, kdy dojde ke změně v dodavatelském řetězci. Pak je povinností poskytovatele strategicky významné služby, aby tuto změnu Úřadu nahlásil.“ Připomínka vypořádána.
704. Hospodářská komora ČR	Z	Připomínka k § 32 odst. 2	Neakceptováno - nyní § 33

		HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text § 32 odst. 2 doplněn tak, že se doba 1 roku ode dne doručení písemného vyrozumění o zápisu se vztahuje i na povinnost zjišťovat informace podle § 32 odst. 1 písm. a), a to ve smyslu níže uvedeného odůvodnění. <u>Odůvodnění:</u> Přechodné období by se nemělo uplatnit pouze pro povinnost hlásit předkladateli informace, ale i pro povinnost je zjišťovat. Není přiměřené požadovat, aby poskytovatelé strategicky významných služeb zahájili sběr informací bezprostředně po účinnosti zákona, bez stanovení přechodného období. Vypořádání připomínky z veřejné konzultace nereflektuje skutečnost, že plnění povinnosti zjišťovat informace nelze zahájit okamžitě. K okamžiku zápisu do evidence poskytovatelů regulované služby nebude mít poskytovatel strategicky významné služby nastaveny odpovídající smluvní a compliance mechanismy a v případě kontroly bezprostředně po tomto zápisu by čelil riziku významných sankcí ze strany předkladatele. I proto je třeba nastavit odložené plnění povinnosti, aby bylo možné zavést příslušné smluvní a compliance mechanismy.	Smyslem roční přechodné lhůty pro hlášení předmětných informací je mimo jiné umožnit poskytovateli strategicky významné služby nastavit do té doby procesy shromažďování a dokumentace požadovaných informací a tyto informace shromáždit v takové kvalitě, aby měl NUKIB po prvotním hlášení informací co nejpřesnější a nejúplnější informace o významnosti dodavatelů a jejich plnění v celé strategicky významné infrastruktuře a mohl tak bezodkladně zahájit jejich prověřování. Realita pak bude taková, že poskytovatel strategicky významné služby si v prvním roce po písemném vyrozumění o označení regulované služby jako strategicky významné služby v evidenci regulovaných služeb (zde proběhla změna oproti původnímu návrhu, kdy se přechodná lhůta vázala na účinnost zákona) nastaví procesy a začne zjišťovat požadované informace. Tyto pak bude muset nejpozději po roce a deseti dnech nahlásit NUKIB. Není tedy důvod stanovovat přechodnou lhůtu i pro povinnost informace zjišťovat. Poskytovatelé strategicky významné služby budou mít dostatek času i podle stávajícího návrhu. Taktéž se nemusí obávat, že v případě kontroly v prvním roce účinnosti zákona budou sankcionováni za neplnění povinnosti podle § 33 odst. 1 písm. a), pokud prokáží, že si již alespoň začali nastavovat procesy potřebné pro plnění této povinnosti. Připomínka vypořádána.
705. Hospodářská komora ČR	Z	Připomínka k § 33 HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text v § 33 upraven takto:	Akceptováno - nyní § 34 Připomínkované ustanovení předkládaného návrhu zákona bylo upraveno podle požadavků připomínky. Možnost ukončení dlouhodobých závazků tak bude přiznána i soukromým subjektům, které nejsou

		„Poskytovatel strategicky významné služby ~~v postavení zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek~~ může závazek ze smlouvy ~~na veřejnou zakázku~~ vypovědět bez zbytečného odkladu poté, co zjistí, že v jeho plnění nelze pokračovat, aniž by nebylo porušeno opatření obecné povahy podle § 30.“ <u>Odůvodnění:</u> I soukromý subjekt, který není zadavatelem podle zákona o zadávání veřejných zakázek, může mít sjednaný dlouhodobý závazek, při jehož sjednávání nemohl vědět, že jeho dodavatel bude shledán rizikovým dodavatelem. Řada takových závazků může být sjednána před účinností navrhovaného zákona. Pro takové případy je třeba stanovit mechanismy umožňující i takovému soukromému subjektu ukončit sjednaný závazek. Vypořádání připomínky z veřejné konzultace nereflektuje skutečnost, že některé kontrakty na bezpečnostně významné dodávky jsou dlouhodobé a mohly být sjednány před přijetím navrhované právní úpravy, a tedy ji nemohly předvídat a nemusí v nich být obsažen adekvátní výpovědní důvod.	zadavateli podle zákona o zadávání veřejných zakázek. Připomínka vypořádána.
706. Hospodářská komora ČR	Z	Připomínka k § 34 HK ČR požaduje, aby byl text § 34 upraven takto: „(1) Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v ~~rozsahu kritické části stanoveného rozsahu ve stanoveném~~ nezbytném čase, ~~a kvalitě a rozsahu~~ z území České republiky. „(2) Poskytovatel strategicky významné služby v odvětví 16.1 Poskytování veřejně dostupné služby elektronických komunikací a 16.2. Zajišťování veřejně dostupné komunikační sítě elektronických komunikací podle přílohy Vyhlášky o regulovaných službách je povinen zajistit dostupnost jím poskytované strategicky významné služby poskytování veřejně dostupné mobilní služby elektronických komunikací nebo	Akceptováno jinak – nyní § 35 Připomínkované ustanovení § 35 bylo v odst. 1 upraveno tak, že „Poskytovatel strategicky významné služby je povinen zajistit její dostupnost v nezbytném rozsahu ve stanoveném čase a kvalitě z území České republiky.“ Tento nezbytný rozsah pak bude stanoven vyhláškou Úřadu. V této vyhlášce bude specifičtější rozvedeno, co se v telekomunikačním sektoru rozumí nezbytným rozsahem při zajištění dostupnosti těchto služeb z území ČR. V případě veřejné správy budou stanovena kritéria dopadu kybernetického bezpečnostního incidentu v podobě narušení dostupnosti služby a nezbytným rozsahem pak budou jen ty služby veřejné správy,

		<i>zajišťování veřejné mobilní komunikační sítě elektronických komunikací a nebo poskytování veřejně dostupné služby elektronických komunikací v pevném místě, a to v rozsahu kritické části stanoveného rozsahu a ve stanoveném čase a kvalitě z území České republiky.“</i> (23) Poskytovatel strategicky významné služby je povinen testovat schopnost zajištění poskytování strategicky významné služby podle odst. 1 a 2 ~~v rozsahu kritické části stanoveného rozsahu z území České republiky nejméně jednou za dva roky.~~ (34) Poskytovatel strategicky významné služby začne plnit povinnosti uvedené v odst. 1 ~~a 2~~ až 3 pro každou strategicky významnou službu nejpozději do jednoho roku ode dne doručení vyrozumění o zápisu strategicky významné služby do evidence poskytovatelů regulovaných služeb nebo od doručení rozhodnutí o určení strategicky významné služby podle § 27 odst. 2. (45) ~~Stanovený~~ Nezbytný čas, ~~a~~ kvalitu a rozsah služby stanoví poskytovatel regulované služby v závislosti na cílech řízení kontinuity činností podle prováděcího právní předpisu. (56) Pro potřeby tohoto ustanovení je kritická část stanoveného rozsahu vymezena v § 28 odst. 3 písm. a). <u>(7) Pokud je pro strategicky významnou službu orgánu veřejné správy využíván informační systém veřejné správy^{x)}, pro který je využíván cloud computing, musí být dostupnost takového informačního systému státní správy na území České republiky pro účely zajištění dostupnosti strategicky významné služby dle odst. 1 zajištěna pouze pro informační systémy veřejné správy zařazené do nejvyšší bezpečnostní úrovně.</u> ^{x)} <i>Ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů.“</i> <u>Odůvodnění:</u>	které budou naplňovat tato kritéria dopadu. Přičemž ta budou zhruba odpovídat kritériím dopadu na úrovni kritická podle vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy. Připomínka vypořádána.

		Ustanovení § 34 návrhu zákona stanoví povinnosti na zajištění dostupnosti strategicky významných služeb z území České republiky. Pro veřejnou správu je strategicky významná služba definována jako „výkon svěřených pravomocí“ ze strany vymezených orgánů státní správy a samosprávy. Vymezený okruh orgánů je velmi široký a zahrnuje mimo jiné všechny ústřední orgány státní správy, správní úřady s celostátní působností, kraje, větší obce s rozšířenou působností, vysoké školy, orgány soudní moci a policejní útvary a dalších orgány (dále označovány také jako „orgány veřejné moci“). Dostupnost na území České republiky musí být podle navrhované právní úpravy zajištěna pro všechna aktiva, u kterých by narušení bezpečnosti informací mělo kritický a vysoký dopad na výkon kterékoli agendy svěřené těmto orgánům. Tato povinnost by se tak v praxi vztahovala na převážnou většinu informačních systémů v české státní správě a samosprávě. Ačkoliv hlavním cílem nového zákona o kybernetické bezpečnosti má být implementace směrnice NIS 2, požadavek na zajištění dostupnosti služeb z území České republiky nemá ve směrnici žádnou oporu a jde nad rámec její implementace do českého právního řádu. Lze i dovozovat, že tento požadavek může být v rozporu s přeshraniční spoluprací v rámci Evropské unie, kdy elektronizace některých agend veřejné správy probíhá ve vzájemné koordinaci jednotlivých zemí. Zdá se, že se jedná o požadavek, který nebyl v navrhované podobě zatím implementován v žádném jiném členském státě EU. Z praktického hlediska to znamená, že orgány veřejné moci by musely mít zajištěnou dostupnost veškerých informačních systémů používaných pro výkon svých agend z území České republiky. Pro tyto informační systémy by tak musela existovat záložní varianta, která by byla za všech okolností dostupná výhradně z území České republiky (dle výkladu předkladatele se musí jednat o variantu, která umožní výkon svěřených pravomocí výhradně s využitím aktiv umístěných na území České republiky a nelze ji zajistit např. dvěma zahraničními poskytovateli či privátním připojením).	

		Tyto požadavky mají zásadní dopad na možnost využívání cloudových služeb v české veřejné správě. Orgány veřejné moci by při využití globálních cloudových služeb musely vytvářet paralelní infrastrukturu na území České republiky (tj. zajistit veškerá aktiva paralelně i na území České republiky, tak aby výkon jejich agend byl možný jen s využitím těchto aktiv). To by vedlo k extrémnímu navýšení nákladů na informační systémy. Tato paralelní infrastruktura by musela být trvale udržována, aktualizována, testována a zabezpečena. Pro některé komplexní SaaS a PaaS služby nemusí být zajištění řešení dostupného výhradně z území České republiky vůbec reálné a tyto služby by tak v české veřejné správě nemohly být vůbec využívány. Tento požadavek by velmi pravděpodobně znemožnil využívání zejména vysoce inovativních služeb s prvky umělé inteligence, které není reálné zajistit výhradně z území České republiky, a to ani s vynaložením vysokých nákladů. Požadavek na zajištění dostupnosti služeb (z lokálního území) považuje HK ČR za opodstatnitelný pouze pro nejkritičtější infrastrukturu státu. Pro veřejnou správu byla tato nejkritičtější informační infrastruktura státu již vymezena prostřednictvím bezpečnostních úrovní (bezpečnostní úroveň 4 – kritická) ve smyslu vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (která má být nově vydaná ve stejném znění na základě nově předvídaného zmocnění v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy). Pro tyto systémy je již v souladu s § 6m odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy, možné využívat cloudové služby pouze, pokud jsou poskytovány státním poskytovatelem cloud computingu (tj. je zajištěna dostupnost i poskytování z území České republiky). Rozšiřování těchto povinností na jakékoliv další systémy veřejné správy tak popírá smysl této úpravy a je nepřiměřené. Dopady takového rozšíření by zahrnovaly několikanásobné navýšení nákladů	

	na informační systémy veřejné správy a výrazné zpomalení rozvoje služeb eGovernmentu a digitalizace státní správy. Vzhledem k tomu, že oblast elektronických komunikací je velmi specifickým sektorem a již krátce po zveřejnění návrhu ZKB v eKLEP bylo zřejmé, že úprava navržená v návrhu ZKB (ve spojení s příslušnými prováděcími právními předpisy) způsobuje výkladové nejasnosti ohledně rozsahu a dopadu daného ustanovení, navrhuje se zakotvení speciální úpravy zajištění dostupnosti strategicky významné služby pro oblast elektronických komunikací, a to s cílem zamezit možným dezinterpretacím daného ustanovení pro oblast elektronických komunikací, které v případě nezakotvení ustanovení v zákoně hrozí. Předkladatel na základě připomínek veřejnosti upustil od požadavků na lokalizaci dat na území České republiky nebo spřátelených států. Zároveň však navrhl nahradit lokalizaci povinností zajistit dostupnost strategicky významných služeb z České republiky, pokud jsou k jejich poskytování využívána zahraniční aktiva. Povinnost má zajistit dostupnost nejkritičtějších služeb pro občany České republiky v případě mimořádných událostí (přírodní katastrofy, pandemie, války atp.), které by mohly omezit možnosti využití zahraničních aktiv, ať už z důvodu faktické vzdálenosti, nebo nemožnosti uplatňovat státní moc na území jiných států. Předkladatel však prostřednictvím strategicky významných služeb spojil mechanismus zajišťování minimální úrovně dostupnosti s mechanismem prověřování bezpečnosti dodavatelského řetězce, přičemž se jedná o odlišné instituty jak z hlediska cíle právní úpravy, tak z hlediska způsobu jeho dosahování. Účelem stanovení minimální úrovně dostupnosti by mělo být zabezpečení dostupnosti nejkritičtějších služeb na „minimální“ úrovni potřebné k fungování společnosti a státu. Navrhovaná právní úprava se však nezaměřuje na stanovení takové minimální úrovně, kterou částečně ponechává na povinných osobách, nýbrž se věnuje konkrétním funkcím technických aktiv stanoveným ve vyhlášce o	

		nepominutelných funkcích stanoveného rozsahu. Ohledně zabezpečení minimální úrovně dostupnosti tedy ponechává v nejistotě jak poskytovatele, tak uživatele regulovaných služeb. Z výše uvedených důvodů se navrhuje oddělení mechanismu bezpečnosti dodavatelského řetězce od stanovování minimální úrovně dostupnosti. Minimální úroveň dostupnosti jednotlivých kritických služeb by měla být určena zákonem, přičemž způsob zajištění její dostupnosti by měl být ponechán na poskytovatelích. Zároveň se navrhuje konkrétní výčet služeb pro sektor telekomunikací, která respektuje přiměřenou úroveň služeb elektronických komunikací v souladu se zákonem č. 127/2005 Sb., o elektronických komunikacích. Poskytovatelé a zajišťovatelé veřejně dostupných služeb elektronických komunikací by měli mít povinnost zajistit dostupnost hlasové komunikace v mobilní síti a připojení k internetu v mobilní síti v takovém rozsahu tak, aby byla při mimořádné situaci umožněna základní komunikace mezi občany a orgány veřejné moci. Minimální úroveň by tak měla zabezpečit komunikaci během mimořádné situace, aniž by kladla nadměrné technické nároky na poskytovatele, přičemž se nepočítá s nutností zajišťovat služby, které vyžadují vysokou rychlost internetového připojení, jako např. streamování videí nebo videohovory. Pokud by měla být zachována povinnost zabezpečit dostupnost regulované služby v celém rozsahu, k čemuž vede navrhovaná podoba, museli by poskytovatelé služeb elektronických komunikací budovat infrastrukturu výlučně na území České republiky, neboť by nedávalo ekonomický smysl budovat jakoukoli infrastrukturu v zahraničí, pokud by zároveň musela existovat její plnohodnotná „záložní kopie“ v České republice. Taková povinnost by tudíž ani byla nepřipustným omezením volného trhu v rámci EU.	
707. Hospodářská komora ČR	Z	Připomínka k § 40 odst. 1 HK ČR požaduje, aby bylo v § 40 odst. 1 vypuštěno písm. g) a stávající písm. h) přečíslováno na g).	Neakceptováno – nyní § 41 Na tuto povinnost je také navázána povinnost součinnosti vyzvaných orgánů a osob právě za tím

		<u>Odůvodnění:</u> Zákon nedefinuje rozsah ani metodiku provedení skenu zranitelností a penetračního testu. Sken zranitelností a penetrační test technických aktiv provedený na jejich produkční části může zásadně narušit funkčnost technických aktiv až do míry ekvivalentní reálnému kybernetickému útoku, může způsobit nestabilitu, dlouhodobé selhání, případně přímo usnadnit budoucí kybernetický útok. Provedení skenu zranitelností a penetračního testu musí být vždy v odpovědnosti vlastníka nebo provozovatele technických aktiv a musí být prováděno v rámci plánovaných výlukových oken, a to v definovaném rozsahu s odhadnutelným dopadem.	účelem, aby nebylo zasaženo do funkčnosti technických aktiv, a to provedením zpravidla méně invazivního skenu zranitelností nebo penetračním testováním. Ohledně rozsahu a metodiky je proto nezbytné konzultovat s příslušnými odpovědnými pracovníky orgánů a osob, u nichž se znalost informačního systému předpokládá a skrze jejichž součinnost by tam mělo být zamezeno narušení funkčnosti technických aktiv. Připomínka vypořádána.
708. Hospodářská komora ČR	Z	Připomínka k § 53 odst. 1 HK ČR požaduje, aby byl text § 53 odst. 1 upraven takto: <i>„(1) Úřad a provozovatel Národního CERT zpracovávají osobní údaje, jsou-li nezbytné pro výkon jejich působnosti. Tyto údaje Úřad a provozovatel Národního CERT předávají oprávněným orgánům veřejné moci nebo osobám, je-li to nezbytné pro plnění jejich ~~úkolů~~ zákonných povinností a nedojde-li tím k porušení povinnosti mlčenlivosti ~~podle tohoto zákona~~.“</i> <u>Odůvodnění:</u> Je nezbytné zajistit soulad s účinnými právními předpisy (jako je např. GDPR), které specifikují pravomoci a zmocnění oprávněných orgánů při plnění jejich zákonných povinností, nejen podle tohoto zákona.	Akceptováno jinak – nyní § 56 Připomínkované ustanovení bylo z návrhu zákona zcela vypuštěno. Připomínka vypořádána.
709. Hospodářská komora ČR	Z	Připomínka k § 53 odst. 3 písm. a) až c) HK ČR požaduje, aby byl obsah § 53 odst. 3 písm. a) až c) uveden do souladu s požadavky GDPR a dalšími předpisy ve smyslu níže uvedeného odůvodnění. <u>Odůvodnění:</u> V případě, kdy mají být subjektům údajů odepřena jejich práva, je nutné zákonem vymezit konkrétní účely a podmínky zpracování	Neakceptováno Odepření práv subjektu údajů je možné pouze po dobu plnění povinností dle tohoto zákona pouze při řešení kybernetického bezpečnostního incidentu nebo kybernetické bezpečnostní události, při prevenci kybernetických hrozeb nebo rizik anebo při výkonu kontroly. Po odpadnutí důvodu zpracování osobních

		osobních údajů, a to včetně retenčních povinností. Současně je nutno zakotvit zákonný mechanismus kontroly oprávněnosti a zpracování takovýchto osobních údajů.	údajů při řešení kybernetického bezpečnostního incidentu nebo kybernetické bezpečnostní události, při prevenci kybernetických hrozeb nebo rizik anebo při výkonu kontroly, postupuje Úřad nebo provozovatel Národního CERT dle přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů. Přípomínka vypořádána.
710. Hospodářská komora ČR	Z	Přípomínka k § 55 odst. 1 V návaznosti na shora uvedené připomínky HK ČR požaduje, aby byl text § 55 odst. 1 upraven takto: „(1) <i>Prováděcí předpis stanoví</i> <i>a) kritéria pro identifikaci regulované služby (§ 4),</i> <i>b) způsob stanovení režimu poskytovatele regulované služby (§ 6 odst. 3),</i> <i>eb) bezpečnostní opatření odpovídající režimu poskytovatele regulované služby a míru a způsob jejich zavedení a provádění (§14 odst. 2 a 4),</i> <i>dc) způsob stanovení významného dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby v režimu nižších povinností (§ 16 odst. 3),</i> <i>ed) obsahové náležitosti, formát a způsob oznámení provedení protiopatření a jeho výsledku (§ 20 odst. 3),</i> <i>f) kritéria pro identifikaci strategicky významné služby (§ 27 odst. 1),</i> <i>g) nepominutelné funkce stanoveného rozsahu (§ 28 odst. 1),</i> <i>h) kritéria rizikovosti dodavatele a způsob jejich vyhodnocení (§ 28 odst. 4),</i>	Neakceptováno Návrh stanovuje okruh povinných osob stejným způsobem jako to činí dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Okruh povinných osob je zpřesňován na základě zákona jak v případě vyhlášky č. 317/2014 Sb., o významných informačních systémech (§ 3 a § 2 písm. d)), tak v případě vyhlášky č. 437/2014 Sb., o kritériích provozovatele základní služby (§ 3, ve spojení s § 2 písm. i) a k) a § 22a). Obdobný způsob stanovení povinných osob obsahuje také současný krizový zákon (§ 4 odst. 1 písm. d) ve spojení s § 2 písm. i), k), l) a m)), a to již od své novelizace v roce 2010, přičemž opět současný zákon toho také využívá (§ 3 a § 2 písm. b)). Jak uvádí také důvodová zpráva, má tento způsob zpřesnění zákona své opodstatnění a dlouhodobě je považován za vyhovující a v souladu s právními předpisy (všechny tyto právní předpisy prošly standardní procedurou přijímání a tento způsob nastavení schválila připomínková místa i Legislativní rada vlády). S ohledem na připomínky zaslané v tomto mezirezortním připomínkovém řízení došlo k dalšímu upřesnění relevantních ustanovení v zákoně (stanovení regulované služby, jejího režimu i strategicky významné služby), především k ještě bližšímu přiblížení k současnému znění § 22a zákona

		<i>if) způsob hlášení údajů subjektem poskytujícím služby registrace jmen domén (§ 35 odst. 1) a</i> <i>ig) technické a organizační podmínky používání Portálu NÚKIB, obsahové náležitosti, formát, strukturu a způsob provádění úkonů uvedených v § 44 odst. 2 (§ 44 odst. 3). “.</i>“ <u>Odůvodnění:</u> Navrhovaná úprava obsahu § 55 odst. 1 je důsledkem požadavku HK ČR na zrušení zákonného zmocnění předkladatele k vydání prováděcích právních předpisů k ustanovením, která mají být v zákoně, případně mají být zcela vypuštěna.	o kybernetické bezpečnosti. V tomto duchu došlo tedy i k upravení institutu strategicky významné služby. Zrušení daných ustanovení tedy není relevantní, a i přesto že došlo ke zrušení zmocňovacích ustanovení v § 55, zůstávají tato zmocnění na příslušných místech návrhu. V případě vyhlášky o kritériích rizikivosti dodavatele došlo ke zrušení této vyhlášky. Připomínka vypořádána.
711. Hospodářská komora ČR	Z	Připomínka k § 58 odst. 15 písm. a) a písm. b) HK ČR požaduje upravit text takto: „(15) <i>Za přestupek lze uložit pokutu do</i> a) <i>250 000 000 Kč nebo, tam, kde je to vzhledem k okolnostem přiměřené, do výše 2 % čistého celosvětového ročního obratu dosaženého právnickou osobou nebo, pokud je obviněný součástí konsolidačního celku, dosaženého konsolidačním celkem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 1 písm. a), písm. d) až k) a písm. m) až p), odstavce 3 písm. a), e) a f), odstavce 6 písm. b) a odstavce 8 písm. a) a b).</i> b) <i>175 000 000 Kč nebo, tam, kde je to vzhledem k okolnostem přiměřené, do výše 1,4 % čistého celosvětového ročního obratu dosaženého právnickou osobou nebo, pokud je obviněný součástí konsolidačního celku, dosaženého konsolidačním celkem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle</i>	Akceptováno jinak – nyní § 60 Dojde k úpravě ustanovení o přestupcích (§ 60 odst. 15 návrhu zákona) a doplnění podmínky pro uplatnění kritéria obratu konsolidačního celku (obviněný skutek spáchal ve spojení s konsolidačním celkem nebo v jeho prospěch). Tím dojde ke sladění s koncepcí podniku ve smyslu čl. 101 a 102 SFEU, jak požaduje směrnice NIS2. Připomínka vypořádána.

		<i>odstavce 2 písm. a), písm. d) až k) a písm. m) až p) a odstavce 8 písm. d).“</i> <u>Odůvodnění:</u> Znění návrhu zákona věrně implementuje znění směrnice, která v souladu s judikaturou k soutěžním článkům 101 a 102 SFEU konstatuje možnost uložení pokuty za přestupek vypočítané na základě obratu podniku ve smyslu soutěžního práva, tj. ekonomické jednotky/skupiny, ke které pachatel patří. V souladu s judikaturou SDEU zdůrazňuje HK ČR „pouhou“ možnost takového postupu, tedy zabránění automatickému používání obratu skupiny jako stropu pro výpočet pokuty u pachatele, který náleží do (nějaké) skupiny/konsolidačního celku.	
712. Hospodářská komora ČR	Z	Připomínka k § 65 odst. 4 HK ČR požaduje, aby byl text § 65 odst. 4 upraven takto: <i>„(4) ~~Pokud má být řízení~~ Rozhodnutí o výmazu z evidence poskytovatelů regulovaných služeb podle § 11 odst. 2 ~~zahájeno z moci úřední~~, může být ~~rozhodnutí o výmazu z evidence poskytovatelů regulovaných služeb~~ prvním úkonem v řízení; v takovém případě se rozhodnutí písemně nevyhotovuje, záznamem ve spisu rozhodnutí o výmazu nabývá právní moci a Úřad provede výmaz z evidence poskytovatelů regulovaných služeb.“</i> <u>Odůvodnění:</u> Ustanovení § 65 odst. 4 si v hypotéze klade za podmínku zahájení řízení podle § 11 odst. 2 z moci úřední. Řízení podle § 11 odst. 2 však nemůže být zahájeno na žádost, tudíž se vždy musí jednat o řízení z moci úřední. Z tohoto důvodu navrhuje vymazat nadbytečnou podmínku.	Akceptováno jinak – nyní § 11 Na základě této, ale i dalších souvisejících připomínek došlo k celkové úpravě ustanovení o výmazu regulované služby z evidence. Ustanovení nyní připouští jak zahájení řízení o výmazu z moci úřední, tak na žádost poskytovatele regulované služby. Připomínka vypořádána.
713. Hospodářská komora ČR	Z	Připomínka k tezí vyhlášky o regulovaných službách – Kritéria pro identifikaci regulované služby	Neakceptováno Teze prováděcích právních předpisů jsou sice již teď součástí předkládaného materiálu, ale budou následně

	HK ČR požaduje, aby ve vyhlášce o regulovaných službách v Příloze v bodě 16.1 a 16.2 sjednotit kritéria na 350 000 SIM karet nebo pevných přípojek. Alternativně obě tato kritéria zrušit a ponechat pouze dělení vyplývající ze směrnice. <u>Odůvodnění:</u> Česká republika je charakteristická velmi vysokým počtem poskytovatelů přístupu k internetu v pevném místě. Tato skutečnost vede k pozitivním jevům v oblastech hospodářské soutěže a různorodosti použitých řešení. Subjekty působící na trhu přístupu k internetu v pevném místě jsou ale vlivem silného konkurenčního boje a (z podstaty věci) jejich omezené hospodářské síly více zranitelné vlivy nadměrné regulatorní zátěže. Stanovení hranice 100.000 přípojek v pevném místě jako kritéria pro identifikaci poskytovatele strategicky významné služby je z tohoto důvodu nevhodné, neboť bez zjevného důvodu vystaví i nižší kategorii (co do rozsahu) poskytovatelů dramatickému nárůstu jejich regulatorních povinností – a to i v případě, že záležitosti související s bezpečností svých sítí spravují odpovědně. Umístění dané hranice v předkládaném návrhu je navíc drasticky nesystémové s ohledem na skutečnost, že na trhu mobilním, který je dominován velkými nadnárodními poskytovateli, je hranice nastavena na 3,5 násobek. Na českém trhu je běžné, že řada operátorů provozuje své sítě jako holding menších společností. Jde o reziduum toho, že některé operátorské skupiny zvláště regionálních hráčů vznikly tak, že provedly akvizice menších hráčů. Protože operátoři mají různé využití technologie, různé dodavatele, různé topologie sítí a různou praxi v nasazování technologií do sítě, má smysl docházet k nějakému sjednocování až v určitém čase, případně – pokud operátorské holdingy seznají, že je to vhodné – k technologické unifikaci nedojít vůbec. Takto vzniklé skupiny mohou překonat předkladatelem stanovený limit 100 tisíc aktivních pevných přípojek, ačkoli se de facto jedná o malé podniky. Vzhledem k této běžné praxi je HK ČR přesvědčena, že by předkladatel měl ustoupit od stanovení objemových kritérií v oblasti pevných sítí, nebo je sjednotit se	předmětem samostatného připomínkového řízení při procesu jejich vydávání. Nelze předpokládat, že jedna pevná přípojka (typicky jedna domácnost) odpovídá jedné osobě (tj. jedné SIM kartě), z pohledu účelu právní úpravy tedy nemá smysl uvedená kritéria sjednocovat. Pokud jde o konkrétní počty SIM karet a pevných přípojek, uvedený minimální počet aktivních přípojek byl stanoven tak, aby pokryl subjekty poskytující společně podle posledních dostupných dat Českého telekomunikačního úřadu (za rok 2021) většinu všech aktivních přípojek (cca 60 %). Minimální počet SIM karet pokrývá subjekty, které společně poskytují veřejně dostupné služby elektronických komunikací uživatelům většiny všech aktivních mobilních SIM karet na maloobchodním trhu (cca 92 %). V případě SIM karet je současně zohledněna skutečnost, že uvedené výrazně nadpoloviční většině poskytují veřejně dostupné služby elektronických komunikací pouze tři subjekty. Na subjekty poskytující tzv. Fixed Wireless Access (FWA) služby bude Úřad nahlížet obdobně jako ČTÚ, tedy podřazením FWA služeb pro regulatorní účely pod pevné služby. Důvodem je předpoklad, že FWA služby rovněž odpovídají potřebě spíše domácností než jednotlivců. Připomínka vypořádána.

		stanoveným limitem pro mobilní sítě (350 tisíc aktivních přípojek). Dobrou orientaci pro tržní poměry na trhu pevného internetu má Český telekomunikační úřad, který vydává přehled o trhu ve svých výročních zprávách https://www.ctu.cz/vyrocní-zpravy. Objemový požadavek, pokud by měl být zachován, by měl kvantifikovat nikoliv počet přípojek celkem, ale počet přípojek v rámci jedné infrastruktury. HK ČR zároveň žádá o upřesnění toho, jak bude předkladatel postupovat v případě operátorů, kteří nabízejí své služby formou tzv. Fixed Wireless Access (FWA) na kmitočtech, které jsou určeny pro služby IMT (3400-3800 MHz). Tito operátoři nabízejí službu, kterou pro některé regulační účely ČTÚ označuje jako pevnou službu, ale zároveň ji nabízí na zařízeních, která mohou mít v sobě SIM kartu a služba je nabízena na kmitočtech harmonizovaných pro pohyblivou službu. Potenciálně mohou mít tito operátoři časem více než 100 tisíc zákazníků.	
714. Hospodářská komora ČR	Z	Připomínka k bodu 1.11 a 1. 14 přílohy – Vyhláška o nepominutelných funkcích stanoveného rozsahu HK ČR požaduje, aby byl text bodů 1.11 a 1.14 Vyhlášky o nepominutelných funkcích stanoveného rozsahu vypuštěn a ostatní body odpovídajícím způsobem přečíslovány. <u>Odůvodnění:</u> Uvedené typy aktiv nepovažuje HK ČR za nezbytné pro zajištění fungování jádra sítě elektronických komunikací, a proto by neměly tvořit součást nepominutelných funkcí stanoveného rozsahu.	Neakceptováno Nejprve je třeba uvést, že teze prováděcích právních předpisů jsou sice součástí předkládaného materiálu, ale budou následně předmětem samostatného připomínkového řízení při procesu jejich vydávání. Vaši připomínku tak bereme na vědomí a doporučujeme ji uplatnit v rámci připomínkového řízení k předmětné vyhlášce, aby mohla být řádným způsobem vypořádána. Již nyní se však můžeme vyjádřit k dotčeným bodům 1.11 a 1.14 vyhlášky. Konkrétně u bodu 1.11 NÚKIB tvrdí, že tyto monitorovací/dohledové funkce jsou jednoznačně kritické. Principiálně se jedná o jediné nástroje, které mají za úkol dohled nad tím dostupností sítě. To, že jádro sítě funguje i bez těchto nástrojů, lze považovat za samozřejmost. Pokud ale v rámci jádra

			dojde k poruše či znefunkčnění jádra nebo jinému problému, tak tyto monitorovací systémy představují první bod interakce a jsou tak absolutně stěžejní z pohledu tzv. telekomunikačních business modelů. Z hlediska důležitosti bodu 1.14, tj, řízení stanic rádiové přístupové sítě jednotlivých generací, uvádíme, že tyto funkce by měly být považovány za kritické (také dle německého přístupu k určení kritických částí či EU 5G Toolboxu). Řízení základnových stanic je kritické z toho důvodu, že v případě kompromitace těchto stanic může dojít přímo ke kompromitaci provozu v dané oblasti nebo omezení dostupnosti sítě. Přestože se nejedná o kritické funkce z pohledu jádra, z pohledu koncových zařízení/zákazníků jsou tyto rozhodující. Připomínka vypořádána.
715. Hospodářská komora ČR	Z	Připomínka k bodu 11 přílohy – Vyhláška o kritériích rizikivosti dodavatele HK ČR požaduje, aby byl text bodu 11 Vyhlášky o kritériích rizikivosti dodavatele vypuštěn a ostatní body odpovídajícím způsobem přečíslovány. <u>Odůvodnění:</u> Bod 11 přílohy vyhlášky nesměruje k ochraně vůči dodavatelům, kteří představují bezpečnostní hrozbu pro Českou republiku nebo vnitřní či veřejný pořádek, ale proti dodavatelům, kteří by potenciálně nemuseli být schopni dostát svým smluvním závazkům. Čistě ekonomické schopnosti dodavatelů jsou záležitostí podnikatelského rizika poskytovatelů strategicky významných služeb, kteří pravděpodobně disponují podrobnějšími informacemi o sektoru, v němž podnikají, než orgány státní správy.	Neakceptováno Je nasnadě zmínit, že teze prováděcích právních předpisů jsou sice součástí předkládaného materiálu, ale následně budou předmětem samostatného připomínkového řízení při procesu jejich vydávání. Vaši připomínku bereme na vědomí a doporučujeme připomínky směřující k prováděcím předpisům uplatnit v rámci připomínkového řízení k těmto prováděcím předpisům tak, aby mohly být připomínky řádně vypořádány. Nutno však dodat, že zmíněná kritéria posuzování rizikivosti dodavatele v rámci vyhlášky sloužila primárně jako vodítko/metodika k určení hrozby, přičemž vyhláška o kritériích rizikivosti dodavatele byla, mimo jiné z důvodů uvedených v této připomínce a připomínkám směřujícím k formě

		Jedná se tudíž o nadbytečné ustanovení, které má zbytečný potenciál omezovat svobodu podnikání poskytovatelů strategicky významných služeb.	kritérií a jejich účelu, vyřazena. Kritériem tudíž zůstává bezpečnost ČR a její vnitřní či veřejný pořádek. Připomínka vypořádána.
716. Hospodářská komora ČR	Z	Připomínka k § 10, odst. 1, písm. f) přílohy – Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností HK ČR požaduje, aby byl text § 10, odst. 1, písm. f) Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností vypuštěn a písm. g) označeno jako písm. f). <u>Odůvodnění:</u> Navrhovaná úprava stanovuje svým adresátům povinnost vynucovat určitý obsah smlouvy vůči třetím osobám, s nimiž vstupuje do obchodního styku. Z podstaty věci jsou tyto třetí osoby zahraničními subjekty s často mezinárodním dosahem. Typický adresát úpravy – například poskytovatel služeb elektronických komunikací v pevném místě v České republice – přitom jako zpravidla regionální subjekt menšího rozsahu nemá vyjednávací pozici, která by mu umožňovala vynucovat si libovolné smluvní podmínky vůči jeho dodavatelům. Navrhovaná úprava pro typické adresáty prakticky nesplnitelná. Přijetí navrhované úpravy by mělo potenciálně katastrofické důsledky pro tyto poskytovatele připojení, neboť by hrozilo znepřístupněním prakticky všech dodavatelských vektorů více než 1500 ISP působícím v České republice a omezením hospodářské soutěže na tomto trhu jen na velké nadnárodní společnosti.	Neakceptováno Teze prováděcích právních předpisů jsou sice součástí předkládaného materiálu, ale následně budou předmětem samostatného připomínkového řízení při procesu jejich vydávání. Vaši připomínku bereme na vědomí a doporučujeme připomínky směřující k prováděcím předpisům uplatnit v rámci připomínkového řízení k těmto prováděcím předpisům tak, aby mohly být připomínky řádně vypořádány. Je však nutné na předmětnou problematiku nahlížet z pohledu řízení rizik u určených aktiv, v rámci určeného rozsahu regulované služby, u řízení dodavatelů tomu není jinak. Povinné subjekty mají přijmout technická, provozní a organizační opatření k řízení rizik. Je důležité mít u povinné osoby v určeném rozsahu nastaven způsob určení bezpečnostních požadavků, způsob hodnocení rizik, způsob stanovení úrovně zabezpečení, zohlednit charakter regulovaného systému a míru zásahu dodavatele do tohoto systému. Důležité je proto provést hodnocení rizik před samotným uzavřením smlouvy a na základě stanovení úrovně a způsobu realizace bezpečnostních opatření lze jako jednu z možností vyhodnotit požadavek na specifická smluvní ujednání s významnými dodavateli, například zohlednit ty uvedené v příloze č. 7. Samotná kontrola dodržování je zaměřena na nastavení celkového procesu řízení dodavatele a zda plní svůj účel. Výklad požadavků vyhlášky na smlouvy s významnými dodavateli, je nutné chápat

			také z pohledu jeho účelnosti a přiměřenosti. NÚKIB má k této problematice vydán podpůrný materiál - Požadavky na smlouvy s dodavateli. Připomínka vypořádána.
717. Hospodářská komora ČR	Z	HK požaduje, aby bylo v důvodové zprávě doplněno, zda zjištění rizikovosti dodavatele z hlediska ohrožení bezpečnosti ČR zakládá bezpečnostní událost nebo bezpečnostní incident. <u>Odůvodnění:</u> Je třeba najisto stanovit pravidla, podle nichž se bude postupovat.	Akceptováno jinak Do Důvodové zprávy bylo doplněno, že zjištění rizikovosti dodavatele je hrozbou, nikoliv kybernetickou bezpečnostní událostí nebo incidentem. Jak už ale z definice hrozby vyplývá, může způsobit kybernetickou bezpečnostní událost nebo i incident. Připomínka vypořádána.
718. Hospodářská komora ČR	D	Připomínka k názvu zákona HK ČR doporučuje v názvu zákona promítnout i slovní spojení „bezpečnost informací“, např. takto: Zákon o kybernetické bezpečnosti a bezpečnosti informací. <u>Odůvodnění:</u> Bezpečnost informací je věcnou součástí návrhu, proto by bylo vhodné ji zdůraznit i v názvu zákona.	Neakceptováno Definice „informační bezpečnosti“, resp. „bezpečnosti informací“ je v kontextu zákona o kybernetické bezpečnosti dlouhodobě asociována s obsahem zákona č. 412/2005 Sb., o ochraně utajovaných informací. Je sice samozřejmě pravdou, že část NÚKIB je do procesů spojených s tímto zákonem zapojena, nicméně ne ve smyslu připomínkovaných ustanovení. Z tohoto důvodu máme za to, že návrh na doplnění tohoto pojmu do definice necílí na upřesnění vztahu ke zmíněnému zákonu, ale k rozšíření pojmu kybernetická bezpečnost (tzn. ve smyslu „neřeší se jen kybernetická stránka, ale také ochrana informací v systémech“). Vedle toho, že existuje obecně více přístupů ke vztahu množin „kybernetické bezpečnosti“ a „bezpečnosti informací“, nemáme za to, že by bylo nutné i s ohledem na dosavadní výklad tento pojem specificky uvádět nad rámec kybernetické bezpečnost ve smyslu chápání tohoto pojmu jako širší množiny - tak jak je tomu doposud. Nadto by to mohlo

			vést také ke zmatení s výše uvedeným zákonem o ochraně utajovaných informací. Připomínka vypořádána.
719. Hospodářská komora ČR	D	Připomínka k § 2 odst. 1 písm. g) HK ČR doporučuje upravit text takto: <i>„g) řízením kybernetické bezpečnosti a bezpečnosti informací činnost poskytovatele regulované služby podle tohoto zákona směřující k zajištění kybernetické bezpečnosti a bezpečnosti informací regulované služby.“</i> <u>Odůvodnění:</u> Jakkoli je bezpečnost informací součástí kybernetické bezpečnosti, je zcela na místě ji určitým způsobem „vytknout před závorku“, aby byl zdůrazněn její význam, což je ostatně posláním i následující připomínky.	Neakceptováno Vypořádání připomínky viz výše. Připomínka vypořádána.
720. Hospodářská komora ČR	D	Připomínka k názvu § 13 HK ČR doporučuje upravit název takto: <i>„§ 13 Stanovení rozsahu řízení kybernetické bezpečnosti a bezpečnosti informací poskytovatelem regulované služby“</i> <u>Odůvodnění:</u> HK ČR má za to, že je nezbytné výslovně stanovit rozsah řízení kybernetické bezpečnosti a bezpečnosti informací.	Neakceptováno Vypořádání připomínky viz výše. Připomínka vypořádána.
721. Hospodářská komora ČR	D	Připomínka k § 45 odst. 1 písm. c) HK ČR doporučuje upravit text takto: <i>„c) dodavatelů bezpečnostně významných dodávek a dodavatelů s vysokou mírou bezpečnostního rizika,“</i>	Neakceptováno Úřad vede toliko evidenci dodavatelů bezpečnostně významných dodávek. Připomínka navrhovatele směřuje k vytvoření zcela nové evidence, které by měla vytvářet seznam „rizikových dodavatelů“. K

		<u>Odůvodnění:</u> Doporučovaná úprava výrazně napomůže uživatelskému komfortu a bude sloužit k předcházení a eliminaci ve vazbě na případné (a hrozící) bezpečnostní incidenty.	tomu však mechanismus prověřování nejenže nesměřuje, ale ani nesmí směřovat. Jednalo by se o výrazný a ničím nepodložený zásah do práv těchto subjektů. V případě, že Úřad pomocí mechanismu prověřování dodavatelského řetězce odhalí rizikového dodavatele, shrne svá zjištění pomocí opatření obecné povahy, či jiných nástrojů, které zákon zná. Tato zjištění jsou vždy veřejná, odůvodněná a umožňují subjektům v nich označených zareagovat. V konečném důsledku pak plní i prevenční funkci tak, jak naznačuje ve své připomínce její navrhovatel. Připomínka vypořádána.
722. Hospodářská komora ČR	D	Připomínka k důvodové zprávě, § 17 odst. 5 HK ČR doporučuje upravit text důvodové zprávy k § 17 odst. 5 tak, že budou vypuštěna slova „nebo svévolným“ takto: <i>„Prvotní hlášení obsahuje informace o tom, zda existuje podezření, že incident byl způsoben nezákonným ~~nebo svévolným~~ zásahem, a zda je pravděpodobné, že bude mít přeshraniční dopad.“</i> <u>Odůvodnění:</u> Incident, který vznikl svévolným způsobem, nenaplní podmínky vzniku takového incidentu v kyberprostoru, jak zakládá znění § 16 odst. 1.	Neakceptováno Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnicí NIS2, pokud bychom do zákona tuto úpravu nezahrnuli, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Obsahem prvotního hlášení podle čl. 23 odst. 4 písm. a) směrnice NIS2 (ve směrnici označen jako včasné varování) je uvedení toho, „zda se [subjekty] domnívají, že byl významný incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad“. Úřad tedy není oprávněn zasahovat v navrženém smyslu do znění dotčeného ustanovení návrhu zákona, nadto informace o případné svévolnosti incidentu představuje pro Úřad cennou informaci pro potřebu následné analýzy. Také pro incident vzniklý v kyberprostoru platí, že může být způsoben nesvévolně. Připomínka vypořádána.

723. Hospodářská komora ČR	D	Připomínka k důvodové zprávě, § 34 HK ČR doporučuje upravit text důvodové zprávy k § 34 takto: - odst. 1 úplně vypustit; - text odst. 2 upravit tak, že se za slova „cíle na rizika spojená s dostupností“ doplní slova „poskytované služby“; - text odst. 2 dále upravit tak, že se za slova „Němčině je limitován nutností zajistit tuto dostupnost“ doplní slova „řídícím systémem“. <u>Odůvodnění:</u> Navrhované znění prvního odstavce důvodové zprávy vychází na původního obsahu § 34 týkajícího se lokalizace a zpracování dat, nicméně změny vyplývající z uplatněných připomínek se zaměřují na zajištění dostupnosti služby výhradně z území ČR. Proto je nedůvodné se nadále zabývat tématem dostupnosti a zpracování dat. Zároveň je nutné zdůraznit, že dostupnost služby a její obnova znamená realizaci takového opatření, aby v případě obnovy bylo možné takovou obnovu zajistit z území České republiky, a nejedná se o reálné poskytování služby z území České republiky. HK ČR předpokládá, že předkladatelem bude vytvořen metodický pokyn, který bude upřesňovat a zajišťovat plnění tohoto ustanovení.	Akceptováno jinak Znění důvodové zprávy k předmětnému ustanovení bylo upraveno ve smyslu připomínky. Odstavec 1 nebyl zcela vymazán, byl pouze upraven s ohledem na změny provedené v legislativním textu. Sousední „řídícím systémem“ nebylo na navrhované místo doplněno, z připomínky není patrný smysl či důvod takové změny. Možnost vydání podpůrného či metodického materiálu není třeba do důvodové zprávy explicitně zmiňovat. Připomínka vypořádána.
724. Kabinet ministra pro legislativu (vláda)	D	Obecně podle Legislativních pravidel vlády platí, že právní předpisy by měly být psány jasně, srozumitelně, jednoznačně a v České republice českým jazykem, tedy za použití českých výrazů, existujících, a nikoli jejich cizojazyčných ekvivalentů. Předloha návrhu zákona o kybernetické bezpečnosti rozeslaná do meziresortního připomínkového řízení podle mého názoru tyto podmínky bohužel v mnoha ohledech nesplňuje. Přehlednost a srozumitelnost návrhu zákona vykazuje určité nedostatky a normativní text je i vinou snahy o zapracování ne vždy zcela zdařilé úpravy předpisů práva Evropské unie do právního řádu České republiky formulačně těžkopádný a tudíž	Akceptováno jinak Body 1 a 2 připomínky byly akceptovány a text byl upraven. První část bodu 3 připomínky byla akceptována, část týkající se §34 odst. 4 se pokusíme vysvětlit: cíle řízení kontinuity činností jsou pojmem vycházejícím z vyhlášky. Stanovení cílů v procesu řízení kontinuity činností je bezpečnostním opatřením. § 71 odst. 1 reflektuje potřebu pokrýt přechodné období nejen z hlediska kontinuity povinností, ale také

	místa hůře srozumitelný. Návrh zákona je proto nezbytné podrobit revizi jak po stránce jazykové, obsahové a stylistické, tak i po stránce legislativně technické, a celkově jej při dodržení zásad tvorby práva zjednodušit tak, aby jej bylo možno lépe číst a tím mu lépe i porozumět. Při úpravě návrhu zákona doporučujeme napravit zejména tyto nedostatky předloženého textu návrhu: 1. Dodržovat pravidla pro tvorbu a používání legislativních zkratk – např. v § 47 odst. 2 a 3 jsou zavedeny legislativní zkratky „žadatel“ a „žádost“, ačkoliv jsou tyto pojmy používány v návrhu zákona i před místem jejich zavedení a po něm a nadto ve zcela jiném smyslu. Uvedené legislativní zkratky proto buď vůbec nezavádět, nebo je uvést v podobě, která bude jednoznačná a v návrhu zákona v jiném významu nepoužívána. 2. Zmocňovací ustanovení k vydání prováděcích právních předpisů jsou v návrhu zákona v některých případech uvedena nadbytečně duplicitně, a to jednak v příslušném hmotněprávním ustanovení, tak i v ustanovení § 55, kde se na příslušná ustanovení znovu odkazuje. S ohledem na skutečnost, že ustanovení § 55 neobsahuje všechna zákonná zmocnění obsažená v návrhu zákona včetně odkazů na ně, mohla by mimo jiné vzniknout i nežádoucí mezera v zákoně, neboť k § 55 odst. 2 ve spojení s § 55 odst. 1 není v návrhu zákona uvedeno, kdo má vydat prováděcí právní předpis např. podle § 12 odst. 6 nebo § 17 odst. 5. Doporučujeme pojetí zmocňovacích ustanovení značně zjednodušit, ustanovení § 55 vypustit a přímo v příslušném ustanovení stanovit, že tak stanoví Úřad vyhláškou. V této souvislosti se připomíná, že prováděcí právní předpisy lze vydávat toliko k provedení zákona a v jeho mezích a v případě vyhlášek na základě (výslovného) zákonného zmocnění. Zákon má tedy stanovit meze a výslovně zmocnit, tj. uvést, co konkrétně má být předmětem úpravy prováděcího právního předpisu; jinými slovy má tedy zákon dostatečně určitým (a nikoliv bezbřehým) způsobem vymezit obsah vyhlášky mantinely. Některá zákonná zmocnění uvedená v návrhu zákona však tyto základní podmínky nenaplnují (např. § 27 odst. 1). 3. Upravit zcela nesrozumitelný text (např. v § 29 odst. 1 „stanovisko	z hlediska možnosti uplatnění sankcí za jejich porušení. Více viz důvodová zpráva. Připomínkové místo s vypořádáním souhlasí.

		o naplnění kritéria rizikovosti dodavatele konkrétním orgánem či osobou“, v § 34 odst. 4 „cílech řízení kontinuity činností“ nebo přechodné ustanovení obsažené v § 71 odst. 1).	
725. Kabinet ministra pro legislativu (vláda)	D	Závěrem si dovoluji konstatovat, že se zároveň plně ztotožňuji se všemi výhradami a připomínkami obsaženými ve stanovisku Odboru kompatibility Úřadu vlády k tomuto návrhu zákona, do jehož působnosti výlučně patří posuzování souladu navrhované právní úpravy s právem Evropské unie. Připomínky v něm obsažené považuji za relevantní a legitimní s tím, že jejich akceptování, popřípadě vysvětlení považuji za klíčové pro projednávání návrhu zákona o kybernetické bezpečnosti v další fázi legislativního procesu.	Akceptováno jinak Bude vyřešeno v závislosti na vypořádání připomínek s OKOM. Připomínkové místo s vypořádáním souhlasí.
726. Kabinet ministra pro legislativu (vláda)	D	K § 1 (1) Tento zákon upravuje práva a povinnosti orgánů a osob a působnost a pravomoci Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“) a dalších orgánů veřejné moci v oblasti kybernetické bezpečnosti. Ve zvláštní části důvodové zprávy k ustanovení § 1 odst. 1 je uvedeno, že slovní spojení „orgány a osoby“ je převzato a kontinuálně užíváno v souladu s předchozí právní úpravou kybernetické bezpečnosti a jeho cílem je pokrýt celé spektrum všech typů potenciálních adresátů této normy. 1. V prvé řadě je nutno konstatovat, že pokud má tento pojem zahrnout co nejširší okruh adresátů připravované právní úpravy, pak není zřejmé, z jakého důvodu je v závěru předmětného ustanovení doplněno sousloví „a další orgánů veřejné moci v oblasti kybernetické bezpečnosti“. Tento dovětek spíše relativizuje zvolený široký pojem „orgány a osoby“ a neodpovídá tak textu důvodové zprávy. Doporučujeme proto toto slovní spojení vypustit. Pro tento krok svědčí i fakt, že pojem „orgány a osoby“ není zaveden jako legislativní zkratka a dále v textu se již používá výlučně bez onoho dovětku „další orgány veřejné moci“. 2. Druhým problémem, který lze v citovaném ustanovení spatřovat je	Akceptováno jinak V rámci předpisu bylo před změnou použito množství různých označení téhož pojmu (osoba, subjekt, každý atd.) a v rámci řešení této připomínky byla tato označení sjednocena a vyjasněna, aby nedocházelo ke zbytečným výkladovým nesrovnalostem. Bylo však zachováno označení orgán a osoba, jelikož toto označení používá již původní zákon o kybernetické bezpečnosti a v rámci této oblasti úpravy je takovéto označení adresátů normy návodné a výstižné. Definice orgánu, dle našeho názoru, není nutná, ale za účelem lepší srozumitelnosti byl pojem „orgán“ v § 2 odst. 2 vymezen. § 1 je koncipován tak, že v první části hovoří o orgánech a osobách jako adresátech normy, v druhé části o orgánech veřejné moci (které zahrnují i Poslaneckou sněmovnu, která vykonává kontrolu činnosti Úřadu) a osobách, které vykonávají státní správu v oblasti kybernetické bezpečnosti. Vybrané konkrétní úpravy: V § 1 byly pro úplnost doplněny osoby vykonávající státní správu. V § 2 odst. 2 bylo doplněno vymezení

		skutečnost, že pojem „orgán“ není legálním pojmem s pevně stanoveným obsahem a rozsahem, a proto se jeví jako vhodné jej v úvodních ustanoveních návrhu zákona alespoň rámcově definovat. Jako vhodný příklad by pak mohlo posloužit ustanovení § 2 písm. d) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Navíc lze mít určité pochybnosti o tom, zda se pojmem „orgán“ rozumějí i ústřední správní úřady, resp. správní úřady v obecném slova smyslu, neboť tímto institutem se zpravidla označují osoby, které stojí v čele správních úřadů, protože jsou to de iure i de facto ony, které vykonávají onu působnost, resp. pravomoc.	pojmu "orgán". Pojem "osoba" již právní řád zná a jedná se samozřejmě o právnickou nebo fyzickou osobu. Připomínkové místo s vypořádáním souhlasí.
727. Kabinet ministra pro legislativu (vláda)	D	K § 5 Regulovanou službou je dále služba ~~stanovená u orgánu nebo osoby určená orgánu nebo osobě~~ rozhodnutím Úřadu 1. Z § 5 i z jiných ustanovení návrhu zákona (např. § 8 odst. 4 nebo § 11) vyplývá, že Úřad svým rozhodnutím určí regulovanou službu. Z § 6 odst. 3 ovšem vyplývá, že Úřad určí orgán nebo osobu poskytující regulovanou službu. Je třeba vyjasnit, co má být obsahem rozhodnutí Úřadu. 2. Nadto se upozorňuje na pojem „poskytovatel regulované služby“, který byl zaveden v § 2 odst. 1 písm. f), a který by tedy měl být použit i v tomto ustanovení namísto slov „orgán nebo osoba poskytující regulovanou službu“.	Akceptováno První část připomínky je akceptována zcela, což činí druhou část připomínky bezpředmětnou. V § 6 odst. 4 byl text upraven následovně: „Je-li regulovaná služba určena rozhodnutím Úřadu podle § 5 odst. 1, je režim jejího poskytovatele vždy režimem vyšších povinností.“ Připomínkové místo s vypořádáním souhlasí.
728. Kabinet ministra pro legislativu (vláda)	D	K § 5 písm. a) Z textu ustanovení § 5 písm. a) úvodní části ustanovení není zřejmé, zda se v případě prováděcího právního předpisu bude též jednat o vyhlášku Úřadu vydanou podle tohoto zákona, nebo o prováděcí právní předpis vydaný v gesci jiného správního úřadu.	Akceptováno Text upraven na „a) jde o službu uvedenou ve vyhlášce Úřadu stanovující kritéria pro identifikaci regulovaných služeb“. Připomínkové místo s vypořádáním souhlasí.
729. Kabinet ministra pro legislativu (vláda)	D	K § 8 odst. 3, 11 odst. 1, 12 odst. 6, 17 odst. 5, 28 odst. 3 písm. a), 32 odst. 1 písm. b), 34 odst. 4, 56 odst. 1, 57 odst. 1	Akceptováno Sousloví „prováděcí právní předpis“ bylo nahrazeno „vyhláškou Úřadu“.

		Obdobná připomínka se pak vztahuje i k ustanovení § 8 odst. 3, § 11 odst. 1, § 12 odst. 6, § 17 odst. 5, § 28 odst. 3 písm. a), § 32 odst. 1 písm. b), § 34 odst. 4, § 56 odst. 1 a § 57 odst. 1, které zcela absentují ve zmocňovacím ustanovení § 55 návrhu zákona. Text zmocnění je v předmětných ustanoveních označen zeleně.	Připomínkové místo s vypořádáním souhlasí.
730. Kabinet ministra pro legislativu (vláda)	D	K § 6 Každý poskytovatel regulované služby má pro všechny poskytované regulované služby stanoven jen jeden režim poskytovatele regulované služby. Je otázkou, zda je nutné pravidlo pro stanovení režimu poskytovatele regulované služby formulovat jako právní domněnku (odstavec 2) a zda by § 7 nebylo možné celkově formulovat stručněji (např. závěrečná část odstavce 2 se zdá být nadbytečná – to, že poskytovatel plní povinnosti pro režim vyšších povinností, není třeba znovu uvádět, vyplývá to z § 6; § 7 by měl pouze upravit pravidla pro určení režimu pro poskytovatele, který poskytuje více regulovaných služeb).	Akceptováno § 7 byl přeformulován následujícím způsobem: Režim poskytovatele regulované služby v případě poskytování více regulovaných služeb (1)Každý poskytovatel regulované služby má pro všechny poskytované regulované služby stanoven jen jeden režim. (2)Poskytovatel regulované služby, kterému je stanoven režim vyšších povinností pro alespoň jednu jím poskytovanou regulovanou službu, má stanoven režim vyšších povinností pro všechny jím poskytované regulované služby. Připomínkové místo s vypořádáním souhlasí.
731. Kabinet ministra pro legislativu (vláda)	D	K § 8 (4)Úřad dále provede registraci poskytovatele regulované služby nebo ~~určení~~ regulované služby na základě rozhodnutí Úřadu ~~o určení regulované služby~~ podle § 5. Z § 8 i z dalších ustanovení návrhu zákona jednoznačně nevyplyvá, zda se registruje poskytovatel regulované služby nebo samotná regulovaná služba. Návrh zákona by měl být formulačně upraven tak, aby nepřipouštěl vznik výkladových nejasností.	Akceptováno Návrh zákona částečně vycházel ze současné koncepce určování (§ 22a zKB), kdy je určován samotný poskytovatel základní služby. Jelikož ten podle nové úpravy může poskytovat současně hned několik regulovaných služeb, bylo třeba přidat úkony jako je registrace, změna r., zápis a výmaz rovněž vůči jednotlivým službám. Stejně tak totiž funguje následné počítání lhůt. Skutečně tak došlo k tomu, že se úprava registrace poskytovatele regulované služby stala nadbytečnou. Údaje o poskytovateli regulované služby jsou vždy součástí registrace samotné regulované služby. Upravili jsme proto znění zákona

			tak, že je vždy registrována, zapsána a vymazávána konkrétní regulovaná služba. Tudíž se mění i název příslušné evidence na evidenci regulovaných služeb. Připomínkové místo s vypořádáním souhlasí.
732. Kabinet ministra pro legislativu (vláda)	D	K § 9 (1)Poskytovatel regulované služby je povinen v případě naplnění kritérií pro identifikaci každé další regulované služby provést změnu ~~své registrace poskytovatele regulované služby~~ a postupovat obdobně podle § 8 odst. 1 a 2. (2)Poskytovatel regulované služby je povinen v případě, že v rámci naplnění kritérií pro identifikaci regulované služby dojde ke změně režimu poskytovatele regulované služby, provést změnu ~~své registrace poskytovatele regulované služby~~ a postupovat obdobně podle § 8 odst. 1 a 2. Při změně režimu poskytovatele regulované služby z režimu vyšších povinností na režim nižších povinností nové lhůty pro zahájení plnění povinností podle § 12 odst. 3, § 14 odst. 3 a § 16 odst. 4 neplynou. Ustanovení § 9 a 11 by bylo možné formulovat přehledněji, méně popisně a tak, aby z nich jednoznačně vyplývalo, v jakých případech poskytovatel regulované služby provede změnu registrace, resp. provede výmaz z evidence.	Akceptováno jinak Došlo ke sjednocení pojmosloví napříč návrhem zákona a zpřesnění procesu registrace a výmazu regulované služby z evidence, v důsledku čehož byly odpovídajícím způsobem upraveny připomínkou dotčené ustanovení návrhu zákona. Připomínkové místo s vypořádáním souhlasí.
733. Kabinet ministra pro legislativu (vláda)	D	K § 4 (1)Kritéria pro identifikaci regulované služby jsou tvořena kritériem služby a kritériem poskytovatele regulované služby. Kritéria pro identifikaci regulované služby stanoví ~~prováděcí právní předpis~~ Úřad vyhláškou. (2)Prováděcí právní předpis Úřad vyhláškou stanoví kritéria pro identifikaci regulované služby v těchto odvětvích	Akceptováno Upraveno průřezově celým návrhem zákona. Připomínkové místo s vypořádáním souhlasí.
734. Kabinet ministra pro legislativu (vláda)	D	K § 10 (1)Po registraci poskytovatele regulované služby podle § 8 nebo po její změně podle § 9 Úřad bez zbytečného odkladu запиše	Akceptováno § 10 odst. 1) byl přeformulován podle připomínky a upraven dle ostatních připomínek

		poskytovatele regulované služby a regulovanou službu do evidence poskytovatelů regulovaných služeb na základě registrace poskytovatele regulované služby či změny registrace poskytovatele regulované služby podle § 8 a § 9. O této skutečnosti Úřad poskytovatele regulované služby písemně vyrozumí.	Připomínkové místo s vypořádáním souhlasí.
735. Kabinet ministra pro legislativu (vláda)	D	K § 11 odst. 2 (2) Pokud se Úřad dozví, že poskytovatel regulované služby, jehož ~~jemuž byla~~ služba byla určena rozhodnutím Úřadu podle § 5, ~~nadále neposkytuje službu naplňující~~ poskytuje službu, která již nesplňuje kritéria pro určení regulované služby, Úřad o této skutečnosti vydá rozhodnutí rozhodne o tom, že služba, kterou poskytovatel regulované služby poskytuje, nesplňuje kritéria pro určení regulované služby.	Akceptováno jinak V závislosti na vypořádání Vaší připomínky k § 8 návrhu zákona, bylo rovněž třeba upravit ustanovení týkající se výmazu. Návrh nově počítá s tím, že výmaz z evidence lze provést rovněž na žádost poskytovatele regulované služby. Připomínkové místo s vypořádáním souhlasí.
736. Kabinet ministra pro legislativu (vláda)	D	K § 11 odst. 3 (3) Pokud se Úřad dozví, že orgán nebo osoba zapsaná v evidenci poskytovatelů regulovaných služeb nadále neposkytuje žádnou službu naplňující kritéria pro identifikaci regulované služby nebo službu určenou rozhodnutím Úřadu pro naplnění kritérií pro určení regulované služby, Úřad tento orgán nebo osobu vymaže z evidence poskytovatelů regulovaných služeb a o této skutečnosti tento orgán nebo osobu písemně vyrozumí. Pokud se Úřad dozví, že poskytovatel regulovaných služeb již neposkytuje žádnou službu naplňující kritéria pro identifikaci regulované služby nebo službu určenou rozhodnutím Úřadu pro naplnění kritérií pro určení regulované služby, Úřad takového poskytovatele z evidence vymaže a o této skutečnosti jej písemně vyrozumí.	Neakceptováno Pokud již subjekt (orgán nebo osoba) neposkytuje žádnou regulovanou službu, nelze jej již označovat za poskytovatele regulované služby. Záměrně jsme proto tento pojem v tomto konkrétním odstavci nepoužili. Změnou koncepce, kdy se registrují, zapisují a vymazávají pouze regulované služby a nikoli poskytovatelé regulovaných služeb, se však stalo toto ustanovení nadbytečným. Výmazem poslední regulované služby daného poskytovatele z evidence regulovaných služeb dojde automaticky k tomu, že poskytovatel nebude dále v evidenci veden. Připomínkové místo s vypořádáním souhlasí.
737. Kabinet ministra pro legislativu (vláda)	D	K hlavě II dílu 2 Díl 2 navrhujeme podrobit revizi a zvážit přesun některých ustanovení na jiné místo v návrhu zákona; díl 2 totiž kromě ustanovení o povinnostech poskytovatele regulované služby obsahuje řadu	Neakceptováno Díl 2 sice obsahuje vybraná kompetenční a procesní ustanovení, ale právě taková, která se týkají poskytovatele a jsou navázána na jeho práva a

		zejména kompetenčních ustanovení (např. 18 odst. 1 a 2, § 20, § 21 nebo § 22 odst. 1), popř. ustanovení procesních.	povinnosti. Úprava byla zvolena takto, aby měl adresát normy jasnou představu o svých právech a povinnostech, stejně tak jako o procesech, které se ho týkají. Na tato kompetenční ustanovení pak odkazuje § 44 odst. 4 písm. o): „plní další úkoly stanovené tímto zákonem [...]“. Připomínkové místo s vypořádáním souhlasí.
738. Kabinet ministra pro legislativu (vláda)	D	K § 12 odst. 5 (5)Poskytovatel regulované služby je povinen zajistit dostatečnou zastupitelnost fyzických osob, které jsou oprávněny jednat za poskytovatele regulované služby ~~ve věcech upravených tímto zákonem~~ podle tohoto zákona	Akceptováno Připomínkové místo s vypořádáním souhlasí.
739. Kabinet ministra pro legislativu (vláda)	D	K 12 odst. 1, 12 odst. 2 písm. c) Podle § 12 odst. 1 a § 12 odst. 2 písm. c) je poskytovatel regulované služby povinen Úřadu hlásit mj. další doplňující údaje, jimiž jsou informace potřebné pro výkon činnosti Úřadu podle tohoto zákona. Tuto konstrukci nepovažujeme za vhodnou. Bylo by tak na poskytovateli regulované služby, aby si sám vyhodnotil, které informace Úřad k výkonu své činnosti potřebuje, a které by tedy měl Úřadu hlásit. Na druhou stranu, pokud by potřebné údaje Úřadu neohlásil, hrozí mu sankce v podobě pokuty až do výše 100 mil. Kč.	Vysvětleno Právní úprava počítá s tím, že tyto údaje budou specifikovány (konkrétně definovány) v prováděcím právním předpise, tedy konkrétně ve vyhlášce o portálu NUKIB (§ 12 odst. 6))§ 12 odst. 6. Připomínkové místo s vypořádáním souhlasí.
740. Kabinet ministra pro legislativu (vláda)	D	K § 13 odst. 3. 13 odst. 5 (3)O provedení identifikace a určení organizačních částí a aktiv podle odstavce 1 vede poskytovatel regulované služby ~~dokumentovaný~~ písemný záznam, a to včetně evidence primárních aktiv, která byla ze stanoveného rozsahu vyjmuta, a odůvodnění jejich vyjmutí	Neakceptováno Chápeme dokumentovaný záznam, jako formalizovaný písemný popis toho, jakým způsobem je či byla prováděna činnost, proces, technika nebo metodika. Slovo písemně je v zákoně a vyhláškách nahrazeno jednotně slovem dokumentovaně. Nepředpokládáme v tomto výkladové nejednoznačnosti i s ohledem na samotné odůvodnění k návrhu zákona.

			Připomínkové místo s vypořádáním souhlasí.
741. Kabinet ministra pro legislativu (vláda)	D	K § 14 odst. 1 (1)Bezpečnostními opatřeními ~~se rozumí úkony~~ jsou organizační a technická opatření , jejichž cílem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv. ~~Bezpečnostními opatřeními jsou organizační a technická opatření.~~	Akceptováno Připomínkové místo s vypořádáním souhlasí.
742. Kabinet ministra pro legislativu (vláda)	D	K § 16 odst. 2 (2)Poskytovatel regulované služby v režimu nižších povinností je povinen v rámci stanoveného rozsahu hlásit Národnímu ~~CERT~~ Computer Emergency Response Team (dále jen „Národní CERT“) všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a mají významný dopad na poskytování regulované služby.	Akceptováno jinak Na základě Vaší připomínky došlo k doplnění definice Národního a Vládního CERT a zavedení legislativní zkratky: „národní/vládní tým koordinace a zvládání kybernetických bezpečnostních incidentů, událostí a hrozeb (dále jen „Národní/Vládní CERT“)“. Podrobnější definice činností obou týmů jsou rozvedeny v příslušných ustanoveních. Připomínkové místo s vypořádáním souhlasí.
743. Kabinet ministra pro legislativu (vláda)	D	K § 16 odst. 5 (5)Orgán nebo osoba může prostřednictvím internetových stránek Úřadu ~~dobrovolně~~ hlásit kybernetické bezpečnostní incidenty, především ty, u kterých lze dovodit úmyslné zavinění, ~~stejně tak jako hlásit~~ kybernetické bezpečnostní události nebo kybernetické hrozby.	Akceptováno jinak Nové znění odst. 5: „(5) <i>Nad rámec odstavců 1 a 2 mohou poskytovatelé regulovaných služeb a další orgány a osoby Úřadu hlásit kybernetické bezpečnostní incidenty, především ty, u kterých lze dovodit úmyslné zavinění, kybernetické bezpečnostní události nebo hrozby. Úřadu mohou být anonymně hlášeny také zranitelnosti, zejména pro účely zajištění koordinovaného zveřejňování zranitelností ze strany vládního týmu koordinace a zvládání kybernetických bezpečnostních incidentů, událostí a hrozeb (dále jen „Vládní CERT“).</i> “. Připomínkové místo s vypořádáním souhlasí.

744. Kabinet ministra pro legislativu (vláda)	D	K § 17 odst. 2, 17 odst. 3 V ustanovení § 17 odst. 2 a 3 je na několika místech použit pojem „kybernetický prostor státu“ a pouze v jednom výskytu je uvedeno sousloví „kybernetický prostor České republiky“. S ohledem na případné budoucí výkladové nejasnosti je proto nutno tyto dva pojmy sjednotit. Jako vhodnější se pak podle našeho názoru jeví slovní spojení „kybernetický prostor České republiky“. V souvislosti s touto připomínkou je pak nutno zmínit i některá další ustanovení návrhu zákona, kde se vyskytuje jen sousloví „kybernetický prostor“ bez dalšího upřesnění. Jedná se o ustanovení § 2 odst. 2, § 16 odst. 1 a 2, § 18 odst. 2, § 38, § 41 a § 45 odst. 3. Otázkou zůstává, zda i v těchto případech má být použito pojmu „kybernetický prostor České republiky“, či zda se jedná o obecněji pojaté vymezení tohoto institutu.	Akceptováno jinak Kybernetický prostor je obecný pojem, kybernetický prostor státu je užší množinou kybernetického prostoru zaměřený na oblast České republiky. Na základě Vaší připomínky bylo slovní spojení "aktuální situace v kybernetickém prostoru České republiky", nahrazeno spojením "aktuální situace v kybernetickém prostoru s potenciálním dopadem na bezpečnost České republiky". Připomínkové místo s vypořádáním souhlasí.
745. Kabinet ministra pro legislativu (vláda)	D	K § 17 odst. 3 písm. b) b)~~na žádost~~ na výzvu Úřadu nebo Národního CERT průběžnou zprávu o podstatných změnách stavu zvládání kybernetického bezpečnostního incidentu, a	Akceptováno Připomínkové místo s vypořádáním souhlasí.
746. Kabinet ministra pro legislativu (vláda)	D	K § 17 odst. 3 písm. c) c)nejpozději do 30 dnů od předložení oznámení podle písmene a) závěrečnou zprávu o vyřešení kybernetického bezpečnostního incidentu;	Akceptováno Připomínkové místo s vypořádáním souhlasí.
747. Kabinet ministra pro legislativu (vláda)	D	K § 17 odst. 4 (4)Poskytovatel regulované služby hlásí kybernetické bezpečnostní incidenty včetně dobrovolných hlášení podle tohoto zákona prostřednictvím Portálu Úřadu (dále jen „Portál“) NÚKIB.	Akceptováno Připomínkové místo s vypořádáním souhlasí.
748. Kabinet ministra pro legislativu (vláda)	D	K § 17 odst. 3 Není zřejmé, jestli je na úvaze poskytovatele regulované služby, zda bude povinnosti podle odstavce 3 plnit vůči Úřadu nebo vůči	Vysvětleno Komu se hlásí kybernetické bezpečnostní incidenty jednoznačně vyplývá z § 16 odst. 1 a 2. Veškerá dílčí hlášení podle § 17 odst. 3 jsou součástí celého procesu

		Národnímu CERT. Pokud nikoli, je třeba ustanovení přeformulovat a povinnost stanovit jednoznačně.	hlášení incidentu, nemůže tedy dojít k situaci, kdy by poskytovatel v určité fázi procesu začal hlásit Úřadu namísto Národnímu CERT či naopak. Připomínkové místo s vypořádáním souhlasí.
749. Kabinet ministra pro legislativu (vláda)	D	K § 17 odst. 4 Rovněž je otázkou, zda v případě vzniku kybernetického bezpečnostního incidentu bude vždy možné hlásit tyto incidenty pouze s využitím elektronických způsobů komunikace (odstavec 4 stanoví, že v případě, že nebude možné využít Portál NUKIB, mají být incidenty hlášeny na adresu elektronické pošty Úřadu nebo do jeho datové schránky).	Vysvětleno Máme za to, že poslat prvotní hlášení prostřednictvím elektronické pošty lze i bez funkční infrastruktury regulované organizace. Kontaktní osoba to může učinit klidně ze svého mobilního telefonu, jde především o to, aby Vládní/Národní CERT mohl na tuto situaci bezprostředně reagovat. Pokud by došlo k nahlášení prostřednictvím neelektronických prostředků, např. standardní poštou, hrozí poměrně velké průtahy v řešení incidentu. Variantou je zachování pohotovostní telefonické linky, nicméně při počtu regulovaných subjektů není možné zajistit dostatečnou dostupnost takové linky, navíc by šlo těžko dodržet obsahové náležitosti hlášení. Připomínkové místo s vypořádáním souhlasí.
750. Kabinet ministra pro legislativu (vláda)	D	K § 18 odst. 5 (5)Odstavce 1 až 4 se při zvládání kybernetických bezpečnostních incidentů nahlášených dobrovolně podle § 16 odst. 5 použijí obdobně	Akceptováno jinak Nové znění § 18 odst. 5: „Odstavce 1 až 4 se při zvládání kybernetických bezpečnostních incidentů nahlášených podle § 16 odst. 5 a incidentů oznámených jiným dozorovým orgánem v souvislosti s plněním povinností podle zvláštního odvětvového předpisu ve smyslu § 71 použijí obdobně.“. Připomínkové místo s vypořádáním souhlasí.
751. Kabinet ministra pro legislativu (vláda)	D	K § 20	Akceptováno - nyní § 21

		Z § 20 není jasné, zda konkrétní protiopatření stanoví svým rozhodnutím Úřad. Toto lze fakticky dovodit až z následujících ustanovení, což nepovažujeme za vhodnou legislativní konstrukci.	Začátek odstavce 1 zní nyní následovně: „(1) Protiopatřeními se rozumí úkony Úřadu [...]“. Připomínkové místo s vypořádáním souhlasí.
752. Kabinet ministra pro legislativu (vláda)	D	K § 21 odst. 1 (1)Úřad je po konzultaci s dotčeným poskytovatelem regulované služby z důvodu ochrany ~~vnitřního~~ či veřejného pořádku a vnitřní bezpečnosti	Neakceptováno - nyní § 22 NÚKIB se z důvodu souladu s obdobnou právní úpravou odkazuje na instituty vnitřní a veřejný pořádek, tak, jak je tomu například v zákoně č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů, který operuje s uvedenými pojmy velmi podobně. Na základě rešeršní činnosti a konzultací s relevantními subjekty jsme dospěli k názoru, že by měly být chráněny množiny takto uvedené v zákoně. Připomínkové místo s vypořádáním souhlasí.
753. Kabinet ministra pro legislativu (vláda)	D	K § 23, 25 odst. 3, 65 Doporučujeme zvážit, zda některá procesní ustanovení (např. v odstavci 3) nepřesunout do § 65 (Společná a zvláštní ustanovení o řízení před Úřadem). Obdobně platí i pro § 25odst. 3.	Neakceptováno - nyní § 24, 26 - § 65 byl zrušen Návrh zákona vychází koncepčně z původního zákona o kybernetické bezpečnosti v tom, že provádí adresáta normy jak hmotněprávní úpravou, tak procesní zárovek. Máme za to, že se jedná o úpravu, která je vůči jejím adresátům návodná a přehledná. Připomínkové místo s vypořádáním souhlasí.
754. Kabinet ministra pro legislativu (vláda)	D	K § 25 odst. 1 Úřad ~~může~~ v rozhodnutí podle věty první ~~určit~~ určí formát, rozsah, způsob a lhůtu předání a stanovit povinnost po provedení předání tyto informace a data a jejich kopie bezpečně zlikvidovat.	Neakceptováno - nyní § 26 Úřad má zasahovat pouze v nezbytně nutných případech, není tedy žádoucí, aby určoval formát, rozsah, způsob a lhůtu předání, pokud to v daném případě není nezbytně nutné. Připomínkové místo s vypořádáním souhlasí.

755. Kabinet ministra pro legislativu (vláda)	D	K hlavě II dílu 4 Navrhujeme formulovat ustanovení o strategicky významné službě obdobně jako ustanovení o regulované službě.	Akceptováno Ustanovení o strategicky významné službě byla naformulována obdobně jako ustanovení o regulované službě. Připomínkové místo s vypořádáním souhlasí.
756. Kabinet ministra pro legislativu (vláda)	D	K § 27 odst. 2 (2)Strategicky významnou službou je dále regulovaná služba stanovená u poskytovatele regulované služby v režimu vyšších povinností rozhodnutím Úřadu v případě, že by narušení bezpečnosti informací regulované služby mohlo způsobit závažný dopad na bezpečnost České republiky nebo ~~vnitřní či veřejný pořádek~~, veřejný pořádek, vnitřní bezpečnost nebo veřejné zdraví.	Neakceptováno - nyní § 28 NÚKIB se v užití těchto pojmů v rámci § 28 odst. 2 inspiroval mimo jiné ze zákona č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů, který tyto pojmy užívá obdobně. Vzhledem k účelu navrhovaného zákona dává smysl ponechání stávajících institutů vnitřního a veřejného pořádku. Na základě rešeršní činnosti a konzultací s relevantními subjekty jsme dospěli k názoru, že by měly být chráněny množiny takto uvedené v zákoně. Připomínkové místo s vypořádáním souhlasí.
757. Kabinet ministra pro legislativu (vláda)	D	K § 28 odst. 1, 30 odst. 1, 31 odst. 1 (1)Úřad shromažďuje a vyhodnocuje informace a data spojené s orgánem či osobou, které se týkají možné hrozby pro bezpečnost České republiky, ~~vnitřní či veřejný pořádek~~ veřejný pořádek, vnitřní bezpečnost nebo veřejné zdraví nebo ~~anebo~~ naplnění kritérií rizikovosti dodavatele.	Neakceptováno - nyní § 29, 31, 32 Jak již bylo zmíněno v obdobné připomínce, směřující k vnitřnímu a veřejnému pořádku v rámci § 28, NÚKIB se v užití těchto pojmů v rámci § 27 odst. 2 inspiroval mimo jiné ze zákona č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů, který tyto pojmy užívá obdobně. Vzhledem k účelu navrhovaného zákona dává smysl ponechání stávajících institutů vnitřního a veřejného pořádku. Připomínkové místo s vypořádáním souhlasí.
758. Kabinet ministra pro legislativu (vláda)	D	K § 29 odst. 1, 29 odst. 2	Akceptováno – nyní § 30

		(1) Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí a Ministerstvo vnitra za účelem výkonu činnosti podle § 28 odst. 1 poskytnou Úřadu na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů ode dne obdržení žádosti, stanovisko o naplnění kritéria rizikovosti dodavatele konkrétním orgánem či osobou, požadované informace <u>nebo jinou součinnost</u>. V ustanovení § 29 odst. 1 se stanoví, že zde vyjmenovaná ministerstva mají povinnost poskytnout Úřadu na základě jeho žádosti stanovisko o naplnění kritéria rizikovosti dodavatele. To je zcela přesně definovaný konkrétní úkon, k jehož vyžádání se v předmětném ustanovení zakládá Úřadu pravomoc. V závěru tohoto ustanovení je však dovětek, který toto ustanovení zcela neúměrně rozšiřuje na jakoukoliv „jinou součinnost“, jejíž rámec není tímto zákonem nijak upraven ani omezen. Domníváme se, že takto vágně stanové oprávnění Úřadu a naproti tomu povinnost ministerstev není vhodným a ani ústavně právně konformním řešením. Totéž pak platí i pro následující odstavec 2.	Byla doplněna navrhovaná úprava a odstraněna formulace „a jinou součinnost“. Připomínkové místo s vypořádáním souhlasí.
759. Kabinet ministra pro legislativu (vláda)	D	K § 29 odst. 3 Z odstavce 3 vyplývá, že pokud Úřad nezíská informace pro výkon své činnosti podle odstavců 1 nebo 2, tj. od zde stanovených subjektů, poskytnout mu požadované informace na jeho žádost orgány a osoby v odstavcích 1 a 2 neuvedené. Tato povinnost je tedy takto stanovena pro kohokoli s tím, že za její nesplnění hrozí sankce ve formě pokuty až do výše 50 mil. Kč. Je otázkou, zda je tato úprava skutečně zamýšlena, nebo by měla být nějak upřesněna (např. přesnějším vymezením okruhu subjektů, na které se má daná povinnost vztahovat).	Vysvětleno - nyní § 30 Formulace ustanovení opravdu míří na neurčitý okruh orgánů a osob. V případě, kdy se NÚKIB nepodaří získat všechny informace potřebné pro prověření dodavatele z vlastní činnosti a z činnosti orgánů uvedených v odstavcích 1 a 2, musí mít NÚKIB možnost dotázat se v zásadě kohokoliv. Zdůrazňujeme však, že tak bude činěno proporcionálně v souladu se základními zásadami činnosti správních orgánů. Připomínkové místo s vypořádáním souhlasí.
760. Kabinet ministra pro legislativu (vláda)	D	K § 30 odst. 1 Z odstavce 1 není zřejmé, jaké podmínky (pro co/čeho) mají být opatřením obecné povahy stanoveny. Navrhujeme upřesnit.	Vysvětleno - nyní § 31 Podmínky stanovené opatřením obecné povahy se budou vztahovat na možnost využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu. Konkrétněji pak mohou mít

			podmínky podobu určitého omezení využití plnění dodavatele, které může být podmíněno ať už z hlediska technického (tedy možností využívat dodavatele pouze v určitých částech infrastruktury) nebo časového (možnost využití dodavatele pouze po určitou dobu). Podmínkami, které budou stanoveny v opatření obecné povahy, se budou muset řídit všichni poskytovatelé strategicky významných služeb, k čemuž jim bude poskytnuta adekvátní lhůta. Připomínkové místo s vypořádáním souhlasí.
761. Kabinet ministra pro legislativu (vláda)	D	K § 30 odst. 2 písm. b) bod 1 Inení stanovena podle doby odpisování podle ~~právního předpisu upravujícího zdanění příjmu~~ zákona o daních z příjmů	Neakceptováno - nyní § 31 Podle čl. 45 odst. 4 Legislativních pravidel vlády může mít normativní odkaz na jiný právní předpis podobu zobecněného názvu umožňujícího jednoznačné určení tohoto jiného právního předpisu. Tento způsob odkazování byl zvolen z toho důvodu, že dojde-li k novelizaci či vydání nového právního předpisu upravujícího dotčenou problematiku, nebude nutné zákon o kybernetické bezpečnosti novelizovat. Připomínkové místo s vypořádáním souhlasí.
762. Kabinet ministra pro legislativu (vláda)	D	K § 30 odst. 2 V případě odstavce 2 nepovažujeme za vhodné, aby do schvalování návrhu opatření obecné povahy vstupovala Bezpečnostní rada státu, která je toliko poradním orgánem (vlády) bez vlastní zákonné působnosti a odpovědnosti. Není ani zřejmé výsadní postavení Ministerstva financí tamtéž, pokud má být toto ministerstvo do procesu tvorby opatření obecné povahy zahrnuto, měla by jeho úloha být přemístěna do § 29	Vysvětleno - nyní § 31 Bezpečnostní rada státu je klíčovým bezpečnostním orgánem ČR, z tohoto důvodu je vhodné, aby byla informována o využívání bezpečnostních mechanismů, jakým je prověřování dodavatelského řetězce a případně aby měla možnost do něj vstoupit způsobem, který její jednací řád umožňuje (návrh neprojedná, přeruší jeho projednávání, vrátí jej k přepracování, případně s ním vyjádří nesouhlas). MF má v procesu vydávání opatření specifickou roli, jelikož na rozdíl od ostatních orgánů uvedených v § 30

			nebude typicky v pozici orgánu posuzujícího bezpečnostní otázky opatření, avšak bude posuzovat soulad opatření se závazky České republiky v oblasti mezinárodní ochrany investic. Pakliže však bude MF disponovat informacemi, které budou pro posouzení předmětné hrozby nezbytné, bude zapojeno také do procesu přípravy opatření postupem dle § 31. Připomínkové místo s vypořádáním souhlasí.
763. Kabinet ministra pro legislativu (vláda)	D	K § 31 odst. 2 (2)Řízení o povolení výjimky podle odstavce 1 ~~lze zahájit se zahajuje~~ na žádost poskytovatele strategicky významné služby nebo z moci úřední. Žadatel je povinen ~~v rámci~~ k žádosti připojit důkazy prokazující skutečnosti, kterých se dovolává.	Akceptováno - nyní § 32 Připomínkové místo s vypořádáním souhlasí.
764. Kabinet ministra pro legislativu (vláda)	D	K § 34 odst. 1, 34 odst. 2 (1)Poskytovatel strategicky významné služby je povinen zajistit ~~její~~ dostupnost ~~strategicky významné služby~~ v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky. (2)Poskytovatel strategicky významné služby je povinen ~~testovat~~ ověřovat schopnost zajištění jejího poskytování ~~strategicky významné služby~~ v rozsahu kritické části [...]	Akceptováno jinak - nyní § 35 Odstavec 1 byl upraven dle připomínky, v odst. 2 bylo slovo "ověřovat" zaměněno za slovo "prověřovat", které lépe odpovídá kladeným požadavkům. Připomínkové místo s vypořádáním souhlasí.
765. Kabinet ministra pro legislativu (vláda)	D	K § 36 odst. 5 Zásady a postupy pro zveřejňování těchto údajů ~~jsou~~ musejí být veřejně dostupné	Akceptováno - nyní § 37 odst. 6 Připomínkové místo s vypořádáním souhlasí.
766. Kabinet ministra pro legislativu (vláda)	D	K § 40 odst. 1 písm. b), 40 odst. 1 písm. c) b)vyžádat si od orgánů a osob informace o věcných prostředcích, o výrobních, provozních a personálních ~~kapacitách~~ zdrojích a o objemu zásob ve stanovených druzích materiálu, přičemž tyto orgány a osoby mají povinnost poskytnout Úřadu vyžadované informace úplně a pravdivě v Úřadem stanovené lhůtě,	Akceptováno jinak – nyní § 41 Text byl upraven, i po vzoru zákona č. 241/2000 Sb., na "výrobní a provozní kapacity a personální zdroje". Připomínkové místo s vypořádáním souhlasí.

767. Kabinet ministra pro legislativu (vláda)	D	K § 40 odst. 1 písm. g) g)nařídit orgánům a osobám provedení skenu zranitelností nebo hodnocení zabezpečení počítačových zařízení, systémů nebo aplikací (dále jen „penetrační test“) ~~penetračního testu,~~	Akceptováno jinak - nyní § 41 § 41 odst. 1 písm. g) byl upraven na: „g)nařídit orgánům a osobám provedení skenu zranitelností nebo provedení identifikace a ověření zranitelností prostřednictvím simulace reálného útoku (dále jen "penetrační test")“. Připomínkové místo s vypořádáním souhlasí.
768. Kabinet ministra pro legislativu (vláda)	D	K § 40 odst. 1 písm. d) Není zřejmé, co se rozumí pojmem „nařídit práce v pohotovostním režimu“ podle § 40 odst. 1 písm. d). Upozorňujeme na zákoník práce, kterým je zaveden institut pracovní pohotovosti. Pokud to má být totéž, je třeba to terminologicky sladit. Dále není zřejmé, komu může Úřad práci v pohotovostním režimu nařídit (pouze svým zaměstnancům, nebo komukoli?).	Akceptováno - nyní § 41 Obsah ustanovení byl v rámci spolupráce s gestorem problematiky krizového řízení - Ministerstvem vnitra, Generálním ředitelstvím Hasičského záchranného sboru upraven. Připomínkové místo s vypořádáním souhlasí.
769. Kabinet ministra pro legislativu (vláda)	D	K hlavě V dílu 1 Díl 1 ~~Instituce zapojené do výkonu státní správy~~ Orgány a osoby vykonávající státní správu v oblasti kybernetické bezpečnosti V celém textu návrhu zákona je opakovaně používán pojem „orgány a osoby“, který by měl podle důvodové zprávy zahrnout co nejširší okruh adresátů této normy. Vzhledem k této skutečnosti by měl být v nadpisu tohoto dílu použity obdobné pojmy, aby nedocházelo k výkladovým nejasnostem. Rovněž slovní spojení „zapojené do výkonu státní správy“ se nejeví jako příliš vhodné, neboť není zřejmé, jaký je obsah a zejména pak rozsah tohoto pojmu.	Akceptováno jinak Text byl v souladu s další připomínkou na toto téma upraven na „Orgány a osoby vykonávající veřejnou správu v oblasti kybernetické bezpečnosti“. Připomínkové místo s vypořádáním souhlasí.
770. Kabinet ministra pro legislativu (vláda)	D	K § 41 odst. 1 ~~Národní úřad pro kybernetickou a informační bezpečnost~~ Úřad (1)Úřad je ústředním správním úřadem pro oblast kybernetické bezpečnosti a pro ~~vybrané tímto zákonem stanovené~~ oblasti ochrany	Neakceptováno - nyní § 44 Oblasti ochrany utajovaných informací, které jsou v působnosti Úřadu, stanovuje zákon o ochraně utajovaných informací, nikoliv tento zákon.

		utajovaných informací podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti	Připomínkové místo s vypořádáním souhlasí.
771. Kabinet ministra pro legislativu (vláda)	D	K § 41 odst. 3 písm. t) ~~t)kontinuálně~~ průběžně se připravuje na zajištění ~~připravenosti na řešení a nápravu~~ nápravy stavu kybernetického nebezpečí	Akceptováno - nyní § 44 odst. 3 písm. s) Text § 44 odst. 3 písm. s) byl upraven dle připomínky na: „ <i>průběžně se připravuje na zajištění řešení a nápravy stavu kybernetického nebezpečí</i> “. Připomínkové místo s vypořádáním souhlasí.
772. Kabinet ministra pro legislativu (vláda)	D	K § 41 odst. 3 písm. x) ~~x)provádí kontrolu plnění povinností podle tohoto zákona a poskytuje jinou~~ nezbytnou součinnost na základě žádosti dozorového orgánu jiného členského státu	Akceptováno - nyní § 44 odst. 3 písm. w) Text § 44 odst. 3 písm. w) byl upraven dle připomínky na: „ <i>poskytuje nezbytnou součinnost na základě žádosti dozorového orgánu jiného členského státu Evropské unie</i> “. Připomínkové místo s vypořádáním souhlasí.
773. Kabinet ministra pro legislativu (vláda)	D	K § 41 odst. 4 písm. b) ~~b)nejméně každých 5 let zpracovává a vládě předkládá ke schválení národní strategii kybernetické bezpečnosti a akční plán k jejímu naplňování a tuto strategii aktualizuje nejméně každých 5 let,~~	Akceptováno - nyní § 44 odst. 4 písm. b) Text § 44 odst. 4 písm. b) byl upraven dle připomínky. Připomínkové místo s vypořádáním souhlasí.
774. Kabinet ministra pro legislativu (vláda)	D	K § 41 odst. 5 písm. f) ~~f)spolupracuje s orgány a osobami působícími v oblasti kybernetické bezpečnosti~~ vykonávajícími státní správu v oblasti kybernetické bezpečnosti	Neakceptováno - nyní § 44 odst. 5 písm. f) Text 44 odst. 5 písm. f) byl upraven na: „spolupracuje s orgány a osobami v oblasti kybernetické bezpečnosti“, aby bylo jasnější, že se jedná o spolupráci i s orgány a osobami, které státní správu v oblasti kybernetické bezpečnosti nevykonávají. Připomínkové místo s vypořádáním souhlasí.
775. Kabinet ministra pro legislativu (vláda)	D	K § 41 odst. 5 písm. i)	Akceptováno - nyní § 44 odst. 5 písm. i)

		i) může s orgány a osobami sdílet sdílí údaje a informace ze své činnosti a z evidencí vedených Úřadem, je-li to nezbytné pro zajišťování kybernetické bezpečnosti;	Text § 44 odst. 5 písm. i) zní: "i) byl upraven dle připomínky. Připomínkové místo s vypořádáním souhlasí.
776. Kabinet ministra pro legislativu (vláda)	D	K § 41 odst. 5 písm. k) k) ve vhodných případech předává bez zbytečného odkladu informace o kybernetickém bezpečnostním incidentu s významným dopadem [...]	Neakceptováno - nyní § 44 odst. 5 písm. k) Jedná se o povinnost přejatou z čl. 23 odst. 6 NIS2, podle kterého danou informaci předává tým CSIRT „tam, kde je to vhodné“. Předávání informací o všech incidentech s významným dopadem bez zvážení vhodnosti předání těchto informací se jeví jako zbytečná zátěž pro adresáty bez zjevného přínosu. Připomínkové místo s vypořádáním souhlasí.
777. Kabinet ministra pro legislativu (vláda)	D	K § 41 Doporučujeme zvážit zvolenou legislativní konstrukci kompetenčních ustanovení. Kompetence Úřadu jsou vymezeny jednak v konkrétních ustanoveních na různých místech návrhu zákona, jednak souhrnně v § 41, který ovšem nezahrnuje všechny kompetence Úřadu nebo některé uvádí dvakrát – např. § 41 odst. 3 písm. v) a § 41 odst. 3 písm. x). Navrhujeme tedy návrh zákona podrobit v tomto směru revizi a zejména odstranit nadbytečná a duplicitní ustanovení.	Neakceptováno - § 44 Duplicitní ustanovení byla částečně upravena, nicméně zákon je takto koncipován proto, aby byl návodný pro svoje adresáty a pokud se některé kompetence týkají vztahu k adresátům normy, jsou zpravidla uvedeny na místě, kde je řešena problematika směrem k nim. Připomínkové místo s vypořádáním souhlasí.
778. Kabinet ministra pro legislativu (vláda)	D	K § 41 odst. 3, 41 odst. 4 Dáváme ke zvážení, zda je v § 41 odst. 3 a 4 nezbytný tak rozsáhlý katalog „důležitosti“ Úřadu, například vydávat Věstník a zveřejnit jej na svých internetových stránkách lze nepochybně i bez kompetenčního ustanovení. Dále považujeme za vhodné přezkoumat, zda je nutné v § 41 odst. 4 písm. c) vypisovat všechna uvedená střediska, pokud se zruší, jejich počet navýší, nebo jen změni název některého z nich, bylo by nutné kvůli tomu zákon novelizovat. Obdobné platí i pro § 41 odst. 4 písm. f).	Neakceptováno Část připomínky, která se týká Věstníku byla akceptována. Pravomoc k vydávání Věstníku byla zavedena kvůli zveřejnění veřejnoprávní smlouvy, uzavírané s provozovatelem Národního CERT a zveřejnění seznamu subjektů, se kterými byla uzavřena veřejnoprávní smlouva podle zákona o ochraně utajovaných informací (§ 52), který je ale aktuálně v procesu novelizace, a povinnost zveřejnit ve věstníku je v něm upravena jinak. Nově bylo

			upraveno, že veřejnoprávní smlouva uzavíraná s provozovatelem Národního CERT bude zveřejňována na Úřední desce Úřadu, nikoliv ve Věstníku, a vydávání Věstníku Úřadu bylo ze zákona vypuštěno. Část připomínky, týkající se specializovaných středisek: Vyjmenovaná střediska vyplývají z mezinárodních předpisů, koncepce NATO a EU a jejich taxativní výčet je žádoucí. Ke změně by došlo pouze v případě, že by byla měněna koncepce ochrany utajovaných informací na úrovni NATO a EU, přičemž v takovém případě by se měnila koncepce i v ČR, a tedy nutně i tento zákon nejen v souvislosti s činností jmenovaných středisek. Připomínkové místo s vypořádáním souhlasí.
779. Kabinet ministra pro legislativu (vláda)	D	K § 41 odst. 5 Navrhujeme přeformulovat úvodní část odstavce 5 a jednoznačně v něm stanovit, že součástí Úřadu je Vládní CERT a následně stanovit jeho kompetence.	Akceptováno - nyní § 44 odst. 5 Text § 44 odst. 5) byl upraven na: „Součástí Úřadu je Vládní CERT, který:“. Připomínkové místo s vypořádáním souhlasí.
780. Kabinet ministra pro legislativu (vláda)	D	K § 42 Z ustanovení § 42 podle našeho názoru jednoznačně nevyplývá, kdo a jakým způsobem se může stát provozovatelem Národního CERT. Navrhujeme v tomto směru návrh zákona upřesnit a formulovat jednoznačně.	Akceptováno – nyní § 45 Byla upravena systematika a některé části ustanovení týkajícího se Národního CERT. Připomínkové místo s vypořádáním souhlasí.
781. Kabinet ministra pro legislativu (vláda)	D	K § 42 odst. 2 písm. b) V ustanovení § 42 odst. 2 písm. b) stanovuje zájemci o provozování Národního CERT povinnost ke své žádosti předložit „potvrzení příslušných orgánů Finanční správy České republiky, Celní správy České republiky, České správy sociálního zabezpečení a příslušné pojišťovny v případě odstavce 1 písm. e), která nesmí být starší než 30 dnů“. V rámci snižování administrativní zátěže by možná stálo za	Akceptováno jinak – nyní § 45 Na základě této a jiné připomínky byl požadavek na potvrzení orgánů Finanční správy České republiky a Celní správy České republiky vypuštěn. Daňový řád v § 53 odst. 1 písm. l) umožňuje orgánům veřejné moci ověřit zákonné požadavky, přičemž prolomí daňovou mlčenlivost.

		úvahu stanovit Úřadu oprávnění si tyto údaje vyžadovat sám v rámci své zákonem stanovené působnosti. Obdobná připomínka se pak týká i ustanovení § 48 odst. 2.	Připomínkové místo s vypořádáním souhlasí.
782. Kabinet ministra pro legislativu (vláda)	D	K § 42 odst. 2 písm. b) Není jasné, proč orgánem potvrzujícím bezdlužnost na pojistném na sociální pojištění má být pouze Česká správa sociálního zabezpečení. Upozorňujeme na to, že orgány sociálního zabezpečení, které toto pojistné vybírají, vymáhají pohledávky na pojistném a rozhodují o penále, jsou okresní správy sociálního zabezpečení. Ustanovení tedy navrhuje uvést do souladu s předpisy upravujícími výběr pojistného na sociální zabezpečení a příspěvek na státní politiku zaměstnanosti.	Akceptováno – nyní § 45 Došlo k úpravě ustanovení § 45 odst. 2 písm. b) (nyní v odst. 5) a bude požadováno doložení potvrzení prokazujícího bezdlužnost na pojistném na sociální pojištění od příslušné okresní správy sociálního zabezpečení. Připomínkové místo s vypořádáním souhlasí.
783. Kabinet ministra pro legislativu (vláda)	D	K § 43 odst. 3 (3) Pokud tento zákon nestanoví jinak, vztahuje se na jednání kontrolního orgánu a na práva a povinnosti jeho členů přiměřeně jiný právní předpis – jednací řád Poslanecké sněmovny.	Akceptováno – nyní § 46 § 46 odst. 3 byl upraven na: „Pokud tento zákon nestanoví jinak, vztahuje se na jednání kontrolního orgánu a na práva a povinnosti jeho členů přiměřeně jednací řád Poslanecké sněmovny.“. Připomínkové místo s vypořádáním souhlasí.
784. Kabinet ministra pro legislativu (vláda)	D	K § 48 odst. 1 písm. e), 42 odst. 2 písm. b) Není jasné, proč neexistenci nedoplatku na pojistném nebo na penále na veřejné zdravotní pojištění podle § 48 odst. 1 písm. e) stačí prokázat čestným prohlášením, ale tutéž skutečnost podle § 42 odst. 2 písm. b) musí potvrdit příslušná zdravotní pojišťovna.	Akceptováno – nyní § 51 Navrhovaná zákonná úprava byla v příslušných ustanoveních sjednocena. Připomínkové místo s vypořádáním souhlasí.

785. Kabinet ministra pro legislativu (vláda)	D	K § 51 (1)Úřad průběžně posuzuje plnění požadavků podle § 47 odst. 2 po celou dobu trvání členství žadatele v Komunitě, ~~jehož žádosti o registraci v Komunitě bylo registrujícím orgánem vyhověno.~~ (2)V případě, že žadatel, který je registrovaný jako člen Komunity, nesplňuje podmínky podle § 47 odst. 2, zahájí Úřad řízení o jeho nezpůsobilosti ~~žadatele k~~ ke členství v Komunitě. (3)Po právní moci rozhodnutí o nezpůsobilosti ~~žadatele k členství v Komunitě~~ registrovaného člena Komunity vydaného v řízení podle odstavce 2 Úřad vyrozumí registrující orgán o jeho nezpůsobilosti ~~žadatele k~~ ke členství v Komunitě.	Akceptováno – nyní § 54 Navržené změny byly v § 54 zohledněny. Připomínkové místo s vypořádáním souhlasí.
786. Kabinet ministra pro legislativu (vláda)	D	K § 52 (1)Úřad ~~uzavírá~~ uzavře veřejnoprávní smlouvu s právnickou osobou vybranou postupem podle § 163 odst. 4 správního řádu za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění činností podle § 42 odst. 3 (dále jen „veřejnoprávní smlouva“). Řízení o výběru ~~žadosti~~ provozovatele Národního CERT vyhláší Úřad	Akceptováno jinak – nyní § 55 V textu upraveno „uzavírá“ na „uzavře“. Formulace „řízení o žádosti“ odkazuje na podávání žádostí v řízení o výběru žádosti podle § 146 zákona č. 500/2004 Sb., správní řád, na který odkazuje § 163 odst. 4 správního řádu, podle nějž se řídí uzavírání veřejnoprávní smlouvy s provozovatelem Národního CERT. Připomínkové místo s vypořádáním souhlasí.
787. Kabinet ministra pro legislativu (vláda)	D	K § 53 odst. 1 (1)Úřad a provozovatel Národního CERT zpracovávají osobní údaje, jsou li nezbytné pro výkon jejich působnosti. Tyto údaje Úřad a provozovatel Národního CERT předávají orgánům ~~veřejné moci~~ nebo osobám vykonávajícím státní správu v oblasti kybernetické bezpečnosti, je-li to nezbytné pro plnění jejich úkolů a nedojde-li tím k porušení povinnosti mlčenlivosti podle tohoto zákona.	Akceptováno jinak – nyní § 56 Ustanovení bylo na základě jiné připomínky vypuštěno. Připomínkové místo s vypořádáním souhlasí.
788. Kabinet ministra pro legislativu (vláda)	D	K § 54 odst. 1 V ustanovení § 54 odst. 1 úvodní části ustanovení je zavedena legislativní zkratka „jiný členský stát“, který z povahy věci nezahrnuje	Vysvětleno – nyní § 57 Legislativní zkratka nebyla v odstavci 5 použita úmyslně. Ovšem za účelem lepší srozumitelnosti byla

		Českou republiku jako členský stát Evropské unie. V následujících ustanoveních, zejména pak v odstavci 5 je však použit pojem „členský stát Evropské unie“, který, na rozdíl o zavedené legislativní zkratky již Českou republiku zahrnuje. Otázkou zůstává, zda to byl úmysl předkladatele, či zda by i v těchto dvou případech v odstavci 5 měla být použita ona legislativní zkratka „jiný členský stát“. Obdobná připomínka se pak týká i dalších ustanovení návrhu zákona, ve kterých je pojem „členský stát Evropské unie“ použit. Například v ustanovení § 35 odst. 1 písm. b) a c) a §48 odst. 4 písm. b).	na základě připomínky legislativní zkratka zrušena a pojem byl na všech místech v zákoně rozepsán, aby bylo zřetelné, zdali se jedná o všechny členské státy EU (včetně ČR), nebo o jiné členské státy EU (bez ČR). Připomínkové místo s vypořádáním souhlasí.
789. Kabinet ministra pro legislativu (vláda)	D	K § 55 ~~§~~ ~~Prováděcí právní předpisy a zmocňovací ustanovení~~ ~~(1) Prováděcí právní předpis stanoví~~ ~~a) kritéria pro identifikaci regulované služby (§ 4);~~ ~~b) způsob stanovení režimu poskytovatele regulované služby (§ 6 odst. 3);~~ ~~c) bezpečnostní opatření odpovídající režimu poskytovatele regulované služby a míru a způsob jejich zavedení a provádění (§ 14 odst. 2 a 4);~~ ~~d) způsob stanovení významného dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby v režimu nižších povinností (§ 16 odst. 3);~~ ~~e) obsahové náležitosti, formát a způsob oznámení provedení protioopatření a jeho výsledku (§ 20 odst. 3);~~ ~~f) kritéria pro identifikaci strategicky významné služby (§ 27 odst. 1);~~ ~~g) nepominutelné funkce stanoveného rozsahu (§ 28 odst. 4);~~ ~~h) kritéria rizikovosti dodavatele a způsob jejich vyhodnocení (§ 28 odst. 4);~~ ~~i) způsob hlášení údajů subjektem poskytujícím služby registrace jmen domén (§ 35 odst. 1) a~~ ~~j) technické a organizační podmínky používání Portálu NÚKIB, obsahové náležitosti, formát, strukturu a způsob provádění úkonů uvedených v § 44 odst. 2 (§ 44 odst. 3).~~ ~~(2) Prováděcí právní předpisy podle odstavce 1 vydá Úřad ve formě~~	Akceptováno § 55 byl vypuštěn. Připomínkové místo s vypořádáním souhlasí.

		vyhlášky. V návaznosti na vypuštění § 55 (k tomu viz obecná připomínka v dopise následující paragrafy a odkazy na ně přečíslovat.	
790. Kabinet ministra pro legislativu (vláda)	D	K § 56 odst. 3 Domníváme se, že ustanovení o tom, které konkrétní osoby jsou oprávněny vykonávat kontrolu (pověření zaměstnanci Úřadu), vyplývá z kontrolního řádu. Odstavec 3 se tedy v tomto kontextu jeví jako nadbytečný a měl by být vypuštěn.	Akceptováno - nyní § 58 Odstavec 3 byl na základě připomínky zrušen. Připomínkové místo s vypořádáním souhlasí.
791. Kabinet ministra pro legislativu (vláda)	D	K § 57 odst. 1 Zjistí-li Úřad ~~při kontrole~~ nedostatky, může ~~rozhodnutím~~ uložit kontrolovanému orgánu nebo osobě, aby je ve stanovené lhůtě odstranila, popřípadě určit jakým způsobem. V odstavci 1 navrhujeme slovní spojení „při kontrole“ vypustit jako nadbytečná a do jisté míry svazující, neboť z ničeho obecně nevyplývá, že by se opatření k nápravě mohla ukládat jen na základě provedené kontroly, jakkoliv tomu tak v praxi zřejmě často bude, ale není to právní podmínka. Obdobná připomínka se pak týká všech dalších ustanovení zákona, ve kterých se institut „kontroly“ ve spojení s nápravnými opatřeními a se sankcemi objevuje.	Akceptováno – nyní § 59 Připomínkové místo s vypořádáním souhlasí.
792. Kabinet ministra pro legislativu (vláda)	D	K § 57 odst. 1 Rovněž v odstavci 1 lze slovo „nedostatky“ považovat za velmi obecné na to, aby jím byla aktivována pravomoc vést správní řízení, jehož výsledkem by bylo například uložení sankce – pokud by to mělo být vázáno na kontrolu, pak by tato právní úprava měla navazovat na § 2 kontrolního řádu, kde se obecně stanoví, co je předmětem kontroly, tzn. povinnosti stanovené právními předpisy nebo uložené na základě právních předpisů (např. rozhodnutími nebo opatřeními obecné povahy).	Akceptováno – nyní § 59 Připomínkové místo s vypořádáním souhlasí.
793. Kabinet ministra pro legislativu (vláda)	D	K § 57 odst. 1, 57 odst. 3 Pokud se v odstavci 3 vylučuje odkladný účinek odvolání, je v zásadě nadbytečné v odstavci 1 zdůrazňovat, že se nápravné opatření ukládá	Akceptováno – nyní § 59 Připomínkové místo s vypořádáním souhlasí.

		rozhodnutím – pokud by to měl být faktický pokyn mimo správní řízení, muselo by to být upraveno jiným způsobem.	
794. Kabinet ministra pro legislativu (vláda)	D	K § 57 odst. 1 V odstavci 1 se stanoví pravomoc Úřadu uložit „orgánu nebo osobě“ nápravné opatření. V případě „orgánu“ je to poněkud složitější, protože pokud se má opatření k nápravě ukládat rozhodnutím ve správním řízení, správní řád vychází obecně z toho, že účastníkem řízení může být jen osoba, viz § 27 správního řádu, tzn. osoba v právním smyslu, neboť i pro veřejné právo obecně platí to, co je v § 17 občanského zákoníku, tzn. že práva a povinnosti může mít jen osoba, nikoliv něco, co nemá právní subjektivitu, tedy např. orgány (státu, obcí, krajů atd.) a v takovém případě platí, že povinnost uložená tomu, co právní subjektivitu nemá, je de iure povinností uloženou tomu, kdo právní subjektivitu má a jehož je tento „nonsubjekt“ součástí, tzn. např. nikoliv státní orgán ale stát jako právnická osoba, viz obecně § 6 zákona č. 219/2000 Sb., koneckonců pokud jsou v § 58 přestupky, tak přestupku se také nemůže dopustit orgán ale jen osoba, viz zákon č. 250/2016 Sb., protože jen osoba může mít de iure povinnost, kterou může porušit, takže i přestupkové řízení by se muselo vést s osobou a ne orgánem.	Neakceptováno – nyní § 59 Úprava vychází z již zavedeného systému, kdy kybernetická bezpečnost státu závisí mimo jiné na zabezpečení jeho orgánů. Norma by bez odpovídající sankce byla imperfektní, což je v případě kybernetické bezpečnosti výrazně nežádoucí. Tento systém zná jak stávající zákon o kybernetické bezpečnosti, tak například zákon č. 110/2019 Sb., o zpracování osobních údajů, jelikož koncepce ochrany údajů v rámci EU, stejně jako koncepce kybernetické bezpečnosti, zahrnuje i takové adresáty, jakými jsou orgány veřejné moci. Připomínkové místo s vypořádáním souhlasí.
795. Kabinet ministra pro legislativu (vláda)	D	K § 57 odst. 2 ~~(2)Považuje-li Úřad skutková zjištění za dostatečná, může uložit nápravné opatření podle odstavce 1 i bez provedení kontroly. Pokud budou z odstavce 1 vypuštěna slova „při kontrole“, stane se odstavce 2 nadbytečný, neboť uložení nápravných opatření nebude vázáno na provedenou kontrolu. V takovém případě bude nutno následující odstavce 3 a případně odkazy na něj přečíslovat.~~	Akceptováno – nyní § 59 Připomínkové místo s vypořádáním souhlasí.
796. Kabinet ministra pro legislativu (vláda)	D	K § 58 odst. 11 (11)Žadatel se dopustí přestupku tím, že v době trvání členství v Komunitě podle § 47 neuvede změnu údajů potřebných pro posouzení jeho základní a zvláštní způsobilosti Úřadem, ~~jejich změnu zamítl~~	Akceptováno – nyní § 60 Upravené znění dotčeného ustanovení: „Člen Komunity se dopustí přestupku tím, že v době trvání členství v Komunitě podle § 47 neuvede změnu údajů potřebných pro posouzení jeho základní a zvláštní

		nebo neuvede další skutečnosti rozhodné pro posouzení jeho základní a zvláštní způsobilosti, ~~nebo tyto skutečnosti zaměří.~~	způsobilosti Úřadem nebo neuvede další skutečnosti rozhodné pro posouzení jeho základní a zvláštní způsobilosti." Připomínkové místo s vypořádáním souhlasí.
797. Kabinet ministra pro legislativu (vláda)	D	K § 59 odst. 2, 59 odst. 4 Zavedení právní domněnky v odstavci 2 považujeme za poměrně nestandardní a není nám ani jasný jeho význam a smysl. Upozorňujeme na definici přestupku podle § 5 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, podle které je přestupek společensky škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin. Čin, které by byl v zákoně za přestupek výslovně označen a vykazoval by znaky zákonem stanovené, ale nebyl by společensky škodlivý, by tak nemohl být přestupkem. Odstavec 2 proto navrhuje vypustit, neboť je v rozporu s úpravou zákona o odpovědnosti za přestupky a řízení o nich. Obdobně platí i pro domněnku uvedenou v odstavci 4.	Akceptováno jinak – nyní § 61 Ustanovení § 59 odst. 2 bude vypuštěno. Ustanovení § 59 odst. 4 naopak nebude z návrhu zákona vypuštěno, neboť z našeho pohledu zvyšuje právní jistotu, jelikož na jisto staví u vymezených skutkových podstat, že se jedná o trvající přestupky a tato skutečnost nemůže být předmětem sporu. Ustanovením je reflektováno, že není postihováno pouze jednorázové porušení povinnosti, ale za vysoce nežádoucí je považováno to, kdy je závažný stav udržován a existuje významný zájem na odstranění tohoto závažného stavu a co nejrychlejší náprava. Připomínkové místo s vypořádáním souhlasí.
798. Kabinet ministra pro legislativu (vláda)	D	K § 60 odst. 1 (1)Úřad může v případě nesplnění povinnosti odstranit zjištěné nedostatky ~~zjištěné při kontrole~~ uložené rozhodnutím Úřadu poskytovateli regulované služby v režimu vyšších povinností, který je držitelem evropského certifikátu kybernetické bezpečnosti podle aktu o kybernetické bezpečnosti nebo jiného certifikátu nebo osvědčení souvisejícího se zajištěním kybernetické bezpečnosti regulované služby, pozastavit tomuto poskytovateli regulované služby platnost evropského certifikátu kybernetické bezpečnosti vydaného Úřadem nebo uložit subjektu posuzování shody povinnost pozastavit platnost jím vydaného certifikátu nebo osvědčení, a to až do doby odstranění zjištěných ~~zjištěných při kontrole~~ nedostatků, nejméně však na 6 měsíců.	Akceptováno – nyní § 62 Text § 62 odst. 1 byl upraven. Připomínkové místo s vypořádáním souhlasí.

799. Kabinet ministra pro legislativu (vláda)	D	K § 60 Doporučujeme zvážit, zda některá procesní ustanovení (např. v odstavci 2) nepřesunout do § 65 (Společná a zvláštní ustanovení o řízení před Úřadem).	Akceptováno jinak § 65 (Společná a zvláštní ustanovení o řízení před Úřadem) byl zrušen a v něm obsažené ustanovení byla rozdělena do jednotlivých ustanovení v zákoně. Připomínkové místo s vypořádáním souhlasí.
800. Kabinet ministra pro legislativu (vláda)	D	K § 62 Ve vztahu k odstavci 3 upozorňujeme na § 10 odst. 2 a zejména § 15 kontrolního řádu. Navrhované ustanovení je tedy nepřímou novelou kontrolního řádu, která je nepřipustná. Uvedené ustanovení je tedy třeba z návrhu zákona vypustit.	Neakceptováno – nyní § 64 Tento stav není v našem právním řádu ojedinělý (například zákon o ochraně hospodářské soutěže). Jsme si však vědomi citlivosti tohoto postupu a proto jsme se v důvodové zprávě u § 64 zaměřili na jeho podrobné odůvodnění. Jedná se z naší strany o důvodnou speciální úpravu vůči kontrolám v oblasti kybernetické bezpečnosti reflektující skutečnost, že současná výše pokut v kontrolním řádu neplní v této oblasti svůj účel a je ve vztahu k výši pokut podle návrhu zákona značně nepoměrná. Připomínkové místo s vypořádáním souhlasí.
801. Kabinet ministra pro legislativu (vláda)	D	K § 68 Finanční zabezpečení stavu kybernetického nebezpečí na běžný rozpočtový rok se provádí podle jiného právního předpisu rozpočtových pravidel	Akceptováno jinak – nyní § 70 Odkaz upraven na následující znění: „podle právního předpisu upravujícího rozpočtová pravidla“. Připomínkové místo s vypořádáním souhlasí.
802. Kabinet ministra pro legislativu (vláda)	D	K § 71 § 71 Přechodná ustanovení ~~1) Správci informačních systémů základní služby, správci informačních a komunikačních systémů kritické informační infrastruktury, správci významných informačních systémů nebo poskytovatelé digitální služby podle § 3 zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona, jimiž~~	Akceptováno jinak Ve vztahu k návěti odst. 1 neakceptováno, neboť přechodné ustanovení se má vztahovat pouze na ty subjekty, které byly správci regulovaných informačních systémů k poslednímu dni účinnosti zákona č. 181/2014 Sb. Bez tohoto upřesnění by bylo možné vykládat ustanovení i tak, že je hovořeno i o správcích, kteří do regulace spadali v období účinnosti

	poskytované služby naplňují kritéria regulované služby podle tohoto zákona, plní pro služby a informační systémy regulované podle dosavadních právních předpisů v rozsahu, ve kterém jsou tyto služby a aktiva regulovány tímto zákonem, alespoň a) povinnosti spojené se zaváděním a prováděním bezpečnostních opatření, hlášením kybernetických bezpečnostních incidentů a plněním opatření Úřadu podle zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona v případě, že je podle tohoto zákona poskytovatelem regulované služby v režimu vyšších povinností, nebo b) povinnosti spojené se zaváděním a prováděním bezpečnostních opatření, hlášením kybernetických bezpečnostních incidentů a plněním opatření Úřadu podle zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona, v rozsahu povinností uložených tímto zákonem poskytovatelům regulovaných služeb v režimu nižších povinností v případě, že je podle tohoto zákona poskytovatelem regulované služby v režimu nižších povinností, a to od okamžiku nabytí účinnosti tohoto zákona až do doby uplynutí lhůt pro zahájení plnění povinností podle tohoto zákona, s výjimkou způsobu hlášení kybernetických bezpečnostních incidentů, který jsou tyto poskytovatele regulované služby povinni realizovat podle tohoto zákona od okamžiku doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb. 2) V řízeních týkajících se splnění povinností uložené zákonem nebo na základě zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona se postupuje podle dosavadních právních předpisů. 3) Varování vydaná podle zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona se považují za varování vydaná podle tohoto zákona. 4) Reaktivní opatření a ochranná opatření, vydaná podle zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona se považují za reaktivní protiopatření vydaná podle tohoto zákona. 5) Nabytím účinnosti tohoto zákona není dotčena platnost	posledního znění zákona, ale z regulace v tomto období také vypadli, což nebylo záměrem. Ve zbytku akceptováno. Připomínkové místo s vypořádáním souhlasí.

	~~veřejnoprávních smluv uzavřených podle zákona č. 181/2014 Sb. přede dnem nabytí účinnosti tohoto zákona.~~ 1.Správci informačních systémů základní služby, správci informačních a komunikačních systémů kritické informační infrastruktury, správci významných informačních systémů nebo poskytovatelé digitální služby podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, jimiž poskytované služby naplňují kritéria regulované služby podle tohoto zákona, plní pro služby a informační systémy regulované podle dosavadních právních předpisů v rozsahu, ve kterém jsou tyto služby a aktiva regulovány tímto zákonem, alespoň c)povinnosti spojené se zaváděním a prováděním bezpečnostních opatření, hlášením kybernetických bezpečnostních incidentů a plněním opatření Úřadu podle zákona č. 181/2014 Sb., ve znění pozdějších předpisů, v případě, že je podle tohoto zákona poskytovatelem regulované služby v režimu vyšších povinností, nebo d)povinnosti spojené se zaváděním a prováděním bezpečnostních opatření, hlášením kybernetických bezpečnostních incidentů a plněním opatření Úřadu podle zákona č. 181/2014 Sb., ve znění pozdějších předpisů, v rozsahu povinností uložených tímto zákonem poskytovatelům regulovaných služeb v režimu nižších povinností v případě, že je podle tohoto zákona poskytovatelem regulované služby v režimu nižších povinností, a to počínaje dnem nabytí účinnosti tohoto zákona až do doby uplynutí lhůt pro zahájení plnění povinností podle tohoto zákona, s výjimkou způsobu hlášení kybernetických bezpečnostních incidentů, který jsou tito poskytovatelé regulované služby povinni realizovat podle tohoto zákona od okamžiku doručení vyznění o zápisu do evidence poskytovatelů regulovaných služeb. 2.V řízeních týkajících se splnění povinností uložené přede dnem nabytí účinnosti tohoto zákona zákonem č. 181/2014 Sb., ve znění pozdějších předpisů, nebo na jeho základě, se postupuje podle	

		dosavadních právních předpisů. 3.Varování vydaná přede dnem nabytí účinnosti tohoto zákona podle zákona č. 181/2014 Sb., ve znění pozdějších předpisů, se považují za varování vydaná podle tohoto zákona. 4.Reaktivní opatření a ochranná opatření, vydaná přede dnem nabytí účinnosti tohoto zákona podle zákona č. 181/2014 Sb., ve znění pozdějších předpisů, se považují za reaktivní protipatření vydaná podle tohoto zákona. 5.Nabytím účinnosti tohoto zákona není dotčena platnost veřejnoprávních smluv uzavřených přede dnem nabytí účinnosti tohoto zákona podle zákona č. 181/2014 Sb., ve znění pozdějších předpisů.	
803. Kabinet ministra pro legislativu (vláda)	D	K § 72 § 72 Zrušovací ustanovení Zrušují se: ~~1.Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).~~ ~~2.Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti.~~ ~~3.Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.~~ ~~4.Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.~~ ~~5.Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.~~ ~~6.Vyhláška č. XX/XXXX Sb., o bezpečnostních pravidlech pro využívání služeb cloud computingu orgány veřejné moci.~~ 1.Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). 2.Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. 3.Vyhláška č. 205/2016 Sb., kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících	Akceptováno Připomínkové místo s vypořádáním souhlasí.

	kritériích. 4.Část druhá zákona č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony. 5.Část dvě stě dvacátá devátá zákona č. 183/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích. 6.Část první zákona č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony. 7.Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. 8.Část šestá zákona č. 35/2018 Sb., o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny. 9.Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). 10.Část třicátá druhá zákona č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. 11.Část devátá zákona č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů. 12.Vyhláška č. 360/2020 Sb., kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb. 13.Vyhláška č. 573/2020 Sb., kterou se mění vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. 14.Část sto padesátá třetí zákona č. 261/2021 Sb., kterým se mění	

		některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci. 15. Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci. 16. Zákon č. 226/2022 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů. 17. Vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro využívání služeb cloud computingu orgány veřejné moci.	
804. Kabinet ministra pro legislativu (vláda)	D	Obecně Připomínky legislativně-technického charakteru, gramatické a syntaktické - souhrnná připomínka, podrobně viz materiál KML	Akceptováno částečně Některé z navrhovaných revizí a úprav byly akceptovány. Připomínkové místo s vypořádáním souhlasí.
805. Asociace provozovatelů mobilních sítí	D	Omezení rozsahu regulace na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni Jak uvedl NÚKIB, Mechanismus se má vztahovat pouze na tu nejkritičtější část strategické infrastruktury. NÚKIB však ve svém návrhu vymezil rozsah Mechanismu formou vyhlášky o nepominutelných funkcích, která pro oblast telekomunikací obsahuje jak ty nejkritičtější části sítě, jako je jádro sítě, tak i v obecné rovině méně kritické části sítě, jako je rádiová přístupová síť nebo aktiva, které nemají přímý vliv na nedostupnost regulovaných služeb, jako je fakturační systém. V návrhu zákona také zcela chybí odůvodnění, proč jsou kritické části stanoveného rozsahu aktiv definovány tak široce. V našem návrhu jsme kritické části strategické infrastruktury transparentně rozdělili dle hrozeb a míry dopadu jejich realizace. Nejvýznamnější hrozbou je výpadek regulované služby. Rozsah	Vysvětleno Co se týče zmínky v důvodové zprávě o šíři aktiv, tak zde je nutno dodat, že daná připomínka směřuje primárně na nepominutelné funkce stanoveného rozsahu, kde bude mít vyhláška o těchto nepominutelných funkcích vlastní důvodovou zprávu a bude součástí následujícího legislativního balíčku. V rámci tohoto nadcházejícího balíčku dojde k dalšímu mezirezortnímu připomínkovému řízení. Již nyní je však možno říct, že rozsah nepominutelných funkcí cílí na ty nejkritičtější funkce v rámci veřejných komunikačních sítí, přičemž tato kritičnost není závislá na umístění funkcí v rámci topologie sítě. Řešeny jsou tedy jak funkce jádra, tak také například funkce rádiové přístupové sítě, pokud jsou tyto kritické pro zajištění funkčnosti sítě. To je dáno také tím, že bez určitých funkcí rádiové přístupové sítě nemůže dojít k propojení koncového zařízení s jádrem sítě, včetně IZS. Nutno dodat, že tyto

		Mechanismu jsme tak omezili na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro oblast telekomunikací se bude jednat zejména o jádro sítě, případně části přenosové sítě. Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je tedy vhodné, aby byla dána možnost státu okamžitým zásahem zakázat vybraného dodavatele, u kterého identifikuje významnou hrozbu. Pro zbylé části aktiv strategicky významné služby, které nemohou ze své podstaty způsobit nedostupnost služby na kritické úrovni, je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika, která v rámci opatření obecné povahy identifikoval NÚKIB. NÚKIB by jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by nově byla upravena zvlášť v bezpečnostní dokumentaci, kterou by poskytovatel strategicky významné služby měl povinnost každoročně aktualizovat. Tento systém jsme nazvali kaskádou bezpečnostních povinností, kdy pro tu nejkritičtější část strategické infrastruktury bude povinnost řídit se případným zákazem uvedeným v opatření obecné povahy, a pro ty méně kritické části strategické infrastruktury bude nově dána povinnost zohlednit rizika identifikovaná státem a implementovat odpovídající bezpečnostní opatření.	nepominutelné funkce musí být chráněny, přičemž neporušují dosavadní princip analýzy rizik jednotlivých povinných osob. Tato analýza rizik a nepominutelné funkce jsou si navzájem komplementární. Připomínka vypořádána.
806. Asociace provozovatelů mobilních sítí	D	Zapojení vlády a sektorového regulátora do Mechanismu a) Zapojení vlády Zákazem či omezením plnění dodavatele dochází k významnému zásahu do svobody podnikání mnoha subjektů na trhu. Zákaz i	Neakceptováno Ad a) NÚKIB si je vědom, že případný zákaz či omezení plnění dodavatele může zapříčinit zásah do svobody

		omezení plnění dodavatele může mít významné ekonomické, ale i geopolitické dopady. Obdobné dopady již stát v minulosti hodnotil v rámci právní úpravy prověřování zahraničních investic. V rámci procesu prověřování zahraničních investic dochází obdobně jako v případě Mechanismu k prověřování osoby investora na základě strategických kritérií. Stejně jako v případě Mechanismu může také dojít k zákazu investice. V případě prověřování zahraničních investic je zákaz investice podmíněn usnesením vlády. Stejně by tomu tak mělo být i v případě Mechanismu, zejména s ohledem na skutečnost, že plošný zákaz či omezení plnění dodavatele může mít mnohem větší dopad na trh než zákaz doposud neuskutečněné investice. b) Zapojení sektorového regulátora Respektujeme, že v rámci posouzení rizikovosti dodavatele bude mít hlavní roli NÚKIB společně s vládou. V rámci určení lhůty pro implementaci případného zákazu je však role sektorového regulátora klíčová. Případný zákaz totiž může mít významný dopad na schopnost povinných osob plnit své zákonné povinnosti vyplývající ze zvláštních právních předpisů. V případě telekomunikací jsou to například výstavbové povinnosti vyplývající ze zákona o elektronických komunikacích. Je tedy naprosto zásadní, aby daný sektorový regulátor, v tomto případě ČTÚ, měl možnost se k implementaci zákazu vyjádřit a NÚKIB musel k jeho stanovisku přihlédnout.	podnikání mnoha subjektů na trhu. Jak uvádíte v připomínce, zákaz nebo omezení plnění dodavatele může mít významné ekonomické, ale i geopolitické dopady. Z toho důvodu je do rozhodovacího procesu o opatření obecné povahy zapojena Bezpečnostní rada státu, jejíž členové jsou pro posuzování bezpečnostních otázek, včetně těch kyberbezpečnostních relevantní z hlediska posouzení rizikovosti z mnoha úhlů pohledu. Ad b) Dle navrhované úpravy NÚKIB v rámci získávání informací spolupracuje s relevantními orgány státu, přičemž v případě jednotlivých sektorů pak zákon v podobě, jaké je dnes, tuto spolupráci předpokládá s regulátory jednotlivých sektorů, je-li to pro daný případ možné. Toto je zaručeno mimo jiné § 8 odst. 2 zákona č. 500/2004 Sb., správního řádu. Dále je tento postup dán principem dobré správy, kdy NÚKIB pro co nejlepší vyhodnocení situace a možných dopadů počítá s dožádáním informací od relevantních orgánů státu v rámci jednotlivých odvětví. Důvodem, proč jsou v navrhovaném zákoně popsány orgány, které jsou obsaženy v § 30, je ten, že tyto fungují napříč jednotlivými sektory a jejich spolupráce je tak pro správné posouzení rizik, včetně vyhodnocení pro případné omezení či zákaz, žádoucí. Připomínka vypořádána.
807. Asociace provozovatelů mobilních sítí	D	Kompenzace Navrhuje se zakotvení možnosti náhrady škody, a to obdobně, jak je tomu např. v zákoně č. 289/2005 Sb., o vojenském zpravodajství	Neakceptováno Zákon, spolu s prováděcími předpisy, považujeme za ústavně konformní, kvůli čemuž není důvod přidávat ustanovení o náhradě škod. Vzhledem k charakteru

	(„zákon o vojenském zpravodajství“), v němž je přiznána náhrada škody každému, komu škoda nebo nemajetková újma vznikla v souvislosti s činností Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu. Náhrada škody je upravena ve vložném ustanovení § 30a předkládaného návrhu, podle nějž má poskytovatel strategicky významné služby vůči státu nárok na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností z opatření obecné povahy. Náhrada škody dle předmětného ustanovení je koncipována jako náhrada za nemožnost používání technologie po plnou dobu jejího životního cyklu a konkrétní výše je určována znalcem, a to na základě účetních odpisů, s tím, že by byla určena na základě rozdílu mezi délkou životního cyklu plnění dodavatele a lhůty stanovené Úřadem pro omezení či odstranění plnění dodavatele. Metoda určení výše náhrady škody dle odpisů se použije právě a jen pro případy náhrady za nemožnost používání dlouhodobého majetku v plném rozsahu. Pokud by tedy např. Úřad stanovil lhůtu pro odstranění plnění dodavatele v délce 3 roky a životní cyklus plnění dodavatele (technologie) by byl dle účetních odpisů 5 let, mohl by poskytovatel strategicky významné služby požadovat náhradu škody odpovídající 2 zbývajícím rokům odpisů. Pro náhradu dalších účelně vynaložených nákladů vzniklých v důsledku plnění povinností uvedených v opatření obecné povahy se metoda odpisů z povahy věci nevyužije. Pro zajištění větší právní jistoty státu je maximální doba odpisů omezena na 7 let, aby nedocházelo k umělému protahování odpisů. Pokud bude rozsah regulace nastaven tak, jak je uvedeno v tomto návrhu, lze říci, že kompenzace např. v oblasti telekomunikací nebudou reálně žádné. Ustanovení je však nastaveno tak, že pokud by škoda způsobena byla (například v jiných dotčených sektorech), nebo	navrhované právní úpravy, převážně v oblasti mechanismu bezpečnosti dodavatelského řetězce, která se snaží vyjít vstříc povinným osobám například v otázkách životních cyklů technologií nebo zamezení možné závislosti na jedné technologii skrz systém výjimek, není nutné, aby možnost kompenzací byla upravena přímo v zákoně. Kompenzací se v obdobných případech lze domáhat na základě již existujících zákonných prostředků, které předmětným ustanovením § 31 nejsou jakkoliv dotčeny. Nutno dodat, že pro vydání omezení či zákazu formou opatření obecné povahy budou posuzovány veškeré okolnosti a reálné dopady na trh a podnikatelské prostředí. Z toho důvodu by NÚKIB posuzoval jak životnost jednotlivých technologií, tak například možnosti jednotlivých povinných subjektů či postavení dodavatele na českém trhu apod. Připomínka vypořádána.

		by došlo k novelizaci zákona a rozšíření rozsahu regulace, existovala by zde zákonná možnost nárokovat náhradu škody.	
808. Asociace provozovatelů mobilních sítí	D	K § 28 návrhu nového ZKB: - je navržena <u>úprava kritické části stanoveného rozsahu aktiv</u> tak, aby se jednalo pouze o aktiva ohodnocená povinnými subjekty na <u>úrovni kritická, jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby</u> - o rozsah mechanismu jsme definovali na základě hrozeb a důsledku jejich případné realizace. Jako nejvýznamnější hrozbu jsme označili nedostupnost strategicky významné služby. -> zákaz dodavatele pro aktiva, jejichž výpadek může způsobit nedostupnost strategicky významné služby je tedy s ohledem na princip proporcionality <u>přiměřený</u> - o pro oblast telekomunikací jde v zásadě o vztahení mechanismu pouze na části sítě zvané: „jádro sítě“ a části „přenosové sítě“. Úprava je formulována obecněji, aby se vztahovala na všechny oblasti, nejen telekomunikace Prověrování rizik spojených s dodavatelem § 28 1. Úřad shromažďuje a vyhodnocuje informace a data spojené s orgánem či osobou, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovitosti dodavatele. 2. Činnosti podle odstavce 1 prioritizuje Úřad podle přístupu založeného na rizicích a dostupných kapacitách.	Neakceptováno NÚKIB považuje dané ustanovení v současné podobě za důležité, vzhledem k zabezpečení strategicky významných služeb. Obzvlášť důležitá je vyhláška o nepominutelných funkcích tak, jak je nyní nastavena. Tu je nutno považovat za kritickou z toho důvodu, že cílí na vše, co je v rámci fungování veřejných komunikačních sítí kritické, a to bez ohledu na umístění daných funkcí v rámci architektury sítě. To znamená, že z pohledu kybernetické bezpečnosti je jednak kritická funkčnost jádra sítě, jednak také vybrané funkce ostatních částí sítě, jako jsou kupříkladu vybrané funkce v rádiové přístupové síti, bez nichž by jádro sítě nemohlo být propojeno s koncovými zařízeními, čímž by mohlo dojít k znefunkčnění takové sítě. Vzhledem ke komplexitě telekomunikačních sítí, ale také vysoké úrovni zpracování architektur těchto sítí na poli mezinárodních standardizačních organizací, má právě toto odvětví vlastní vyhlášku. V případě kompromitace nepominutelných funkcí může být narušeno či porušeno nejen poskytování služeb koncovým uživatelům, ale také dalších strategicky významných služeb, které jsou na telekomunikačních sítích závislé. NÚKIB tedy skutečně cílí na to, co je pro fungování ICT infrastruktury strategicky významných služeb kritické, včetně všech funkcí uvedených ve vyhlášce o nepominutelných funkcích. Obdobný způsob určení nepominutelných funkcí zvolilo také Finsko, Německo či Velká Británie. Co se týče ochrany rádiové přístupové sítě, tak ta je mimo

		3. Pro potřeby mechanismu prověřování bezpečnosti <u>dodavatelského řetězce se rozumí</u> a. <u>kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovni kritická, a jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby,</u> b. bezpečnostně významnou dodávkou plnění směřující do kritické části stanoveného rozsahu spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu 1. technického prostředku nebo vybavení s výpočetní kapacitou, 2. programového prostředku nebo vybavení, nebo 3. informační či komunikační služby, c. dodavatelem bezpečnostně významné dodávky ten, kdo poskytovateli strategicky významné služby poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku.	jiné chráněna například v Dánsku, Lotyšsku, Švédsku, Finsku, ale také například v Belgii. Připomínka vypořádána.
809. Asociace provozovatelů mobilních sítí	D	K § 30 návrhu nového ZKB: - Nad rámec výše uvedeného jsme zavedli tzv. kaskádu bezpečnostních opatření, kdy v případě vydání opatření obecné povahy (OOP) je pro poskytovatele strategicky významné služby zakotvena nově povinnost provést <u>analýzu rizik</u> pro aktiva strategicky významné služby, která nezařadil do kritické části stanoveného rozsahu (tj. pro	Neakceptováno – nyní § 31 K návrhu na doplnění povinnosti provedení analýzy rizik V opatření obecné povahy lze kromě zákazu využití dodavatele uložit také povinnost, vč. povinností doplňujících řízení rizik, které jinak poskytovatelé strategicky významných služeb budou muset plnit již dle vyhlášky o bezpečnostních opatřeních

		zbývající aktiva, která nejsou na úrovni kritická) – § 30 odst. 9-10 ○ v rámci analýzy rizik musí povinná osoba zohlednit rizika, která NÚKIB uvedl v OOP ○ na základě analýzy rizik poskytovatel vypracuje plán zvládání rizik, jehož součástí jsou i bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v OOP ○ tento plán musí pravidelně aktualizovat ○ NÚKIB tedy může zakázat dodavatele v kritické části stanoveného rozsahu (kde hrozí nedostupnost strategicky významné služby na kritické úrovni). Pro zbytek aktiv vznikne povinným osobám automaticky povinnost provést analýzu rizik uvedených v OOP a vypracovat strategii zvládání rizik včetně implementace odpovídajících bezpečnostních opatření - do procesu posuzování dodavatele je <u>nově zapojen(a)</u>: ○ <u>vláda</u> (obdobně je tomu v zákoně o prověřování zahraničních investic) – § 30 odst. 1-4 ○ <u>sektorový regulátor</u> – § 30 odst. 5-6 ▪ poskytuje konzultaci a stanovisko k tématice lhůty omezení či zákazu plnění dodavatele a možnosti ohrožení plnění povinností dle zvláštního právního předpisu → NÚKIB musí stanovisko zohlednit § 30 Omezení rizik spojených s dodavatelem 1. <u>Zjistí-li Úřad na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České</u>	poskytovatele regulované služby v režimu vyšších povinností, která je v podobě tezí součástí připomínkováného legislativního materiálu. Další doplnění povinností v tomto ohledu nepovažujeme za přiměřené. K návrhu na doplnění sektorového regulátora Dle navrhované úpravy NÚKIB v rámci získávání informací spolupracuje s relevantními orgány státu, a to i s regulátory jednotlivých sektorů, je-li to pro daný případ vhodné a potřebné. Takový postup předpokládá jak předmětná navrhovaná právní úprava, tak pak obecná úprava postupu správních orgánů, např. v § 8 odst. 2 zákona č. 500/2004 Sb, správního řádu. Tento postup je rovněž dán principem dobré správy, kdy NÚKIB pro co nejlepší vyhodnocení situace a možných dopadů počítá s dožádáním informací od relevantních orgánů státu v rámci jednotlivých odvětví. Opakování této obecné povinnosti Úřadu proto nepovažujeme za potřebné ani za vhodné. K návrhu na zapojení vlády Co se týče zapojení vlády, byla do procesu zapojena Bezpečnostní rada státu, ve které jsou členové vlády zastoupeni. Jedná se o bezpečnostní orgán, který zastupuje bezpečnostní zájmy státu. V případě potřeby může samozřejmě problém eskalovat až na vládní úroveň. S tím také souvisí procesní stránka věci, kdy Bezpečnostní rada státu může návrh opatření obecné povahy v případě, že je jí předložen, neprojednat, přerušit jeho projednávání, vrátit jej k přepracování, případně s ním vyjádřit nesouhlas. Jakékoliv rozhodnutí je pro Úřad samozřejmě závazné. Předmětné ustanovení bylo nicméně v návaznosti na připomínky k němu dále rozpracováno a upraveno.

		republiky nebo vnitřního či veřejného pořádku, předloží věc k projednání Vládě České republiky (dále jen “Vláda”). Před předložením věci Vládě je Úřad povinen vyhotovit odhad nákladů povinných osob spojených se zavedením omezení či zákazu plnění dodavatele, který je nedílnou součástí dokumentace předkládané Vládě. Poskytovatel strategicky významné služby je povinen na výzvu poskytnout Úřadu potřebnou součinnost. 3. Vláda přijme do 45 dnů ode dne, kdy jí byla věc předložena k projednání, usnesení o tom, zda plnění dodavatele může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Při posuzování věci Vláda zohlední soulad případného plnění dodavatele s principy demokratického právního státu, dopad na ochranu života a zdraví obyvatel, obranu státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku. 4. V návaznosti na usnesení vlády, že plnění dodavatele představuje významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, vydá Úřad opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu. 5. Usnesení vlády je pro Úřad závazné a vydání opatření obecné povahy omezující či zakazující plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu je vydáním usnesení vlády podmíněno. 6. Zakáže-li nebo omezí-li Úřad opatřením obecné povahy dle odstavce 3 plnění dodavatele, určí zároveň v opatření obecné	Připomínka vypořádána.

		<u>povahy přiměřenou lhůtu zákazu nebo zohlednění podmínek plnění dodavatele. Lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy stanoví Úřad s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby. Úřad vždy musí lhůtu předem konzultovat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele.</u> 7. <u>Před vydáním opatření obecné povahy je Úřad povinen projednat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele, zda návrh opatření obecné povahy a jeho možné dopady neohrozí plnění povinností stanovených a vyplývajících ze zvláštních právních předpisů. Úřad je povinen při vydání opatření obecné povahy stanovisko ústředního orgánu státní správy zohlednit.</u> 8. <u>Jestliže zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle odstavce 3 může ohrozit poskytování strategicky významné služby anebo představuje bezprostřední hrozbu kybernetického bezpečnostního incidentu, který podstatným způsobem ohrožuje poskytování strategicky významné služby, je poskytovatel strategicky významné služby povinen plnit opatření obecné povahy až po pominutí takové hrozby.</u> 9. Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu opatření obecné povahy podávali připomínky. Lhůta pro podání připomínek činí 30 dnů, nestanoví-li Úřad jinak. Ustanovení § 172 odst. 1 a 5, § 173 odst. 1 věty první, část věty za středníkem, a § 173	

		odst. 1 věty druhé správního řádu se pro postup podle tohoto ustanovení nepoužijí. 10. <u>V případě vydání opatření obecné povahy odstavce 3 musí poskytovatel strategicky významné služby provést analýzu rizik spojených s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3 pro aktiva strategicky významné služby, která nezařadil do kritické části stanoveného rozsahu podle § 28 odst. 3 písm. a).</u> 11. <u>Na základě analýzy rizik vypracuje poskytovatel strategicky významné služby plán zvládání rizik dle odstavce 9, v němž uvede bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3. Plán zvládání rizik je poskytovatel strategicky významné služby povinen aktualizovat alespoň jednou za kalendářní rok.</u> 12. Úřad přezkoumá alespoň jednou za 3 roky trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 3. Zjistí-li Úřad, že tyto skutečnosti pominuly, opatření obecné povahy zruší	
810. Asociace provozovatelů mobilních sítí	D	K § 30a návrhu nového ZKB: - v § 30a je nově zakotvena možnost náhrady škody - o poskytovatel strategicky významné služby má vůči státu právo na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností z OOP - o náhrada škody je určována znalcem, a to na základě účetních odpisů - o maximální doba odpisů je omezena na 7 let, aby nedocházelo k umělému protahování odpisů	Neakceptováno – nyní § 31 Zákon, včetně prováděcích předpisů, považujeme za ústavně konformní. Na tomto základě NÚKIB neshledává důvod přidávat zvláštní ustanovení o náhradě škody. Vzhledem k charakteru navrhované právní úpravy, převážně v oblasti mechanismu bezpečnosti dodavatelského řetězce, která se snaží vyjít vstříc povinným osobám například v otázkách životních cyklů technologií či zamezení možné závislosti na jedné technologii skrz systém výjimek, není nutné, aby možnost náhrady škod byla upravena přímo v zákoně. Náhrady, tedy kompenzace, se v

		○ v případě zachování znění § 28 nevznikne operátorům škoda, kterou by nárokovali po státu §30a Náhrada účelně vynaložených nákladů 1. <u>V případě, že lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle §30 odstavce 3 je kratší, než životní cyklus bezpečnostně významné dodávky, nejdéle však 7 let, má každý poskytovatel strategicky významné služby vůči státu právo na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností podle § 30 odstavce 3, a to včetně nákladů na náhradu dlouhodobého majetku, který poskytovatel strategicky významné služby v důsledku opatření obecné povahy podle § 30 odstavce 3 nemůže dále využívat. Výši účelně vynaložených nákladů podle věty první určí Úřad na základě znaleckého posudku, pro jehož vyhotovení poskytne poskytovatel strategicky významné služby součinnost.</u> 2. <u>Životní cyklus bezpečnostně relevantní dodávky bude znalcem určen na základě účetních odpisů zařízení.</u> 3. <u>Zrušením opatření obecné povahy podle § 30 odstavce 11 nezaniká právo na náhradu nákladů podle tohoto ustanovení. Ve věci náhrady nákladů podle tohoto ustanovení jménem státu jedná Úřad.</u>	obdobných případech lze domáhat na základě již existujících zákonných prostředků, které předmětným ustanovením § 30 nejsou jakkoliv dotčeny. Nutno dodat, že pro vydání omezení či zákazu formou opatření obecné povahy budou posuzovány všechny okolnosti a reálné dopady na trh a podnikatelské prostředí. Z toho důvodu by NÚKIB posuzoval jak životnost jednotlivých technologií, tak například možnosti jednotlivých povinných subjektů nebo kupříkladu postavení dodavatele na českém trhu. Připomínka vypořádána.
811. Asociace provozovatelů mobilních sítí	D	K § 31 návrhu nového ZKB: - navrhuje se doplnění odstavce č. 5, v němž je zakotveno, že všechny informace týkající řízení o udělení výjimky a obsahu vydaného rozhodnutí Úřadu o povolení výjimky jsou	Akceptováno jinak Již nyní se informace týkající se řízení o povolení výjimky a samotného rozhodnutí považují za informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti podle § 38 nZKB. Zároveň se tyto informace uchovávají mimo

		považovány za informace, jejichž zpřístupnění může ohrozit zajišťování kybernetické bezpečnosti - na doplněné ustanovení navazuje ustanovení § 37 návrhu nového ZKB ve znění předloženém NÚKIB, v němž jsou upraveny výjimky z práva na informace, a na jehož základě se podle právních předpisů upravujících svobodný přístup k informacím neposkytují informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost protiopatření vydaného podle ZKB § 31 Výjimky z omezení rizik spojených s dodavatelem (1) Úřad může, pokud to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku připouští, povolit výjimku z podmínek či zákazu stanovených opatření obecné povahy podle § 30, jestliže by plnění opatření obecné povahy poskytovatelem strategicky významné služby mohlo podstatným způsobem ohrozit poskytování strategicky významné služby. (2) Řízení o povolení výjimky podle odstavce 1 lze zahájit na žádost poskytovatele strategicky významné služby nebo z moci úřední. Žadatel je povinen v rámci žádosti připojit důkazy prokazující skutečnosti, kterých se dovolává. (3) Úřad v rozhodnutí o povolení výjimky stanoví podmínky jejího uplatnění. V případě závažného porušení podmínek pro uplatnění výjimky nebo v případě pominutí důvodu, pro který byla povolena, Úřad výjimku rozhodnutím zruší. (4) Úřad výjimku nepovolí, pokud by to zcela zmařilo účel opatření obecné povahy podle § 30. (5) <u>Veškeré informace týkající se rozhodnutí o povolení výjimky a řízení o povolení výjimky jsou považovány za</u>	spis dle § 66 nZKB. Z těchto důvodů neakceptujeme navrhovanou úpravu, protože by byla nadbytečná. Pro zvýšení jistoty žadatelů, že se k jejich důvěrným informacím nedostanou třetí osoby, došlo k úpravě důvodové zprávy v následujícím znění: „Informace týkající se řízení o povolení výjimky se považují za informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti.“. Připomínka vypořádána.

		<u>informace, jejichž zpřístupnění může ohrozit zajišťování kybernetické bezpečnosti.</u>	
812. Asociace provozovatelů mobilních sítí	D	K § 34 návrhu nového ZKB: - nově vloženo ustanovení (nový odstavec 2) deklarující speciální úpravu zajištění dostupnosti strategicky významné služby ve vymezených oblastech elektronických komunikací - o cílem je zamezení možných dezinterpretací a výkladových nejasností problematiky zajištění dostupnosti strategicky významných služeb pro oblast telekomunikací § 34 Zajištění dostupnosti strategicky významné služby (1) Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky. (2) <u>Poskytovatel strategicky významné služby v odvětví 16.1 Poskytování veřejně dostupní služby elektronických komunikací a 16.2. Zajišťování veřejně dostupné komunikační sítě elektronických komunikací podle přílohy k vyhlášce o regulovaných službách je povinen v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky zajistit dostupnost strategicky významné služby spočívající v</u> a) <u>poskytování veřejně dostupné mobilní služby elektronických komunikací,</u> b) <u>zajišťování veřejné mobilní komunikační sítě elektronických komunikací,</u>	Akceptováno jinak - nyní § 35 Připomínkové ustanovení § 35 bylo v odst. 1 upraveno tím způsobem, že „Poskytovatel strategicky významné služby je povinen zajistit její dostupnost v nezbytném rozsahu, ve stanoveném čase a kvalitě z území České republiky.“ Tento nezbytný rozsah bude stanoven vyhláškou Úřadu. V této vyhlášce rovněž bude blíže rozvedeno, co se v telekomunikačním sektoru rozumí nezbytným rozsahem při zajištění dostupnosti těchto služeb z území ČR. Připomínka vypořádána.

		c) <u>poskytování veřejně dostupné služby elektronických komunikací v pevném místě.</u> (3) Poskytovatel strategicky významné služby je povinen testovat schopnost zajištění poskytování strategicky významné služby v rozsahu kritické části stanoveného rozsahu z území České republiky nejméně jednou za dva roky. (4) Poskytovatel strategicky významné služby začne plnit povinnosti uvedené v odst. 1 a 2 pro každou strategicky významnou službu nejpozději do jednoho roku ode dne doručení vyrozumění o zápisu strategicky významné služby do evidence poskytovatelů regulovaných služeb nebo od doručení rozhodnutí o určení strategicky významné služby podle § 27 odst. 2. (5) Stanovený čas a kvalitu služby stanoví poskytovatel regulované služby v závislosti na cílech řízení kontinuity činností podle prováděcího právní předpisu. (6) Pro potřeby tohoto ustanovení je kritická část stanoveného rozsahu vymezena v § 28 odst. 3 písm. a).	
813. hSOC a CESNET	Z	K § 2 odst. 1 písm. b) Doporučujeme změnit definici primárního aktiva následovně: „primárním aktivem jsou data, informace, služby a procesy“ Data a informace jsou rozdílné pojmy. Stejně tak jsou rozdílnými pojmy služby a procesy. Data v sobě mohou a nemusí nést část informace. Současně informace bude vždy složena z dat. Informace jsou vnímány jako něco „kvalifikovanějšího“, nežli data. Data jsou fakta, která se stávají informacemi tehdy, pokud jsou vnímána či vyjádřena v kontextu a nesou význam, který je pochopitelný pro lidi. Pokud tedy chcete jako primární aktivum označit i data, pak nelze dát	Akceptováno jinak Definice byla upravena tak, aby nepůsobila zmatečně. Definice primárního aktiva byla dána do původní podoby. Pro účely tohoto zákona se rozumí: primárním aktivem informace a služby. Připomínka vypořádána.

		rovnítko mezi pojem informace a data. Služby nejsou totéž, co procesy. Pokud chcete vymezit procesy jako primární aktivum, bylo by vhodnější uvést definici ve které procesy přímo označíte za primární aktivum. Je zřejmé, že je využívána terminologie jak ze zák. 181/2014 Sb., tak i z norem ISO 27000. Nicméně uvedení že: „službou se rozumí také procesy“ může být v praxi mnohem více matoucí a zavádějící. Výslovné uvedení procesů a dat, jakožto samostatných primárních aktiv by tak mělo vést k posílení právní jistoty adresátů.	
814. hSOC a CESNET	Z	K § 2 odst. 1 písm. b) Doporučujeme vypouštění slov: „včetně provozních údajů“ Jako primární aktivum jsou nově určeny i provozní údaje. Vlastní pojem může být vykládán značně různorodě. Může se jednat o data spadající např. pod § 97 odst. 4 zák. č. 127/2005 Sb., o elektronických komunikacích, ale také se může jednat např. o údaje v podobě „data sheetu“, na kterém budou zaznamenány údaje o provozu či o metadata ze systémů. Byť jsou provozní údaje v současném zákoně č. 181/2014 Sb., uvedeny v § 6a a § 15a, tak se vztahují toliko ke KII či KKI. U § 15a je to o vyžádání dat k incidentu. Dle návrhu zákona se ale bude tato povinnost (tj. určit provozní údaje jako primární aktivum) nově vztahovat na všechny regulované subjekty (jak v režimu vyšších, tak nižších povinností) a zejména na všechny jimi spravované služby, systémy aj. Provozní údaje jsou stále data. Evidovat data či provozní údaje bez kontextu jako samostatná primární aktiva nemá smysl a půjde o zbytečné a neúčelné zatížení povinného subjektu. Domníváme se, že je na povinném subjektu, aby vyhodnotil, která data a provozní údaje bude identifikovat a hodnotit jako aktiva.	Akceptováno Připomínka vypořádána.

815. hSOC a CESNET	Z	K § 2 odst. 1 písm. c) Doporučujeme vypouštění slov: „technickým aktivem technické a programové prostředky a vybavení, kdy technickým a programovým prostředkem a vybavením se rozumí také komunikační prostředky, sítě elektronických komunikací a průmyslová, řídicí nebo jiná obdobná specifická aktiva.“ V zákoně dochází k uvedení některých technických aktiv. Domníváme se, že by zákon měl být dostatečně srozumitelný, ale na druhou stranu dostatečně obecný a neomezující vývoj ICT. Z tohoto důvodu se domníváme, že je vhodné odstranit uváděný demonstrativní výčet. Byť se jedná o demonstrativní výčet, tak právě jeho uvedení nemusí posílit právní jistotu adresátů a jednoznačně stanovit, že tato aktiva spadají do kategorie podpůrných aktiv. Dle našeho názoru je vhodnější: -Mít v zákoně uvedenu obecnou definici -V případě nejasností v praxi vymezit, co se rozumí technickým aktivem např. metodickým výkladem NÚKIB aj.	Akceptováno jinak Stávající definice neomezuje vývoj ICT a Úřad se domnívá, že výčtem byla naopak zajištěna vyšší míra právní jistoty, nicméně Akceptováno jinak – Úprava, nové znění: "technickým aktivem technické a programové prostředky a vybavení, a to včetně průmyslových, řídicích nebo jiných obdobných specifických aktiv". Byl odstraněn demonstrativní výčet, kdy současně byla zachována část, kterou povinné osoby často opomíjí při identifikaci technických aktiv, na které se vztahují bezpečnostní opatření vyhlášek, potažmo ZKB. Dle Úřadu, nově navrhované znění tak nad rámec velice obecné definice konkretizuje, že OT je součástí technických aktiv, což posiluje právní jistotu. Připomínka vypořádána.
816. hSOC a CESNET	Z	K § 2 odst. 2 písm. a) Změna definice: „kybernetickým prostorem digitální prostředí tvořené aktivity umožňující vznik, výměnu a další zpracování informací a dat,“ Pokud má být vytvořen soulad s dalšími právními předpisy (EU a ČR), zejm. (EU) 679/2016, pak pojmy: „vznik, výměna a další“ jsou nadbytečné, protože jsou již obsaženy v pojmu „zpracování“. Z hlediska větší právní jistoty je tedy vhodnější využít toliko pojem zpracování.	Akceptováno Připomínka vypořádána.
817. hSOC a CESNET	D	K § 2 odst. 2 písm. b) Doplnění definice: bezpečností informací zajištění dostupnosti, důvěrnosti, integrity a autentičnosti informací a dat. Původní triáda CIA je v současné době ne zcela dostačující.	Neakceptováno Nahrazení CIA modelu jiným konceptem je na NÚKIB pravidelně diskutovaná otázka a prozatím jsme vždy došli k závěru, že je stávající pojetí dostatečné. Zákon o kybernetické bezpečnosti má

		Navrhovaná definice obsahující „dostupnost, důvěrnost a integritu dat“ nepokrývá identifikaci, autentizaci, autorizaci jako metody zajišťující základní kontroly přístupu, stejně jako některé další služby související s digitálním podpisem. Vysvětlení: Autenticita - originalita - prokazatelnost místa, času nebo zdroje původu informací. Specificky je chráněna i autentičnost (tj. pravost, původnost) dat. (EU) 2022/2555 explicitně tuto oblast zmiňuje. Uvědomujeme si, že tato problematika byla uvedena již v NIS1, nicméně v současné době, zejména s výrazným rozmachem neuronových sítí (typu ChatGPT, AzureOpenAI aj.) bude na místě se zaměřit právě na problematiku autentičnosti tj. pravosti/původnosti dat a informací. Současně je s autentičností spojena i hrozba spočívající v záměně dat, informací či identity. Doporučujeme rozšířit znění zákona či prováděcí vyhlášky	sloužit jako univerzální předpis řešící kybernetickou bezpečnost různých druhů služeb, které reguluje. Navrhované doplnění se v převážné míře váže na oblast digitálních podpisů nebo obecně služeb vytvářejících důvěru a upravuje trochu jinou otázku, než která je předmětem úpravy kybernetické bezpečnosti v navrhovaném zákoně. Legislativa, která odvětví služeb vytvářejících důvěru reguluje, však i nadále zůstává v platnosti (pouze část kybernetické bezpečnosti je nově přenesena do zákona o kybernetické bezpečnosti), problematiku jdoucí nad rámec zákona o kybernetické bezpečnosti tedy budou i nadále řešit k tomu příslušné předpisy a příslušní regulátoři. Pojem bezpečnost informací se netýká obsahu informace, ale pouze funkčnosti prostředí, v němž je informace tvořena, zpracována, uchovávána a komunikována. Narušením autenticity obsahu informace ovšem zároveň dochází k narušení integrity tohoto funkčního prostředí. Autenticita informace je tedy pro potřeby zákona o kybernetické bezpečnosti chápána jako součást integrity. Připomínka vypořádána.
818. hSOC a CESNET	Z	K § 2 odst. 2 písm. d) Vymezit konkrétněji, co je myšleno pod závažným ovlivněním aktiva poskytovatele nebo uživatelů. V kontextu upřesnění pojmu „významný dopad“ považujeme za potřebné i upřesnění pojmu „závažného ovlivnění aktiva poskytovatele nebo uživatelů.“	Neakceptováno Významné hrozby jsou v zákoně definovány pro potřeby informační povinnosti poskytovatele regulované služby, který má informovat své uživatele o způsobech eliminace dopadů realizace hrozby nebo o hrozbě samotné. Toto informování se však bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek, zejména ve vztahu k uživatelům. Závažné ovlivnění bude v různých situacích a v kontextu různých poskytovatelů regulovaných služeb

		Přestože bylo odůvodněno v předchozím vypořádání, že dopad pojmu „závažné ovlivnění“ bude záležet na konkrétní situaci, problematická může být interpretační praxe a rozdílnost aplikací, a to zvláště při sektorové rozsáhlosti a rozdílnosti poskytovatelů regulovaných služeb. Vzhledem k unikátnímu využití pojmu (a tomu, že je s ním pracováno de facto jen zde) by ještě stálo za úvahu zavést alespoň na úrovni podzákonného předpisu demonstrativní indikaci relevantních určujících znaků či situací	vykládáno různě. Odvětví od odvětví a poskytovatel od poskytovatele bude vliv na aktiva a újma, kterou je hrozba schopna způsobit, posuzována různě. Z toho důvodu se Úřadu nejeví jako vhodné definici významné hrozby blíže rozvádět (taková definice by pořád musela být dostatečně obecná, aby byla univerzálně aplikovatelná na všechny regulované subjekty, a tedy by ani v jiné formě nemohla přinést žádné významné zpřesnění). Máme za to, že v kombinaci s podmínkou značné újmy, kterou významná hrozba musí být schopna způsobit, by mělo být adresátům normy jasné, jakým způsobem mají u sebe v organizaci stanovit hranici pro určení významnosti hrozby. Způsob stanovení této hranice by měl být zanesen v bezpečnostních politikách a bezpečnostní dokumentaci regulované osoby. Pokud pak bude hranice významnosti hrozby stanovena smysluplně a s ohledem na specifika a potřeby organizace a jejích zákazníků, Úřad nemá důvod nastavené metriky rozporovat. Připomínka vypořádána.
819. hSOC a CESNET	Z	K § 2 odst. 2 písm. e) Změna definice: kybernetickou bezpečnostní událostí událost, která může způsobit kybernetický bezpečnostní incident mohla narušit dostupnost, integritu nebo důvěrnost aktiv, ale plnému vzniku takové události bylo úspěšně zabráněno nebo taková událost nenastala odst. 5 směrnice NIS 2 a lépe vystihuje podstatu „kybernetické bezpečnostní události“. „Událost“ by měla být definována jako situace, která nastala nebo se předpokládá, že nastala. Tento předpoklad existuje, protože existuje přímá nebo nepřímá indicie, že událost nastala. Takováto definice dle našeho názoru lépe a pochopitelněji reflektuje	Akceptováno jinak Definice byla změněna na „událost, která může nebo mohla vyústit v kybernetický bezpečnostní incident“. S pojmem „kybernetická bezpečnostní událost“ pracuje současný ZKB, zároveň Úřad rozlišuje i pojem „významná kybernetická bezpečnostní událost“, který odpovídá definici „významná událost“ (near miss) podle NIS2. Významná událost je chápána jako podmnožina události. Událost má potenciál způsobit narušení bezpečnosti aktiv. U významné události nedošlo ke vzniku škody díky tomu, že zafungovala zavedená bezpečnostní opatření. Jedná se tedy o rozdíl

		podstatu kybernetické bezpečnostní události (i z časového hlediska – „mohla“, nikoliv „může“), je stále v souladu se stávající definicí kybernetického bezpečnostního incidentu a inkorporuje prvky významné události dle čl. 6 odst. 5 směrnice NIS 2, kterou zákon jinak nepřejímá.	v tom, zda událost v incident vyústí, či nikoliv. Přičemž Vládnímu CERT mohou být hlášeny všechny události a jejich klasifikace na významné pro potřeby sdílení informací mezi relevantními subjekty podle NIS2 probíhá na interní úrovni. Připomínka vypořádána.
820. hSOC a CESNET	Z	K § 2 odst. 2 písm. g) Změna definice: zvládáním kybernetického bezpečnostního incidentu úkony vedoucí k zajištění prevence, detekce, analýzy, omezení dopadů incidentu, reakce na incident a ~~následného zotavení~~ nápravným opatřením , Uvedení pojmu „zotavení“ není vhodné. Po incidentu nemusí nutně dojít k zotavení, ale je třeba přijmout nápravná opatření, která mohou být různého charakteru . V praxi mnohdy nemusí záměrně dojít k zotavení napadeného systému, naopak incident a jeho řešení může vést k záměrnému odstavení zranitelných systémů. Tyto úkony lze považovat za nápravná opatření, nikoli však za zotavení.	Akceptováno jinak Zotavení může v praxi představovat nejen obnovu, ale i zrušení systému (např. zapomenuté služby na které se incident stal), nebo náhradu HW. Zavedení opatření vedoucích k tomu, aby se incident znovu nestal (tedy Vámi zmiňovaná nápravná opatření) jsou součástí reakce na incident. Samotný pojem „nápravná opatření“ je v rámci zákona vyhrazen pro rozhodnutí Úřadu podle § 59. Na základě připomínky došlo k nahrazení termínu „zotavení“ pojmem „obnova“. Připomínka vypořádána.
821. hSOC a CESNET	Z	K § 2 Doplnění pojmu: „významný dopad“. Zákon na řadě míst pracuje s pojmem významný dopad, jakožto ze skutečností, která má vztah k obecné regulaci subjektů spadajících do působnosti ZKB. Tento je do určité míry vymezen jen ve vztahu k poskytovateli v režimu nižších povinností (viz § 16 odst. 3). Ale s pojmem významný dopad je pracováno i ve vztahu k poskytovateli v režimu vyšších povinností, kde však jakýkoliv rámec toho, co je považováno za významný dopad chybí. Je zřejmé, že pro každého poskytovatele může významný dopad představovat jinou situaci . Navrhujeme uvést, že významný dopad a jeho hodnocení je uvedeno v jednotlivých vyhláškách vztahujících se k poskytovatelům	Akceptováno jinak Přístup k výkladu neurčitých právních pojmů použitých v návrhu zákona byl doplněn do důvodové zprávy v tom smyslu, že jejich obecná definice není právě s ohledem na jejich charakteristiku coby neurčitých právních pojmů a současně univerzální aplikovatelnost na skutkově zcela odlišné situace žádoucí (nadto např. pojem významný dopad je v rámci zákona používán pro různé situace a v závislosti na místě jeho použití nabývá v jednotlivých částech zákona odlišných významů). Jakákoli definice, o kterou by se předkladatel návrhu zákona pokusil, by z povahy věci musela poměrně obecná (aby pokryla

		regulovaných služeb. Aplikovatelným kritériem by mohla být například finanční ztráta regulovaného subjektu v důsledku incidentu či riziko finanční újmy vyjádřené v procentech (např. 0,5 % ročního obrátu).	všechny zamýšlené situace) a nepřinášela by adresátům normy žádnou přidanou hodnotu. Tam, kde je to možné a vhodné, jsou pojmy buďto vysvětleny v prováděcích předpisech, nebo jsou blíže přiblíženy v důvodové zprávě. Bližší výklad těchto pojmů pak bude prováděn v závislosti na konkrétních skutkových okolnostech posuzovaného případu. Obecně však tyto pojmy slouží k vydefinování situací, které dosahují natolik významné intenzity, že stát považuje za nezbytné je podřadit pod zákonnou regulaci. Připomínka vypořádána.
822. hSOC a CESNET	Z	K § 2 Doplnění pojmu CERT. Navrhované znění: „CERT je tým, který je v jasné definovaném poli působnosti zodpovědný za řešení kybernetických bezpečnostních incidentů a reakcí na kybernetické hrozby. Jedná se o tým zajišťující řešení a koordinaci činností souvisejících s kybernetickým bezpečnostním incidentem vedoucích k jeho zvládnutí.“ V zákoně je s pojmem CERT pracováno jako s notoriitou, nicméně roli bezpečnostního/reakčního týmu běžně plní týmy typu CERT/CSIRT. V profesním vnímání jsou zkratky CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team) vnímány „synonymně“, rozhodně se o synonymum nejedná. Rozdíl je jednak v licencování značky CERT u Carnegie Mellon Univerzity a jednak i v drobném rozdílu: Emergency Response a Security Incident Response. Doporučujeme umožnit výkon týmu CERT i jiným akreditovaným týmům CSIRT (viz https://www.trusted-introducer.org/index.html). Národní bezpečnostní tým využívá označení CSIRT, přičemž fakticky vykonává úkony požadované po CERT	Akceptováno jinak Na základě Vaší připomínky došlo k doplnění definice Národního a Vládního CERT a zavedení legislativní zkratky: „národní/vládní tým koordinace a zvládání kybernetických bezpečnostních incidentů, událostí a hrozeb (dále jen „Národní/Vládní CERT“)“ v § 16 odst. 2 a 5. Podrobnější výčet činností obou týmů je rozveden v příslušných ustanoveních. Připomínka vypořádána.

823. hSOC a CESNET	Z	K § 14 odst. 3 Prodloužení lhůty. Navrhovaný časový rámec je pro nově regulované subjekty velice krátký. V subjektech, kde nejsou definována aktiva vůbec může proces zmapování primárních aktiv trvat dlouho, zvláště v organizacích, kde není management organizace seznámen s procesem identifikace aktiv a zároveň se jedná buď o alokaci finančních prostředků na externího dodavatele, který zajistí patřičné činnosti nebo na zajištění interních lidských zdrojů. Taktéž může být problematické, či nereálné v tomto krátkém časovém období získat potřebné lidské zdroje, či realokovat finanční prostředky určené na jinou činnost organizace. Doporučujeme minimálně nově regulované subjekty či pro subjekty v režimu nižších povinností tuto lhůtu prodloužit na 24 měsíců.	Neakceptováno Subjekty budou zjišťovat naplnění identifikačních kritérií regulovaných služeb, na základě čehož budou provádět registraci daných služeb. Teprve od doručení vyrozumění o zápisu do evidence regulovaných služeb začnou subjektům běžet lhůty pro plnění povinností vůči daným službám. Pro zavádění bezpečnostních opatření se tak jedná o lhůtu 12 měsíců. Se stejnou délkou přitom rovněž pracuje současná právní úprava. Regulované subjekty pak mají další nástroje, jak s nově nabytými povinnostmi pracovat. Jedná se například o plán zvládání rizik, který subjektům umožňuje postupné zavádění bezpečnostních opatření. Dle našeho názoru je proto lhůta přiměřená. Připomínka vypořádána.
824. hSOC a CESNET	Z	K § 15 odst. 1 písm. b) bod 2 Změna definice: ~~„bezpečnost komunikačních sítí technických aktiv“~~ Případně: ~~„bezpečnost informačních a komunikačních systémů“~~ V rámci technických opatření uvedených v zákoně není nikde uvedena ochrana informačních systémů (počítače, servery aj.). Domníváme se, že je třeba mít v zákoně uveden pojem obecný, nadřazený a tento by pak měl být blíže specifikován v prováděcích předpisech. S ohledem na vymezení základních pojmů v § 2 odst. 1 písm. c) je jako vhodný nadřazený pojem jeví „technické aktivum“, nicméně uvádíme i možnou alternativu.	Neakceptováno V rámci zavádění bezpečnostních opatření jsou obecně nad technickými aktivy zaváděna veškerá technická opatření dle § 15 odst. 1 písm. b) nZKB. Požadavky v oblasti „bezpečnost komunikačních sítí“ dle § 15 odst. 1 písm. b) bod 2 nZKB jsou pouze podmnožinou technických opatření, které cílí na zavádění bezpečnostní opatření nad komunikačními sítěmi a jejich komunikací (např. sítíovou infrastrukturou) nad užší podmnožinou technických aktiv. Zatímco jiná technická opatření v § 15 odst. 1 písm. b) nZKB cílí na jiné oblasti zabezpečení v rámci technických aktiv, jako např. i na Vámi uvedené počítače a servery. Jednotlivá bezpečnostní opatření, včetně těch technických, jsou již náležitě rozvedena v dílčích prováděcích předpisech, jak navrhuje.

			Přípomínka vypořádána.
825. hSOC a CESNET	Z	K § 17 odst. 1 Změna lhůty 24 hodin pro předložení hlášení o kybernetickém bezpečnostním incidentu. <u>Poskytovatel regulované služby bez zbytečného odkladu po zjištění kybernetického bezpečnostního incidentu, nejpozději však do 24 72 hodin předloží Úřadu nebo Národnímu CERT prvotní hlášení, v němž uvede, zda se domnívá, že byl kybernetický bezpečnostní incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad.</u> Úprava, která stanovuje lhůtu 24 hodin na nahlášení informací týkajících se každého kybernetického bezpečnostního incidentu [tj. dle §2 odst. 2 písm. f) – každé „narušení bezpečnosti informací v rámci aktiv“]. Tato úprava zásadně podstatně mění současnou právní úpravu a mnohdy nebude reálně proveditelná. Proces hlášení kybernetických bezpečnostních incidentů je sice upraven směrnicí NIS2, ale lhůta 24 hodin se dle čl. 23 odst. 4 písm. a) směrnice NIS2 vztahuje pouze k zjištění významného incidentu. Dle čl. 23 odst. 1 je významným incidentem takový „každý incident, který má významný dopad na poskytování jejich služeb“. Dle této dikce se tedy rozhodně nejedná o každý kybernetický bezpečnostní incident, ale pouze o takový, který má významný dopad na poskytování služeb regulovaného subjektu. Česká právní úprava v tomto případně významně, a ne zcela odůvodněně rozšiřuje povinnost hlásit všechny kybernetické bezpečnostní incidenty ve velmi krátké a mnohdy nesplnitelné lhůtě. Doporučujeme vypustit limitaci lhůtou 24 hodin na prvotní hlášení, případně alespoň tuto lhůtu prodloužit a stanovit ji obdobně jako tomu je např. u GDPR (resp. § 41 odst. 2 zák. 110/2019 Sb., o zpracování osobních údajů) na 72 hodin.	Neakceptováno. Lhůta pro hlášení incidentů ve stávající právní úpravě je stanovena na „bezodkladně“ po detekci incidentu. Takto stanovená lhůta má zajistit případnou rychlou reakci Vládního CERT, příp. Národního CERT při řešení incidentu a napomoci navazujícím preventivním či analytickým aktivitám těchto týmů. Obsahové náležitosti prvotního hlášení jsou omezeny na nezbytné minimum, díky kterému bude vládní CERT schopen posoudit, zda má incident významný dopad na kybernetický prostor státu. Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnicí NIS2, tzn. pokud bychom do zákona nezahrnuli požadavek na lhůtu, která je podle čl. 23 odst. 4 písm. a) NIS2 stanovena na „bez zbytečného odkladu, nejpozději však do 24 hodin po zjištění“, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Z uvedeného důvodu národní právní úprava tento požadavek kopíruje. Poskytovatelé regulované služby v režimu nižších povinností hlásí pouze kybernetické bezpečnostní incidenty s významným dopadem, poskytovatelé regulované služby ve vyšším režimu hlásí všechny kybernetické bezpečnostní incidenty. Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto

			subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob. Připomínka vypořádána.
826. hSOC a CESNET	D	K § 17 odst. 1 Navrhujeme pojem „prvotní“ vypustit či nahradit vhodnějším synonymem. „Poskytovatel regulované služby bez zbytečného odkladu po zjištění kybernetického bezpečnostního incidentu, nejpozději však do 24 hodin předloží Úřadu nebo Národnímu CERT prvotní hlášení, v němž uvede, zda se domnívá, že byl kybernetický bezpečnostní incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad.“ Užití pojmu „prvotní“ může evokovat, že se jedná o jakýsi draft – doporučujeme slovo „prvotní“ vypustit či nahradit vhodnějším synonymem.	Neakceptováno Směrnice NIS2 pro tuto fázi hlášení používá pojem „včasné varování“ (early warning), který indikuje předložení prvotního draftu obsahujícího pouze nezbytně nutné informace jako příp. přeshraniční dopad a informaci, zda byl incident způsoben svévolným nebo nezákonným zásahem. V ZKB je pojem "varování" vyhrazen pro jiný institut, proto bylo ve vztahu k hlášení incidentů přistoupeno k pojmu vystihujícímu důraz na skutečnost, že je hlášení rozděleno do více fází. Připomínka vypořádána.
827. hSOC a CESNET	Z	K § 17 odst. 4 Nemožnost nahlášení kybernetických bezpečnostních incidentů včetně dobrovolných hlášení jiným způsobem. Veškeré hlášení je vztaženo toliko k elektronické komunikaci. Absolutně není počítáno s výpadkem těchto služeb na straně toho, kdo má povinnost hlásit, avšak z objektivních důvodů (např. právě významné zasažení kybernetickým bezpečnostním incidentem), toto není schopen tímto způsobem učinit (např. mu nefunguje IT infrastruktura). Současně je v § 58 odst. 1 písm. h) uvedeno, že pokud tak povinný subjekt neučiní, dopustí se přestupku.	Neakceptováno Máme za to, že poslat prvotní hlášení prostřednictvím elektronické pošty lze i bez funkční infrastruktury regulované organizace. Kontaktní osoba to může učinit klidně ze svého mobilního telefonu, jde především o to, aby CERT mohl na tuto situaci bezprostředně reagovat. Pokud by došlo k nahlášení prostřednictvím neelektronických prostředků, např. standardní poštou, hrozí poměrně velké průtahy v řešení incidentu. Variantou je zachování pohotovostní telefonické linky, nicméně při počtu regulovaných

		Domníváme se, že by bylo vhodné definovat i jinou možnou „krizovou“ komunikaci v případě hlášení incidentu než jen tu uvedenou v § 17 odst. 4 a současně by mělo dojít k úpravě § 59 odst. 2, kde by v takovýchto případech měl být posuzován i materiální znak přestupku, tj. jeho škodlivost.	subjektů není možné zajistit dostatečnou dostupnost takové linky, navíc by šlo těžko dodržet obsahové náležitosti hlášení. Připomínka vypořádána.
828. hSOC a CESNET	Z	K § 19 odst. 1 Navrhujeme rozšíření pravomocí uvedených v tomto odstavci o pozdržení zveřejnění, např. následovně: „Úřad je oprávněn uložit poskytovateli regulované služby, který je dotčen kybernetickým bezpečnostním incidentem s významným dopadem, povinnost informovat uživatele regulované služby o tomto incidentu. Úřad je dále oprávněn uložit poskytovateli regulované služby, který ví o významné kybernetické hrozbě, zranitelnosti či je dotčen kybernetickým bezpečnostním incidentem s významným dopadem, povinnost zveřejnění daných informací pozdržet v případech, ve kterých by vedlo k ohrožení dalších poskytovatelů regulovaných služeb. V rozhodnutí o uložení této povinnosti stanoví Úřad rozsah informační povinnosti či informačního embarga“ Tento návrh je motivován zavedením systémů koordinovaného zveřejňování zranitelností směrnicí NIS 2. Zveřejněné informace o významných hrozbách, zranitelnostech postihujících více poskytovatelů regulovaných služeb, či incidentech s významným dopadem mohou občas citelně ohrozit další regulované subjekty v momentech, kdy neměly dostatečný čas se na danou výzvu připravit (zveřejnění se může de facto stát návodem pro méně informované či schopné hackery). V takových případech může být vhodné zavést dočasné informační embargo.	Neakceptováno - nyní § 20 Rozsah informační povinnosti je v NIS2 vztažen pouze na incidenty (čl. 23 odst. 1) a hrozby (čl. 23 odst. 2). Informování o proběhlých incidentech je přednostně ponecháno v dispozici zasaženého subjektu, který, na rozdíl od Úřadu, má o incidentu podrobný přehled a sám nejlépe posoudí, zda je vhodné a žádoucí o něm informovat (v krajních případech mu tuto povinnost může uložit Úřad). Informace o hrozbách mohou obsahovat skutečnosti, které ve výsledku přispívají k příp. odvrácení incidentů u dalších subjektů, a nemají potenciál tyto subjekty ohrozit. Úřad na základě svých zkušeností nepovažuje neinformování o incidentech a hrozbách za vhodné, naopak podporuje sdílení a předávání těchto informací. Zranitelnosti jsou právě z důvodů souvisejících s CVD z informační povinnosti vyňaty. CVD bude řešeno na jiné než zákonné úrovni, a to v souladu s požadavky NIS2 uvedenými v čl. 12. Připomínka vypořádána.
829. hSOC a CESNET	Z	K § 23 odst. 6 Nejasné fungování institutu připomínek k opatření obecné povahy v případě vyloučení § 172 správního řádu. Zákon sice vylučuje v § 23 odst. 5 použití § 172 správního řádu, ale v	Neakceptováno – nyní § 24 Zákon o kybernetické bezpečnosti ani v současné podobě neobsahuje jiný, než v současnosti navrhovaný proces vydávání reaktivního protipatření

		odst. 6 nedostatečně nahrazuje fungování institutu připomínek a souvisejících záruk transparentnosti výkonu státní správy, doporučujeme tedy výslovně uvést, že se NÚKIB musí připomínkami zabývat a vypořádat je v odůvodnění opatření obecné povahy (analogicky k § 172 odst. 4 správního řádu).	(dříve reaktivního opatření). Účelem reaktivního protiopatření je co nejrychleji a v případech, které nesnesou odkladu reagovat na vyvstálé riziko. Z tohoto důvodu byl jediný přílehlavý nástroj obsažený v rámci správního řádu příslušně upraven a návrhová část celého procesu opatření obecné povahy nebyla zavedena jako součást procesu vydávání reaktivního protiopatření, stejně jako nebyla součástí procesu původního reaktivního opatření. Zavedení navrhovaného by tedy bylo v přímém rozporu s účelem tohoto ustanovení, které je již ověřeným institutem, který byl ze strany Úřadu již několikrát úspěšně použit. Připomínka vypořádána.
830. hSOC a CESNET	Z	K § 28, 32 odst. 1, 58 odst. 3 písm. b), 58 odst. 3 písm. c)., 58 odst. 3 písm. d) Nejasný termín „bezpečnostně významná dodávka“. Z nového návrhu zákona vyplývá povinnost hlásit informace o dodavatelích bezpečnostně významných dodávek a evidovat tyto informace, přičemž nedodržení této povinnosti je přestupkem podle § 58. Pojem „bezpečnostně významné dodávky“ je sice definován v § 28, nicméně stále zůstává velmi vágní, není jasné, co pod takovou dodávku spadá a co nikoliv – není například jasné, jakého rozsahu nebo předmětu musí předmětná dodávka být. Není tedy jasné, který dodavatel spadá pod povinnost hlášení. Navrhujeme proto povinnost hlášení v návrhu vypustit, případně alespoň lépe specifikovat, zejména s ohledem na rozsah, předmět takové dodávky. Ve vztahu k tomuto pojmu není zejména jasné: 1) co vše je považováno za Bezpečnostně významnou dodávku 2) jaká má být úroveň detailu posuzovaného podpůrného aktiva 3) který dodavatel spadá do povinnosti hlášení.	Neakceptováno Pojem bezpečnostně významné dodávky je v návrhu zákona a ve zvláštní části důvodové zprávy k němu rozpracován co nejpodrobněji, jak to jeho povaha umožňuje. Vymezení konkrétních dodávek a jejich dodavatelů vychází z oboru činnosti dotčeného poskytovatele strategicky významné služby a zejména z jeho vlastního hodnocení aktiv dle prováděcího právního předpisu – vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. Pro odstranění případné přílišné tvrdosti zákona, kdy by někteří poskytovatelé služeb vztahovaly do tohoto pojmu výrazně více či méně dodavatelů a poddodavatelů než jiní, slouží korektiv vynaložení přiměřeného úsilí při zjišťování a hlášení dodavatelů a dodávek dle § 33 odst. 1 návrhu zákona. NÚKIB v tomto ohledu rovněž plánuje pokračovat v dosavadní dobré praxi vydávání podpůrných a metodických materiálů, které poskytnou vodítka pro

		Jako vhodné řešení se jeví odkázat na prováděcí předpis, kde bude výše uvedené vysvětleno.	co možná nejjednodušší aplikaci povinností, které s těmito pojmy pracují. Připomínka vypořádána.
831. hSOC a CESNET	Z	K § 32 odst. 1 písm. b) Lhůta pro hlášení 10 dnů je příliš krátká. Není možné pro instituce větší velikosti (např. univerzita) hlásit v takto krátké lhůtě požadované informace o dodavatelích, zvláště pokud by bylo nutné hlásit všechny dodávky, i malého rozsahu. Navrhujeme nahradit lhůtu textem „bez zbytečného odkladu“ nebo významně prodloužit. Zásadní otázkou je, zda je v praxi takové hlášení s ohledem na množství změn a procesy vůbec realizovatelné.	Neakceptováno - nyní § 33 Lhůta 10 dnů je mířena na proces nahlášení informací podle § 33 odst. 1 písm. a) a jejich změn. Nemíří na proces zjišťování těchto informací. Lhůta počne běžet až ve chvíli, kdy poskytovatel strategicky významné služby bude těmito informacemi disponovat. Realita pak bude taková, že poskytovatel strategicky významné služby si v prvním roce po písemném vyrozumění o označení regulované služby jako strategicky významné služby v evidenci regulovaných služeb (zde proběhla změna oproti původnímu návrhu, kdy se přechodná lhůta vázala na účinnost zákona) nastaví procesy a začne zjišťovat požadované informace. Tyto pak bude muset nejpozději po roce a deseti dnech nahlásit NÚKIB. Připomínka vypořádána.
832. hSOC a CESNET	D	K § 40 písm. e) e) zakázat orgánům a osobám, ~~které k tomu byly Úřadem vyzvány,~~ používání technických aktiv v případě, že jsou taková [...]Z navrhovaného textu předpisu není jasné, o jakou výzvu se má jednat. Z důvodu nespecifičnosti tak navrhujeme vypustit.	Akceptováno - nyní § 41 Připomínka vypořádána.
833. hSOC a CESNET	Z	K § 41 odst. 5 Doplnění činnosti: poskytovatelům regulovaných služeb v režimu vyšších povinností poskytuje své vyjádření ke kybernetickému bezpečnostnímu incidentu V ustanovení § 18 odst. 1) je uvedeno: „Úřad nebo Národní CERT	Neakceptováno - nyní § 44 Vyjádření ke kybernetickému bezpečnostnímu incidentu ze strany Vládního CERT je součástí činností souvisejících se zvládáním a koordinací kybernetických bezpečnostních incidentů, které jsou zakotveny v § 44 odst. 5 písm. a) bod 4 navrhovaného

		poskytne bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení podle § 17, poskytovateli regulované služby své vyjádření ke kybernetickému bezpečnostnímu incidentu.“ Tato povinnost však pak není provozovateli stanovena v § 41. Úřad může činit toliko to, co mu zákon umožňuje, a proto se domníváme, že by bylo vhodné předmětné ustanovení doplnit.	znění zákona. Jelikož je zvládání upraveno v § 18, není nutné tuto povinnost znovu zmiňovat. Připomínka vypořádána.
834. hSOC a CESNET	Z	K § 42 odst. 3 písm. c) Doplnění činnosti: poskytovatelům regulovaných služeb v režimu nižších povinností poskytuje své vyjádření ke kybernetickému bezpečnostnímu incidentu, metodickou podporu, pomoc a součinnost při výskytu a zvládání kybernetického bezpečnostního incidentu s významným dopadem a při zveřejňování informací o zranitelnostech v oblasti kybernetické bezpečnosti, V ustanovení § 18 odst. 1) je uvedeno: „Úřad nebo Národní CERT poskytne bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení podle § 17, poskytovateli regulované služby své vyjádření ke kybernetickému bezpečnostnímu incidentu.“ Tato povinnost však pak není provozovateli stanovena v § 42 odst. 3.	Neakceptováno - nyní § 45 Vyjádření ke kybernetickému bezpečnostnímu incidentu ze strany Národního CERT je součástí pomoci a součinnosti při výskytu a zvládání incidentu, které jsou zakotveny (a tedy obsaženy) ve Vámi zmiňovaném ustanovení navrhovaného znění zákona. Jelikož je zvládání upraveno v § 18, není nutné tuto povinnost znovu zmiňovat. Připomínka vypořádána.
835. hSOC a CESNET	Z	K § 54 odst. 3 písm. i), 67 odst. 1 Doporučujeme opravit používání zkratk pro řízené služby a poskytovatele řízené služby. Zkratka MSP je zavedena jednou pro řízené služby, podruhé pro poskytovatele řízené služby.	Akceptováno - nyní § 57 a 68 Zkratka byla z § 57 odstraněna, resp. byla změněna celá struktura ustanovení, naopak v § 68 odst. 1 byla ponechána. Připomínka vypořádána.
836. hSOC a CESNET	Z	K § 59 odst. 2 Navrhujeme vypustit daný odstavec. Kromě toho, že se dané ustanovení může jevit jako narušující současné pojetí a použitelnost materiálního korektivu, také je formulováno formou vyvratitelné domněnky a tím pádem fakticky zbytečné.	Akceptováno - nyní § 61 Ustanovení bylo vypuštěno. Připomínka vypořádána.
837. hSC a CESNET	Z	K § 65 odst. 3	Neakceptováno - nyní § 5 odst. 2

		Navrhujeme vypustit z daného odstavce nepřipustnost rozkladu proti rozhodnutí o určení regulované služby podle § 5. Zatímco v případě rozhodnutí o výmazu je nepřipustnost rozkladu pochopitelná, rozhodnutí o určení regulované služby může pro daný subjekt představovat podstatně zásadnější zásah do práv a povinností, mělo by tak být možné proti němu podat rozklad. Institut přezkoumání splnění kritérií regulované služby a relevance zápisu do evidence poskytovatelů nemůže tuto možnost v plném rozsahu a srovnatelné efektivitě nahradit, zejména z pohledu vzniknuvších povinností a včasnosti opravy. Vybancování dotčených zájmů provedené v důvodové zprávě se nám pak jeví jako nedostatečné a nepřesvědčivé.	Důvody pro vyloučení možnosti podat rozklad proti rozhodnutí o určení podle § 5 návrhu zákona jsou vedeny veřejným zájmem na rychlém a efektivním zařazení poskytovatele regulované služby do regulace. Jde o obdobnou situaci jako při určování provozovatelů základní služby podle současného zákona o kybernetické bezpečnosti, u něhož je také vyloučena možnost podat rozklad. Za dobu účinnosti současného zákona a určování provozovatelů základní služby se přitom nestalo, že by subjekt se svým určením nesouhlasil a podal proti rozhodnutí Úřadu žalobu. Vzhledem k zájmům, jejichž ochrana byla určováním provozovatelů základních služeb sledována (zejména národní bezpečnosti a ochrana obyvatelstva), bylo nutné, aby proces určování podle zákona o kybernetické bezpečnosti probíhal, pokud možno, bez výraznějšího zpoždění. Tyto důvody lze v plném rozsahu aplikovat i na určování subjektů podle § 5 návrhu zákona, a to tím spíše, že kritéria § 5 zákona míří na strategické a vysoce důležité služby/subjekty (u nichž by narušením bezpečnosti jejich informačních systémů mohlo dojít k významnému ohrožení veřejné bezpečnosti, zdraví osob nebo majetku nebo jiných chráněných zájmů státu). Ve veřejném zájmu je tak provedení zařazení regulované služby do regulace co nejvíce v souladu se zásadou rychlosti a hospodárnosti, neboť neúměrným a nijak účelným prodlužováním celého procesu může být výše zmíněný zájem, představující účel tohoto návrhu zákona, ohrožen. Do doby registrace a zápisu do evidence regulovaných služeb tyto orgány nebo osoby nejsou odpovědné za zabezpečování svých systémů a hlášení incidentů. Jakékoli prodlužování

			procesu zařazení orgánů nebo osob do regulace návrhu zákona oddaluje okamžik, od kterého jsou tyto orgány a osoby odpovědné za zajišťování kybernetické bezpečnosti své organizace a ochranu poskytované služby.
838. Vodafone	D	K § 5 písmeno d), Kritéria pro určení regulované služby Navrhuje doplnit §5, písmeno d) takto: <u>orgán nebo osoba je subjektem kritické infrastruktury podle právního předpisu upravujícího krizové řízení a kritickou infrastrukturu; v takovém případě je regulovanou službou služba odpovídající prvku kritické infrastruktury určenému u tohoto subjektu v maximálním rozsahu Přílohy k vyhlášce č. [bude doplněno] Sb. Kritéria pro identifikaci regulované služby.</u> Doporučujeme vymežit pouze na rozsah odvětví a služeb, které definuje ZKB. Pokud například směrnice CER rozšíří počet regulovaných subjektů, upozorňuje na možné velké rozšíření počtu povinných osob, odvětví a služeb v rámci tohoto zákona.	Neakceptováno Jsme si tohoto možného velkého rozsahu vědomi a jsme v kontaktu s gestorem této problematiky: Ministerstvem vnitra - Generálním ředitelstvím Hasičského záchranného sboru. Toto ustanovení je navrženo především pro mezidobí před účinností avizované změny krizového zákona a vyžádá si s jeho účinností téměř jistě novelizaci. Tak jako tak ale vstupem bude vždy skutečnost, že pokud stát označuje některé služby/prvky/subjekty za kritickou infrastrukturu, není možné u nich neřešit regulaci kybernetické bezpečnosti - subjekty spadající pod kritickou infrastrukturu jsou naopak těmi prvními, kteří pod ni mají spadat. Smyslem daného ustanovení je také vždy reflektovat ochranu služby/prvků pro kterou je daný subjekt kritickou infrastrukturou - to nejsou vždy ty stejné služby pro které je služba regulována podle zákona o kybernetické bezpečnosti. Připomínka vypořádána.
839. Vodafone	D	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností §9 Řízení rizik, f) Navrhujeme narovnat definici Prohlášení o aplikovatelnosti (SoA) tak, aby byla v souladu s ISO/IEC 27001, zavedenou praxí a ustáleným významem. změnit	Neakceptováno Samotné vyhlášky nejsou nyní součástí mezirezortního připomínkového řízení, to proběhne samostatně. S Vaším návrhem na úpravu § 9 písm. f) nesouhlasíme, současné znění ve vyhlášce je širší. Máme za to, že bezpečnostní opatření budou

		(...prohlášení o aplikovatelnosti, které obsahuje přehled všech bezpečnostních opatření požadovaných touto vyhláškou, která, i) nebyla aplikována, včetně odůvodnění a přehledu přijatých náhradních bezpečnostních opatření, ii) byla aplikována, včetně způsobu plnění) na (...prohlášení o aplikovatelnosti, které obsahuje přehled všech bezpečnostních opatření požadovaných touto vyhláškou, která, i) jsou aplikovatelná včetně odůvodnění jejich aplikovatelnosti a zda jsou nebo nejsou zavedena ii) jsou neaplikovatelná včetně zdůvodnění jejich neaplikovatelnosti) SoA je pojítkem mezi výsledky hodnocení rizik a plánem zvládání rizik. SoA by mělo obsahovat všechna opatření, která jsou nezbytná k ošetření rizik v oblasti bezpečnosti informací. Přičemž by neměla být opomenuta žádná aplikovatelná opatření uvedená ve vyhlášce. Zároveň však mohou být zavedena opatření nad rámec těch uvedených ve vyhlášce. Nezavedená opatření jsou pak předmětem plánu zvládání rizik (RTP), kde je také uvedena informace o stavu jejich implementace.	aplikovatelná; je zásadní, zda je povinná osoba fakticky realizuje či nikoliv. Navíc by vypadla potřeba identifikace bezpečnostních opatření, která jsou aplikovatelná, nejsou ale aplikována, přičemž v budoucnu aplikována budou. Stejně tak by vypadla kategorie přehledu přijatých náhradních opatření, která má svůj praktický účel dán. Samotná vyhláška však nikomu nebrání, aby SoA Vámi navrhovanou diferenciaci opatření zavedla. Z našeho pohledu zvolený způsob úpravy požadavků na PoA si neodporuje s normou ISO/IEC 27001; požadavek na proces dokumentování PoA v současné podobě neshledáváme jako neefektivní nebo potřebný v současné fázi příprav vyhlášek měnit. Připomínka vypořádána.
840. Vodafone	D	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností §10 Řízení dodavatelů Navrhujeme do §10 doplnit odstavec upravující možný způsob kontroly plnění bezpečnostních opatření u významných dodavatelů v režimu vyšší regulace v rámci uzavíraných smluvních vztahů (odst. 2 písm. b) a v rámci poskytovaných plnění (odst. 2 písm. c). (3) Pokud se jedná o smluvní vztah mezi povinnou osobou a významným dodavatelem, který je poskytovatelem regulované	Vysvětleno Jak bylo uvedeno u předchozí připomínky, samotné vyhlášky nejsou nyní součástí mezirezortního připomínkového řízení, to proběhne samostatně. Váš dotaz pravděpodobně směřuje na požadavek k provádění například zákaznických auditů k ověření poskytovaných plnění u významných dodavatelů, kteří jsou zároveň poskytovatelem regulované služby, a tedy spadají pod regulaci. Chápeme Vaši úvahu a

		služby ve vyšším režimu povinností a regulovaná služba je předmětem plnění, je dostatečné prohlášení dodavatele o plnění aplikovatelných bezpečnostních opatřeních. Návrh doplnění do důvodové zprávy. <i>Dodavatel nemusí dokládat důkazy, které v rámci kontroly ověřuje Úřad.</i> Zpravidla se jedná o citlivé a klasifikované informace a požadavek na sdílení představuje bezpečnostní riziko pro poskytovatele regulovaných služeb ve vyšším režimu povinností. Zároveň kontrolu plnění povinností, včetně evidence, zajišťuje u těchto poskytovatelů NUKIB. Při počtu 6000 tis. regulovaných subjektů mohou zákaznické audity představovat další administrativní a finanční zátěž pro regulované subjekty.	možnou ekonomii tohoto řešení, ale nelze zákaznický audit dávat na roveň kontrole plnění požadavku u povinné osoby ze strany Úřadu. V případě, kdy jdeme vykonat kontrolu u PRS ve vyšším režimu (případně nižším režimu), který je dodavatelem například Vaší společnosti, budeme na něj pohlížet jako na správce a kontrolovat jeho regulované služby a jakým způsobem plní zákonné povinnosti z pohledu zákona a vyhlášky pro PRS vyšší (případně nižší); neprovádíme kontrolu plnění požadavků vzniklých ze smlouvy mezi Vaší společností a PRS ve vyšším nebo nižším režimu. U smluvních ujednání se jednotlivé požadavky mohou znatelně lišit, mohou být třeba mnohem přísnější než-li požadavky vyhlášky (například Vaše bezpečnostní požadavky do smluv jsou přísnější s ohledem na vlastní bezpečnostní politiku) a dále při řádném řízení rizik spojených s dodavatelem lze vyhodnotit, že některé požadavky do smluv s dodavatelem není nutné aplikovat, například z důvodů slabší vyjednávací pozice, je však nutné tyto skutečnosti v rámci PoA a RTP reflektovat resp. vyhodnotit zda lze akceptovat i jiné bezpečnostní záruky, jako je například provedení zákaznického auditu, zpráva z průběžného auditu v případě, že má společnost ISO certifikaci pro systém řízení informační bezpečnosti, případně doložení čestného prohlášení, zprávu o kontrole procesů řízení incidentů apod. Připomínka vypořádána.
841. O2	Z	<i>Zákon o kybernetické bezpečnosti, § 30 Omezení rizik spojených s dodavatelem</i> Mezi odstavce 1 a 2 vložit nový odstavec 2 ve znění: <i>„2) Opatřením obecné povahy podle odstavce 1 nelze poskytovateli služeb elektronických komunikací stanovit podmínky</i>	Neakceptováno Ve vztahu k poskytovatelům sítí či službám elektronických komunikací NÚKIB považuje za nutné chránit veškeré funkce veřejné komunikační sítě, které jsou považovány za kritické. Tyto kritické funkce

	<i>nebo zakázat využití plnění dodavatele bezpečnostně významné dodávky v přístupové nebo transportní části sítě elektronických komunikací.“</i> V současném znění dopadají opatření obecné povahy podle § 30 (dále jen „OOP“) vůči provozovatelům služeb elektronických komunikací nejen na jádro jimi provozovaných sítí elektronických komunikací, ale také na jejich transportní a přístupové části. Pokud by měl být zachován současný mechanismus OOP, který umožňuje vydat zákaz či podmínky využití bez ohledu na životní cyklus dotčených plnění (srov. níže), považujeme takový zásah do práva na svobodu podnikání za nepřiměřený vůči naplňování účelu ustanovení – zajištění kybernetické bezpečnosti kritických prvků informační infrastruktury, kdy důvěrnost, integritu a dostupnost přenášovaných a zpracovávaných dat mohou relevantně ohrozit pouze bezpečnostně významné dodávky do jádra sítě, nikoli do přístupové nebo transportní části sítě. Takto intenzivní zásah lze shledat přiměřeným a odůvodnitelným pouze vůči skutečně nejkritičtější částem sítě elektronických komunikací, tedy jádru sítě, nikoli vůči jejím ostatním částem. Navrhovaná změna proto směřuje k omezení možného dopadu OOP pouze na jádro sítě. <u>Regulaci na úrovni transportní a přístupové části sítí nepovažujeme za adekvátní, jelikož takto vynucená výměna technologií by nikterak nezvyšovala odolnost a zabezpečení sítí (resp. nesnižovala riziko výpadku sítí v důsledku jejich napadení hackery nebo neposkytnutí podpory dodavatele), protože žádná technologie na světě není odolná na 100,00%. Zároveň deklarujeme, že v případě vzniku mimořádných situací máme plány zajištění provozuschopnosti sítí a jsme schopni provozovat síť elektronických komunikací po dobu minimálně dvou let i bez případné aktivní součinnosti s našimi technologickými dodavateli. V případě vzniku této situace by zároveň byl spuštěn migrační plán k jiným technologickým dodavatelům tak, aby byl zajištěn kontinuální a bezvýpadkový provoz všech sítí.</u>	nemusí být nutně vztaženy pouze na jádro sítě, jelikož mnohdy zabezpečují a udržují chod poskytování služeb koncovým uživatelům, a to zejména v rámci rádiové přístupové sítě. Například řízení či monitorovací funkce rádiových stanic představují prostředek, pomocí kterého se koncoví uživatelé připojují právě ke službám poskytovaným jádrem sítě. V případě jejich kompromitace tak může být narušeno či zcela porušeno poskytování služeb koncovým uživatelům. Je pravdou, že jádro sítě je nejvýznamnější z hlediska bezpečnosti a integrity sítě a dostupnosti poskytovaných služeb, ale bez zabezpečené rádiové přístupové sítě pozbývá funkční jádro smysl, jelikož nemůže dojít k propojení koncových zařízení s jádrem, což souvisí s nemožností zajistit dostupnost. Obdobný přístup ke kritičnosti sítí, nehledě na jejich umístění v rámci architektury sítě, zvolilo také Dánsko, dále pak v rámci EU Belgie či Finsko. Kritické části sítě jsou omezeny rozsahem zahrnutých aktiv a rozsahem bezpečnostně významných dodávek. Připomínka vypořádána.

		Rovněž z mezinárodního srovnání v zemích EU vyplývá, že většina zemí nepřistoupila k žádné regulaci anebo jen k regulaci na úrovni jádra sítě. K regulaci na úrovni transportní a přístupové části sítě přistoupilo jen několik zemí z celé EU. Alternativní cestou k omezení nepřiměřených dopadů na poskytovatele strategicky významných služeb je zavedení lhůty zohledňující životní cyklus dotčených plnění, a tedy šetřící hospodářská práva povinných osob, jak navrhuje níže.	
842. O2	Z	<i>Zákon o kybernetické bezpečnosti, § 30 Omezení rizik spojených s dodavatelem</i> Doplnit do odst. 1 poslední věty za slovo „služby“ slova: „a délce životního cyklu dotčených plnění.“ Mezi odstavce 1 a 2 vložit nové odstavce 2 a 3 ve znění: „2) <i>Lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle odstavce 1 nesmí být kratší než 7 let, vyjma případů naléhavého mimořádného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku.</i> 3) <i>Jestliže by zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle odstavce 1 představovalo bezprostřední hrozbu kybernetického bezpečnostního incidentu, který by mohl podstatným způsobem ohrozit poskytování regulované služby, je poskytovatel strategicky významné služby povinen plnit opatření obecné povahy až po pominutí takové hrozby.</i>“ V odstavci 4 (odst. 2 před vložením nových odst. 2 a 3) písm. a) bod 2. a písm. b) bod 2. nahradit slova „5 let“ za „7 let“. Doplnit za odst. 6 (4) nový odstavec 7 (5) ve znění: „7) <i>V případě stanovení kratší lhůty pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle odstavce 2 má každý poskytovatel strategicky významné služby vůči státu právo na náhradu účelně vynaložených nákladů, které mu vznikly v důsledku plnění povinností podle odstavce 1 včetně nákladů na náhradu</i>	Neakceptováno Hranice lhůty je v návrhu stanovena jako pětiletá, což vychází z přílohy zákona upravujícího daňové předpisy. Tato lhůta zohledňuje v dostatečné míře zájmy státu na straně jedné a zájmy poskytovatelů strategicky významných služeb na straně druhé. Současně s tím mechanismus umožňuje v případě nutnosti „uhnout“ na obě strany, tedy pokud je to nutné, lhůtu zkrátit a pokud je to možné, nastavit lhůtu delší. Navrhovaná právní úprava je ve své současné podobě ústavně konformní, kvůli čemuž není důvod přidávat ustanovení o náhradě škod. Vzhledem k charakteru navrhované právní úpravy, převážně v oblasti mechanismu bezpečnosti dodavatelského řetězce, která se snaží vyjít vstříc povinným osobám například v otázkách životních cyklů technologií nebo zamezení možné závislosti na jedné technologii skrz systém výjimek, není nutné, aby možnost kompenzací byla upravena přímo v zákoně; přirozeně tím však nejsou dotčena např. práva na náhradu škody či kompenzace podle jiných právních předpisů. Připomínka vypořádána.

	<i>dlouhodobého majetku, který poskytovatel strategicky významné služby v důsledku opatření obecné povahy podle odstavce 1 nemůže dále využívat. Výši účelně vynaložených nákladů podle věty první určí Úřad na základě znaleckého posudku, pro jehož vyhotovení poskytne poskytovatel strategicky významné služby součinnost. Zrušením opatření obecné povahy podle odstavce 6 nezaniká právo na náhradu nákladů podle tohoto odstavce. Ve věci náhrady nákladů podle tohoto odstavce jménem státu jedná Úřad.“</i> OOP má potenciál velmi závažně zasáhnout do hospodaření poskytovatelů strategicky významných služeb. Při současném znění není Úřad jakkoli omezen v dispozici s tímto nástrojem a povinné osoby na rozdíl od Úřadu, který při posuzování dodavatelů mimo jiné využívá informace zpravodajských služeb, nejsou schopny vydání OOP dostatečně jasně předvídat, natož možnému vydání přizpůsobovat své podnikatelské plány. Navrhovaná změna má za cíl zamezit nepřiměřeným hospodářským ztrátám povinných osob za současného zachování možnosti efektivně zabezpečit kyberprostor České republiky. Zákaz budoucího využití dodavatele pro bezpečnostně významné dodávky v kritické části stanoveného rozsahu je dle našeho názoru adekvátním krokem k zajištění kybernetické bezpečnosti a náklady povinných osob spočívajících v omezení výběru dodavatelů lze ve většině případů považovat za přiměřené opatření. Problém ovšem vyvstává při aplikaci zákazu na již využívaná plnění rizikového dodavatele, kdy by dle současného znění mohl Úřad povinné osoby donutit okamžitě vyměnit klíčové části jejich infrastruktury nezávisle na tom, v jaké části svého životního cyklu se v době vydání OOP nacházejí. V takovém případě by povinným osobám vznikaly náklady, které by mohly být v naprosto nepřiměřené míře ohrožení chráněného zájmu. Z toho důvodu navrhuje zavést dostatečně dlouhou lhůtu, která by umožnila již	

	uskutečněným plněním dokončit jejich životní cyklus, čímž dojde k snížení vzniku zbytečných nákladů za současného zachování účelu OOP. <u>Délka lhůty by z povahy jejího účelu měla být posuzována individuálně s ohledem na druh omezovaného plnění, ale zásadně nesmí překročit minimální délku. Minimální délka 7 let byla stanovena s ohledem na analýzu životnosti technologických prvků v pevné a mobilní síti elektronických komunikací, kdy je u celé řady prvků technologická životnost delší než je navrhovaných 7 let. Zároveň je však nutné zákonem stanovit pevnou časovou hranici, od které se budou anebo nebudou odvíjet případné finanční kompenzace za regulačně vynucenou předčasnou výměnu technologií.</u> S tím právě souvisí návrh zavést výjimku, která v případě mimořádně významného a naléhavého ohrožení dává státu prostor ke zkrácení této sedmileté lhůty, avšak za podmínky náhrady nákladů, které povinné osoby budou muset vynaložit ke splnění OOP. Finanční odpovědností státu za zkrácení sedmileté lhůty by mělo být zajištěno využívání tohoto institutu pouze ve skutečně odůvodněných případech. Výše účelně vynaložených nákladů musí být stanovena objektivně, avšak na základě individuálně účelně vynaložených nákladů jednotlivých povinných osob. Ke spravedlivému určení výše náhrady proto nelze dospět pomocí paušální částky stanovené prováděcím předpisem. Z těchto důvodů se navrhuje, aby výše účelně vynaložených nákladů byla určena soudním znalcem pověřeným Úřadem, přičemž povinné osoby budou mít povinnost poskytnout znalci ke stanovení výše náhrady požadovanou součinnost. V některých případech, obzvláště při stanovení kratší lhůty k naplnění povinností podle OOP, nemusí být plnění zákazu nebo podmínek podle OOP bez ohledu na vynaložené prostředky možné, aniž by zároveň došlo k hrozbě kybernetického bezpečnostního	

		incidentu ohrožujícího poskytování regulované služby. Příklad takové hrozby by mohla představovat nemožnost nahradit plnění zakázaného nebo stanovenými podmínkami omezeného dodavatele plněním jiného dodavatele, pokud by například jiní dodavatelé nebyli ve stanovené lhůtě schopni plnění poskytnout. Navrhuje se proto také, aby povinnost plnit OOP byla v takových případech odložena do doby, než bude pro poskytovatele strategicky významné služby reálně možné povinnost naplnit, aniž by tím bylo podstatným způsobem ohroženo poskytování regulované služby.	
843. O2	Z	<i>Zákon o kybernetické bezpečnosti, § 31 Výjimky z omezení rizik spojených s dodavatelem</i> Doplnit odstavce 5 a 6 ve znění: „5) Úřad vede seznam rozhodnutí o povolení výjimky veřejně dostupný na internetových stránkách Úřadu. 6) Seznam podle odstavce 5 obsahuje alespoň a) označení poskytovatele strategicky významné služby, jemuž byla výjimka povolena, b) označení opatření obecné povahy, které bylo výjimkou dotčeno, c) vymezení strategicky významné služby dotčené výjimkou, d) podmínky a rozsah udělené výjimky, odůvodnění rozhodnutí.“ Výjimky z OOP jsou velmi riskantním institutem z pohledu potenciálního ohrožení hospodářské soutěže, neboť udělením výjimky může dojít k významnému zvýhodnění některých soutěžitelů na relativně úzkých trzích.	Neakceptováno - nyní § 31 Povolení výjimky bude vedeno jako standardní správní řízení, ze kterého se informace nezveřejňují (nárok na informace mají pouze osoby, které mají oprávnění nahlížet do správního spisu). Nadto lze poukázat na to, že zveřejnění informací o udělení výjimky v požadovaném rozsahu by mohlo mít přímé dopady na bezpečnost dotčených subjektů, v tomto případě poskytovatelů strategicky významných služeb. Připomínka vypořádána.

		Navrhované zveřejňování udělených výjimek přispívá k transparentnosti celého mechanismu omezování rizik dodavatelského řetězce. Povinné osoby tak budou mít přehled o rozhodovací praxi Úřadu, které se budou moci přizpůsobit, což zvýší míru jejich právní jistoty a umožní jim podávat podněty k zahájení řízení o povolení výjimky, pokud u nich nastane obdobný skutkový stav, který vedl k udělení výjimky jiné povinné osobě. Mimo to bude zajištěna veřejná kontrola rozhodování Úřadu. Alternativou navrhovaného zvýšení transparentnosti může být také zrušení institutu výjimek z OOP jako takových. Úřad by měl mít dostatek prostředků k posouzení dopadů OOP, a tedy i k dostatečně konkrétnímu vymezení jeho rozsahu tak, aby nebylo nutné výjimky udělovat. Vydávání OOP je navíc spojeno s lhůtou pro uplatnění připomínek, která by měla umožnit povinným osobám vyjádřit se k možnému ohrožení poskytování regulované služby.	
844. O2	Z	<i>Zákon o kybernetické bezpečnosti, § 34 Zajištění dostupnosti strategicky významné služby</i> V celém paragrafu nahradit slova „strategicky významné služby“ za „regulované služby“. V odstavci 1 nahradit slova „v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě“ za slova „uvedené v příloze tohoto zákona“. V odstavci 1 za slovo „republiky“ doplnit „v kvalitě uvedené v příloze k tomuto zákonu“. V odstavci 2 za slova „zajištění poskytování strategicky významné služby“ doplnit slova „uvedené v příloze k tomuto zákonu“. V odstavci 2 nahradit slova „kritické části stanoveného rozsahu“ za slova „podle odst. 1“.	Akceptováno jinak - nyní § 35 Připomínkové ustanovení § 35 bylo v odst. 1 upraveno tak, že "Poskytovatel strategicky významné služby je povinen zajistit její dostupnost v nezbytném rozsahu, v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky." Tento nezbytný rozsah bude stanoven vyhláškou o nezbytném rozsahu dostupnosti strategicky významných služeb. V této vyhlášce bude blíže rozvedeno, co se v telekomunikačním sektoru rozumí nezbytným rozsahem při zajištění dostupnosti těchto služeb z území ČR. Připomínka vypořádána.

		V odstavci 3 na konci věty nahradit slova „§ 27 odst. 2“ za slova „§ 5“. Odstavce 4 a 5 vypustit. Doplnit přílohu k zákonu dle přílohy těchto připomínek. Úřad na základě připomínek veřejnosti upustil od požadavků na lokalizaci dat na území České republiky nebo spřátelených států. Zároveň však navrhl nahradit lokalizaci povinností zajistit dostupnost strategicky významných služeb z České republiky, pokud jsou k jejich poskytování využívána zahraniční aktiva. Povinnost má zajistit dostupnost nejkritičtějších služeb pro občany České republiky v případě mimořádných událostí (přírodní katastrofy, pandemie, války atp.), které by mohly omezit možnosti využití zahraničních aktiv, ať už z důvodu faktické vzdálenosti, nebo nemožnosti uplatňovat státní moc na území jiných států. Úřad však prostřednictvím strategicky významných služeb spojil mechanismus zajišťování minimální úrovně dostupnosti s mechanismem prověřování bezpečnosti dodavatelského řetězce (dále jen „BDŘ“), přičemž se jedná o odlišné instituty jak z hlediska cíle právní úpravy, tak z hlediska způsobu jeho dosahování. Účelem stanovení minimální úrovně dostupnosti by mělo být zabezpečení dostupnosti nejkritičtějších služeb na „minimální“ úrovni potřebné k fungování společnosti a státu. Navrhovaná právní úprava se však nesoustředí na stanovení této minimální úrovně, které částečně ponechává na povinných osobách, nýbrž se věnuje konkrétním funkcím technických aktiv stanoveným ve vyhlášce o nepominutelných funkcích stanoveného rozsahu. Ponechává tedy v nejistotě ohledně zabezpečení minimální úrovně dostupnosti jak poskytovatele, tak uživatele regulovaných služeb. Z výše uvedených důvodů se navrhuje oddělení mechanismu BDŘ od stanovování minimální úrovně dostupnosti. Minimální úroveň	

	dostupnosti jednotlivých kritických služeb by měla být určena zákonem, přičemž způsob zajištění její dostupnosti by měl být ponechán na poskytovatelích. Zároveň se navrhuje konkrétní podoba určení minimální úrovně dostupnosti pro sektor telekomunikací, která respektuje přiměřenou úroveň služeb elektronických komunikací v souladu se zákonem č. 127/2005 Sb., o elektronických komunikacích (dále jen „ZEK“). Poskytovatelé a zajišťovatelé veřejně dostupných služeb elektronických komunikací by měli mít povinnost zajistit dostupnost hlasové komunikace v mobilní síti a připojení k internetu v mobilní síti v takovém rozsahu, aby byla při mimořádné situaci umožněna základní komunikace mezi občany a orgány veřejné moci. Úroveň této základní komunikace vychází z pojmů „přiměřený přístup k internetu v pevném místě“ a „přístup k hlasové komunikační službě v pevném místě“ dle § 40 ZEK, které jsou s ohledem na současný stav techniky převedeny do prostředí mobilních sítí. Minimální úroveň by tak měla zabezpečit komunikaci během mimořádné situace, aniž by kladla nadměrné technické nároky na poskytovatele, protože se nepočítá s nutností zajišťovat služby, které vyžadují vysokou rychlost internetového připojení, jako např. streamování videí nebo videohovory. Pokud by měla být zachována povinnost zabezpečit dostupnost regulované služby v celém rozsahu, k čemuž vede stávající podoba návrhu, museli by poskytovatelé služeb elektronických komunikací budovat infrastrukturu výlučně na území České republiky, neboť by nedávalo ekonomický smysl budovat jakoukoli infrastrukturu v zahraničí, pokud by zároveň musela existovat její plnohodnotná „záložní kopie“ v České republice. Taková povinnost by tudíž byla nepřipustným omezením volného trhu v rámci EU.	

845. O2	Z Zákon o kybernetické bezpečnosti, § 28 Prověřování rizik spojených s dodavatelem odst. 3 písm. c) <i>„... dodavatelem bezpečnostně významné dodávky každý, kdo poskytovateli strategicky významné služby poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku.“</i> <i>Ve spojení s § 32 odst. 1 písm. a)</i> <i>„... zjišťovat s vynaložením přiměřeného úsilí informace o dodavatelích bezpečnostně významných dodávek a...“</i> Doplnit úroveň poddodavatelského řetězce, která má být předmětem zjišťování povinné osoby mechanismu prověřování dle § 32 odst. 1 písm. a), nebo způsoby pro její stanovení (např. odkaz na prováděcí právní předpis a zmocnění k jeho vydání). Je třeba blíže specifikovat úroveň dodavatelského řetězce, do které jsou poskytovatelé strategicky významných služeb povinni zjišťovat informace dle § 32 odst. 1 písm. a). V souladu s cílem a účelem předmětné úpravy je přiměřené, aby poskytovatel strategicky významné služby zjišťoval informace nejen o primárním dodavateli, kterým bude často pouze distributor, ale také o přímém výrobcí daného produktu nebo poskytovateli služby ve vztahu, ke kterým je stěžejní prověřit rizikovost. Původní znění však lze vykládat i jako povinnost zjišťovat informace i o dodavatelích jednotlivých komponent daného výrobku (polovodičových prvků) nebo dodavatelích dílčích programových prostředků (licencí), pomocí kterých je poskytována služba přímým dodavatelem. Taková povinnost pro poskytovatele strategicky významných služeb by byla nepřiměřená a není opodstatněna bezpečnostními riziky, která jednotlivé komponenty či programové	Neakceptováno - nyní § 29 Definice dodavatele a poddodavatele koresponduje s cíli mechanismu prověřování dodavatelského řetězce. Záměrně není definována hloubka dodavatelského řetězce, protože to by mohlo vést k obcházení povinností stanovených v návrhu zákona, a tak k maření jeho cíle. Naopak riziko pro strategicky významnou službu může přijít z kterékoliv úrovně dodavatelského řetězce. Přiměřenost prověřování a její posouzení pak bude brát v potaz všechny aspekty, které navrhovatel v připomínce požaduje zohlednit. Stejně tak z návrhu zákona vyplývá možnost nehlásit (a tedy ani neprověřovat) dodavatele, kteří nemají význam z hlediska kybernetické bezpečnosti. Připomínka vypořádána.

		vybavení představují pro kybernetickou bezpečnost regulované služby. Tato hloubka prověřování by naopak byla přiměřená v případě služeb elektronických komunikací, kde by poskytovatelé strategicky významných služeb měli zjišťovat informace o dodavatelích použité infrastruktury, jakožto bezpečnostně významných dodavatelích, přičemž by měli promítnout opatření obecné povahy spočívající v zákazu nebo stanovení podmínek využívání plnění bezpečnostně významného dodavatele i na dodavatele infrastruktury pro využívané služby elektronických komunikací. Vypořádání připomínky z veřejné konzultace SE nevyrovnává s různorodou povahou poddodavatelů pospanou výše (dodavatele software vs. komponent). Ze skutečnosti, že hloubka prověřování musí být přiměřená, neplyne možnost některé dodavatele, kteří nemají význam z hlediska kybernetické bezpečnosti, zcela ignorovat.	
846. O2	Z	Zákon o kybernetické bezpečnosti, § 28 odst. 4 <i>„... kritéria rizikovosti dodavatele a způsob jejich vyhodnocení stanoví prováděcí právní předpis.“</i> Nevydávat Vyhlášku o kritériích rizikovosti dodavatele a její obsah přenést do zákona o kybernetické bezpečnosti (přílohu vyhlášky, která stanovuje kritéria rizikovosti, doplnit jako přílohu samotného zákona). Původní znění zakládá právní nejistotu pro poskytovatele strategicky významných služeb i bezpečnostně významné dodavatele, protože kritéria hodnocení rizikovosti se mohou v budoucnu významně a snadno změnit změnou vyhlášky. Původní znění v tomto směru pro obsah vyhlášky nestanoví žádné limity.	Neakceptováno Vyhláška o kritériích rizikovosti dodavatele byla z návrhu vypuštěna. Připomínka vypořádána.

		Ponechání této kompetence v rukou moci výkonné, nikoli zákonodárné, by vedlo k nepřiměřené koncentraci pravomocí v rukou jednoho z orgánů veřejné moci, nesouladné s principem dělby moci, která je v demokratickém právním státě nezbytná. Nelze přitom akceptovat vypořádání připomínky z veřejné konzultace, dle kterého je úprava kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. Podstata hodnocení bezpečnosti dodavatelského řetězce a dostupná opatření se závažností dopadu blíží opatřením podle zákona č. 34/2021 Sb. o prověřování zahraničních investic, přičemž zde jsou základní parametry hodnocení rovněž stanoveny zákonem. Současně již nyní navrhovaná kritéria jsou svou povahou obecná lze proto očekávat minimum jejich změn. K jejich vyčlenění do prováděcího právního předpisu tedy není racionální důvod. S ohledem na závažný ekonomický i provozní dopad na poskytovatele regulované služby tedy nelze akceptovat model, kdy by kritéria byla stanovena vyhláškou.	
847. O2	Z	Zákon o kybernetické bezpečnosti, § 30 Omezení rizik spojených s dodavatelem Za odstavec 3 vložit nový odstavec 4 ve znění „Ukládá-li opatření obecné povahy povinnost poskytovateli služeb elektronických komunikací, má Český telekomunikační úřad v řízení o vydání opatření obecné povahy postavení dotčeného orgánu. Dotčený orgán uplatňuje v řízení stanoviska, která nejsou rozhodnutím ve správním řízení a jejichž obsah je závazný pro vydání opatření obecné povahy podle odst. 1.“	Neakceptováno - nyní § 31 Dle navrhované úpravy NÚKIB v rámci získávání informací spolupracuje s relevantními orgány státu, přičemž v případě jednotlivých sektorů pak zákon v podobě, jaké je dnes, tuto spolupráci předpokládá s regulátory jednotlivých sektorů, je-li to pro daný případ možné. Toto je zaručeno mimo jiné § 8 odst. 2 zákona č. 500/2004 Sb., správního řádu. Dále je tento postup dán principem dobré správy, kdy NÚKIB pro co nejlepší vyhodnocení situace a možných dopadů počítá s dožádáním informací od relevantních orgánů státu v rámci jednotlivých odvětví. Důvodem, proč jsou v navrhovaném zákoně popsány orgány, které jsou obsaženy v § 29, je ten, že tyto fungují napříč

	ČTÚ disponuje nejširší expertízou v oblasti trhu služeb elektronických komunikací a dohlíží nad bezpečností a integritou veřejných komunikačních sítí a služeb elektronických komunikací. Závažné zásahy do trhu poskytování služeb elektronických komunikací nelze efektivně provádět bez informací, jimiž disponuje pouze sektorový regulátor, který je ze zákona eviduje a zpracovává. ČTÚ ze zákona náleží dohled nad trhem se službami elektronických komunikací, který nelze účinně provádět, bude-li do trhu zasahovat jiný správní orgán bez nutnosti vyžádání stanoviska, potenciálně i bez vědomí ČTÚ. Současně musí mít sektorový regulátor k dispozici informace o připravovaných zásadních zásazích do jím regulovaného trhu. Spolupráce s dotčeným orgánem také snižuje zátěž povinných osob z hlediska poskytování obdobné součinnosti jak NÚKIB, tak ČTÚ. Návrh má za cíl vytvořit obdobný mechanismus stanovisek dotčeného orgánu k mechanismu stanovisek dotčených orgánů podle § 54 zákona č. 283/2021 Sb., stavebního zákon (a obdobně podle zákona č. 183/2006 Sb.), přičemž kromě ČTÚ by dotčenými orgány mohli být také ostatní sektorový regulátoři (např. ERÚ, ÚCL apod.). Takový mechanismus zároveň sníží koncentraci pravomocí NÚKIB, který má v původní podobě návrhu možnost významně zasáhnout do téměř všech odvětví národního hospodářství bez ohledu na existenci a stanovisko regulační autority příslušného sektoru. Vypořádání připomínky z veřejné konzultace nepovažujeme za dostatečné. Argumenty vznesené ve vztahu k NÚKIB lze analogicky uvést i u obce či kraje jako pořizovatelů územně plánovací dokumentace, přesto jsou obec i kraj při pořizování územně plánovací dokumentace vázány stanovisky dotčených orgánů a nadřízeného orgánu.	jednotlivými sektory a jejich spolupráce je tak pro správné posouzení rizik, včetně vyhodnocení pro případné omezení či zákaz, žádoucí. Připomínka vypořádána.

848. O2	Z	Zákon o kybernetické bezpečnosti, § 32 Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce odst. 1 písm. a) a b) <i>„... zjišťovat s vynaložením přiměřeného úsilí informace o dodavatelích bezpečnostně významných dodávek a dokumentovat tyto informace alespoň v rozsahu identifikace všech bezpečnostně významných dodávek a dodavatelů bezpečnostně významných dodávek, kteří je poskytují,“</i> Upřesnit, že bezpečnostně významnou dodávkou plynoucí z rámcové smlouvy je uzavření rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb jako celku (se specifikací rozsahu rámcové smlouvy), nikoli jednotlivé dílčí plnění (objednávky). V případě, že by každé jednotlivé dílčí plnění (realizovaná objednávka) z rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb, mělo být hlášeno jako samostatná bezpečnostně významná dodávka, byla by na poskytovatele strategicky významné služby kladena neúměrně vysoká administrativní zátěž a stejně tak NÚKIB by byl zatížen řadou nadbytečných hlášení bez přidané informační hodnoty. Účel tohoto ustanovení bude naplněn i ve znění navrhované změny, dle které se plnění plynoucí z rámcové smlouvy budou hlásit jako jedna bezpečnostně významná dodávka s určením možného rozsahu plnění. Vypořádání připomínky z veřejné konzultace nereflektuje, že návrh se vztahuje k opakovanému objednávání stejného plnění (zboží) tedy nezměněného bezpečnostního rizika.	Akceptováno jinak - nyní § 33 Souhlasíme, že v případě, kdy se dílčí plnění z rámcové smlouvy nijak nezmění, bylo by nadbytečné každé toto plnění hlásit. Úprava této problematiky na úrovni zákona je však s ohledem na její specifickou nevhodná. Z těchto důvodů byla upravena DZ k § 32 nZKB následujícím způsobem: „Úřad specifikuje, že vzhledem k účelu ustanovení není v případě rámcových smluv na dodávku určitého výrobku nebo služby žádoucí, aby byla opakovaně hlášena jednotlivá dílčí plnění. Postačí hlášení rámcové smlouvy jako celku. Výjimkou jsou však situace, kdy dojde ke změně v dodavatelském řetězci. Pak je povinností poskytovatele strategicky významné služby, aby tuto změnu Úřadu nahlásil.“ Připomínka vypořádána.

849. O2	Z	Zákon o kybernetické bezpečnosti, § 32 Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce odst. 2 <i>„Poskytovatel strategicky významné služby začne plnit povinnost hlásit informace podle odstavce 1 pro každou strategicky významnou službu nejpozději do 1 roku ode dne doručení písemného vyrozumění o jejím zápisu do evidence poskytovatelů regulovaných služeb podle § 10 odst. 1.“</i> Doplnit, že doba 1 roku ode dne doručení písemného vyrozumění o zápisu se vztahuje také na povinnost zjišťovat informace podle § 32 odst. 1 písm. a). Přechodné období by se nemělo uplatnit pouze pro povinnost hlásit NÚKIB informace, ale i pro povinnost je zjišťovat. Není přiměřené požadovat, aby poskytovatelé strategicky významných služeb zahájili sběr informací bezprostředně po účinnosti zákona, bez stanovení přechodného období. Vypořádání připomínky z veřejné konzultace nereflektuje skutečnost, že plnění povinnosti zjišťovat informace nelze zahájit okamžitě. K okamžiku zápisu do evidence poskytovatelů regulované služby nebude mít poskytovatel strategicky významné služby nastaveny odpovídající smluvní a compliance mechanismy a v případě kontroly bezprostředně po tomto zápisu bude čelit riziku významných sankcí ze strany NÚKIB. I proto povinnost je tak třeba nastavit odložené plnění, aby bylo možné zavést příslušné smluvní a compliance mechanismy.	Neakceptováno - nyní § 33 Úřad považuje zmíněnou povinnost, tj. zahájení přiměřeného prověřování dodavatelů a bezpečnostně významných dodávek za zcela adekvátní k účelu a cíli navrhovaného mechanismu. Naopak navrhovatelem požadovanému odložení zahájení těchto kroků o jeden rok, by vedlo k významnému zpoždění aplikace celého mechanismu. Tak, jak jsou ustanovení navržena, začne poskytovatel zavádět kroky a procesy ve chvíli, kdy se na něj předmětná úprava vztáhne. Tento proces následně po roce završí tím, že Úřadu ohlásí informace týkající se dodavatelů a bezpečnostně významných dodávek. Připomínka vypořádána.

850. O2	Z	Zákon o kybernetické bezpečnosti, § 33 Omezení rizik spojených s dodavatelem ve veřejných zakázkách Odstranit z § 32 slova „<i>v postavení zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek</i>“ a slova „<i>na veřejnou zakázku</i>“. I soukromý subjekt, který není zadavatelem podle zákona o zadávání veřejných zakázek, může mít sjednaný dlouhodobý závazek, při jehož sjednávání nemohl vědět, že jeho dodavatel bude shledán rizikovým dodavatelem. Řada takových závazků může být sjednána před účinností navrhovaného zákona. Pro takové případy je třeba stanovit mechanismy umožňující i takovému soukromému subjektu ukončit sjednaný závazek. Vypořádání připomínky z veřejné konzultace nereflektuje skutečnost, že některé kontrakty na bezpečnostně významné dodávky jsou dlouhodobé a mohly být sjednány před přijetím navrhované právní úpravy a tedy ji nemohly předvídat a nemusí v ní být obsažen adekvátní výpovědní důvod.	Akceptováno - nyní § 34 Připomínka byla zapracována tak, aby bylo vyhověno návrhu. Připomínka vypořádána.
851. O2	Z	Zákon o kybernetické bezpečnosti, § 17 Náležitosti hlášení kybernetických bezpečnostních incidentů odst. 3 písm. b) a c) odst. 5 Vyhláška o Portálu NÚKIB a požadavcích na vybrané úkony § 3 Hlášení kybernetického bezpečnostního incidentu Doplnit náležitosti závěrečné zprávy buď přímo do odstavce 3 nebo do § 3 Vyhlášky o Portálu NÚKIB	Akceptováno Ustanovení § 17 odst. 5 návrhu zákona obsahuje zmocňovací ustanovení pro vydání prováděcího předpisu, který stanoví mj. obsahové náležitosti hlášení incidentu. Tímto předpisem je vyhláška o Portálu Úřadu a požadavcích na vybrané úkony, která v § 3 odst. 1 stanovuje obsahové náležitosti formuláře pro hlášení incidentů, přičemž z odst. 2 písm. d) tohoto ustanovení vyplývá, že lze přes daný formulář vytvořit i závěrečnou zprávu, jejíž náležitosti byly doplněny do odst. 3.

		Paragraf 17 odst. 3 písm. b) a c) ZKB ukládá poskytovatelům regulované služby povinnost do 30 dní od oznámení incidentu nebo předložení zprávy o aktuálním stavu zvládání kybernetického bezpečnostního incidentu předložit závěrečnou zprávu, jejíž náležitosti mají být dle odst. 5 stanoveny prováděcím předpisem. Vyhláška o Portálu NÚKIB v § 3, který popisuje obsahové náležitosti úkonů spojených s hlášením kybernetických bezpečnostních incidentů se ale nevěnuje konkrétním náležitostem závěrečné zprávy, nýbrž pouze popisu obsahu formuláře pro hlášení incidentů, z něhož vyplývá, že slouží primárně k oznamování incidentů dle § 17 odst. 1 písm. a) nebo c) podávání průběžné zprávy o podstatných změnách stavu zvládání kybernetického bezpečnostního incidentu podle § 17 odst. 3 písm. b) zákona. Navrhujeme proto doplnit obsahové náležitosti závěrečné zprávy, aby se předešlo nejistotě regulovaných osob ohledně způsobu plnění povinností podle § 17 odst. 1 písm. b) a c), obzvláště vzhledem k tomu, že za jejich porušení hrozí dle § 58 odst. 1 písm. h) ve spojení s odst. 15 písm. a) pokuta ve výši až 250 000 000 Kč nebo do výše 2 % čistého celosvětového ročního obrátu.	Připomínka vypořádána.
852. O2	Z	Zákon o kybernetické bezpečnosti, § 19 Informační povinnost poskytovatele regulované služby odst. 2 Na začátku odstavce 2 nahradit slova „<i>Poskytovatel regulované služby</i>“ za slova „<i>Dozví-li se poskytovatel regulované služby o významné kybernetické hrozbě ohrožující poskytování jím poskytované regulované služby</i>“. Ze současného znění zákona není patrné, o jakých hrozbách by měl poskytovatel regulované služby uživatele informovat a zároveň je povinnost stanovena nezávisle na vědomosti poskytovatele o	Neakceptováno - nyní § 20 O hrozbách, o kterých se poskytovatel regulované služby nedozví a nemohl dozvědět, není z podstaty věci možné kohokoliv informovat a toto jednání sankcionovat. Vztahovat informační povinnost na uživatele kterékoliv regulované služby se zároveň jeví jako výrazně extenzivní výklad, který úmyslem zákonodárce není a nevyplývá z textu zákona ani důvodové zprávy. Vzhledem k provázanosti poskytovatele regulované služby, regulované služby a uživatele regulované služby, by nemělo dojít k pomýlení, že bude poskytovatel regulované služby

		existenci hrozby. Povinnost je přitom spojena s nejvyšší možnou pokutou dle § 58 odst. 1 písm. k) ve spojení s odst. 15 písm. a). Navrhujeme proto jasně definovat, že poskytovatel je povinen informovat pouze o hrozbách, o kterých se dozví, a které ohrožují jím poskytovanou regulovanou službu. Dle současného znění by totiž bylo možné sankcionovat jakéhokoli poskytovatele za jakoukoli významnou hrozbu nezávisle na tom, jestli se hrozba dotýká jím poskytované regulované služby a jestli o hrozbě poskytovatel věděl nebo vědět měl.	muset informovat o hrozbách, jež se službou, kterou poskytuje, vůbec nesouvisí, případně pak informovat uživatele jiných regulovaných služeb. Připomínka vypořádána.
853. O2	Z	Zákon o kybernetické bezpečnosti § 65 Společná a zvláštní ustanovení o řízení před Úřadem odst. 4 Ve spojení s § 11 odst. 2 Část odst. 4 před středníkem nahradit za slova „<i>Rozhodnutí o výmazu z evidence poskytovatelů regulovaných služeb podle § 11 odst. 2</i>“. Ustanovení § 65 odst. 4 si v hypotéze klade za podmínku zahájení řízení podle § 11 odst. 2 z moci úřední. Řízení podle § 11 odst. 2 však nemůže být zahájeno na žádost, tudíž se vždy musí jednat o řízení z moci úřední. Z tohoto důvodu navrhujeme vymazat nadbytečnou podmínku.	Akceptováno jinak Na základě této, ale i dalších souvisejících připomínek došlo k celkové úpravě ustanovení o výmazu regulované služby z evidence. Ustanovení nyní připouští jak zahájení řízení o výmazu z moci úřední, tak na žádost poskytovatele regulované služby. Připomínka vypořádána.
854. O2	Z	Vyhláška o kritériích rizikivosti dodavatele Příloha bod 11 Vypustit bod 11 přílohy vyhlášky „<i>Je důvodná obava, že schopnost dodavatele poskytovat plnění může být významným způsobem omezena či jinak narušena</i>“. Bod 11 přílohy vyhlášky nesměřuje k ochraně vůči dodavatelům, kteří představují bezpečnostní hrozbu pro Českou republiku nebo	Akceptováno jinak Vyhláška o kritériích rizikivosti dodavatele byla z návrhu vypuštěna. Připomínka vypořádána.

		vnitřní či veřejný pořádek, ale proti dodavatelům, kteří by potenciálně nemuseli být schopni dostát svým smluvním závazkům. Čistě ekonomické schopnosti dodavatelů jsou záležitostí podnikatelského rizika poskytovatelů strategicky významných služeb, kteří pravděpodobně disponují podrobnějšími informacemi o sektoru, v němž podnikají, než orgány státní správy. Jedná se tudíž o nadbytečné ustanovení, které má zbytečný potenciál omezovat svobodu podnikání poskytovatelů strategicky významných služeb. Z tohoto důvodu navrhuje ustanovení vypustit.	
855. Český zeměměřický a katastrální	úřad Z	Obecně k návrhu Předložená právní úprava v řadě aspektů překračuje rámec směrnice NIS2, aniž by v důvodové zprávě bylo řádně zdůvodněno, proč předkladatel k takto náročnějšímu řešení přistoupil. Navrhované změny v organizaci kybernetické bezpečnosti budou znamenat významné navýšení administrativní zátěže a nákladů na státní rozpočet, a není reálné zajistit je v rámci rozpočtu jednotlivých kapitol bez toho, aby se tak stalo na úkor ostatních činností ústředních správních úřadů. Navrhovaná právní úprava zavádí nové povinnosti, které ústřední správní úřady objektivně nebudou moci naplňovat, zvláště v současné době, kdy je usilováno o snižování strukturálního deficitu státního rozpočtu a cílem by mělo být spíše snižování výdajů než jejich nepřiměřené navyšování. Požaduji důslednou revizi návrhu zákona z pohledu, co je opravdu nezbytné pro naplnění smyslu směrnice a zároveň reálné, a v případě zachování navrhovaného rozsahu povinností požaduji zajištění finančního a personálního pokrytí nad rámec stávajícího rozpočtu a stávající systemizace.	Neakceptováno V prvé řadě musíme zdůraznit, že pokud připomínkové místo neuvede co připomínkuje, není taková připomínka v souladu s požadavky Legislativních pravidel vlády. Důvodová zpráva a hodnocení dopadů regulace, jakožto předložené materiály, mají přes 200 stran a jejich podstatou je zdůvodnit předložený návrh, což dle předkladatele činí. Pokud připomínkové místo obecně uvede, že v důvodové zprávě nebylo řádně zdůvodněno, proč předkladatel k takto náročnějšímu řešení přistoupil, bez uvedení konkrétních míst kde se to podle autora stalo, lze na takovou připomínku reagovat jen velmi obtížně. Stejně tak je tomu v případě části připomínky "Navrhovaná právní úprava zavádí nové povinnosti, které ústřední správní úřady objektivně nebudou moci naplňovat" opět bez dalšího upřesnění. Dle předkladatele je každou z uvedených povinností možné objektivně naplňovat, jinak by taková povinnost ani nebyla v návrhu předložena.

			Bez ohledu na výše uvedené však v odpovědi na tuto připomínku uvádíme, že návrh v současné podobě reflektuje požadavky směrnice NIS2, dále zohlednění kontinuity současné právní úpravy zákona o kybernetické bezpečnosti a v neposlední řadě poznatky Úřadu vzhledem k zhoršující se bezpečnostní situaci a v neposlední řadě poznatky z kontrol aktuálně regulovaných subjektů. Pokud připomínka směřuje vůči zahrnutí obcí typu III. o návrhu regulace, což je oproti požadavkům směrnice nebo dosavadní právní úpravě největší změna (kraje i ostatní úřady jsou již regulovány), vedou k tomu předkladatele zkušenosti se stále se stupňujícími kybernetickými útoky zaměřenými přesně na tento typ instituce. Pokud bylo podstatou připomínky něco jiného, musí NÚKIB, přestože takové vypořádání pro něj není běžné, tuto připomínku s ohledem na čl. 5 odst. 6 Legislativních pravidel vlády neakceptovat. Připomínky byly vysvětlením vypořádány.
856. Český úřad zeměměřický a katastrální	Z	K § 4 odst. 2 ve spojení s tezemi vyhlášky o regulovaných službách, příloha bod 19 Požadují, aby byly vědeckovýzkumné instituce nebyly zařazovány mezi poskytovatele regulované služby v režimu vyšších povinností z důvodu, že většina prováděných výzkumných projektů je financována z více než 50 % z veřejných zdrojů. Vědeckovýzkumné instituce nedisponují pro zajištění požadovaných opatření dostatečným finančním ani personálním vybavením. Zahrnutí nekomerčních výzkumných organizací do národní regulace překračuje rámec požadavků směrnice NIS2. Navrhovaná právní úprava bude mít značný a zcela nepřiměřený dopad na činnost a rozpočet výzkumných institucí, aniž by to bylo řádně odůvodněno a podloženo skutečnou potřebou.	Akceptováno jinak Výběr služeb a subjektů regulovaných v rámci odvětví 19. Výzkum a vývoj nad rámec požadavků směrnice NIS2 proběhl na základě vyhodnocení aktuální úrovně kybernetické bezpečnosti odvětví, posouzení strategičnosti a relevance subjektů, které by do regulace měly být zařazeny, a v neposlední řadě i po konzultaci se subjekty, na které regulace bude dopadat. Odvětví výzkumu a vývoje je strategickým odvětvím, v němž jsou jednak investovány nemalé veřejné prostředky, na jejichž ochraně má stát logický zájem, jednak v něm vzniká a je uchováváno obrovské množství strategicky cenných informací. Výsledky výzkumů jsou v posledních letech častým terčem

			kybernetických útoků, jež mají za cíl odcizit dosažené poznatky a využít je buďto komerčně (bez nutnosti financovat jejich legální opatření), nebo pro působení proti zájmům České republiky. S ohledem na skutečnost, že výzkumné instituce a vysoké školy soustřeďují v rámci svých kapacit nadkritické množství materiálních, lidských a finančních zdrojů potřebných pro dosahování průlomových poznatků, které přinášejí znalostní řešení socioekonomických výzev, je tak veřejný zájem na zajištění dostatečné úrovně jejich kybernetické bezpečnosti zcela zřejmý a odůvodněný. Zároveň však došlo k přehodnocení rozřazení regulovaných subjektů do jednotlivých režimů a také k redukci regulovaných osob. Došlo tedy k úpravě kritérií pro identifikaci povinných osob v odvětví 19.1. Výzkum a vývoj a k přesunutí jiné výzkumné organizace do režimu nižších povinností. Rovněž jsou nyní v režimu nižších povinností zahrnuty pouze jiné výzkumné organizace, které se věnují průmyslovému výzkumu nebo experimentálnímu vývoji. Kritérium financování z veřejných zdrojů však zůstalo zachováno, a to právě za účelem ochrany veřejných prostředků investovaných do výzkumné činnosti. Připomínky byly vysvětlením vypořádány.
857. Český úřad zeměměřický a katastrální	Z	K § 7 Požaduji předložený návrh upravit tak, aby nebyl zaváděn princip, kdy poskytovatel regulované služby, který poskytuje více regulovaných služeb, přičemž alespoň jedna z nich naplňuje kritéria pro zařazení poskytovatele do režimu vyšších povinností, musí ke všem regulovaným službám přistupovat z pohledu režimu vyšších povinností. Takový přístup významně zvyšuje administrativní, finanční i personální zatížení subjektů, aniž by pro to existovaly	Neakceptováno V případě této připomínky je nutné vysvětlit způsob fungování režimu vůči fungování zavádění bezpečnostních opatření v rámci daného režimu. Pokud se připomínkové místo obává neúčelného plnění přísnějších povinností nadbytečně i tam, kde to není nutné, je možné v rámci bezpečnostních opatření tento problém řešit plánem zvládání rizik a

		objektivní důvody. Nesouhlasím s tvrzení uvedeným v důvodové zprávě, že „zavádění několika různých systémů řízení kybernetické bezpečnosti v jedné organizaci poskytovatele regulované služby je neúčelné a dlouhodobě neudržitelné.“ Naopak je neúčelné plnit přísné povinnosti nadbytečně i tam, kde to není nutné, neboť to charakter dané regulované služby nevyžaduje.	prohlášením o aplikovatelnosti, což vyhláška o bezpečnostních opatřeních pro vyšší režim požaduje a je to ústřední nástroj pro práci s vyhláškou. Adresát to bude muset udělat, protože v dané situaci alespoň jednu regulovanou službu ve vyšším režimu bude mít. Právě tam může se všemi systémy napříč organizací pracovat účelně. U jiných povinností, např. hlášení incidentů, ustanovení o jednotnosti režimu vynikne ještě více - pokud by v organizaci existovaly různé režimy pro různé regulované služby, bude organizace nákladně udržovat v chodu dva přístupy k bezpečnosti, což je nejen neekonomické, ale také uživatelsky nepřívětivé - právě tento aspekt pak v důsledku snižuje celkovou bezpečnost. Je také potřeba poznamenat, že dle zkušeností z kontrol vykonávaných Úřadem je snaha rozdělovat systémy na jednotlivé služby spíše jen optická - i kdyby pravidlo o jednotnosti režimu nebylo zavedeno, tak pokud se na aktivu „sejde“ režim vyšších a nižších povinností, bylo by k tomuto aktivu potřeba přistupovat tak, aby splnilo pravidla jak pro vyšší, tak pro nižší režim. To pak ale v praxi znamená, že je podstatná část architektury ve vyšším režimu, protože bývá téměř vždy využívána pro všechny regulované služby společně. Navíc celá regulace veřejné správy podle tohoto návrhu je postavena na jedné službě v příloze vyhlášky o regulovaných službách, odvětví I., kde se pro danou službu zařadí celek do vyššího nebo nižšího režimu. Připomínky byly vysvětlením vypořádány.
858. Český úřad zeměměřický a katastrální	Z	K § 13 odst. 1 písm. a) Požaduji ustanovení uvést v následujícím znění: „a) identifikuje všechna primární aktiva související s poskytováním regulované služby v rámci celé organizace,“.	Neakceptováno Stanovený rozsah se vztahuje na aktiva související s regulovanou službou (nikoliv na všechna

		Vzhledem k tomu, že definice primárních aktiv je velice široká, kdy primárním aktivem se rozumí informace a služby, přičemž informacemi se rozumí také data, včetně provozních údajů, a službou se rozumí také procesy, musel by poskytovatel služby provádět vyhodnocení a identifikovat i např. docházkový systém, proces vypisování dovolenek nebo stanovování odměn. Požadavek na identifikaci veškerých primárních aktiv se tak jeví jako zcela nepřiměřený a nadbytečně administrativně zatěžující.	identifikovaná primární aktiva - pokud všechna nesouvisí s regulovanou službou). Je pracováno s typovými aktivy, nikoliv s každou službou/informací jako takovou zvlášť. Jde o základní identifikaci služeb, které organizace poskytuje (za jakým účelem je vytvořena a co jsou její zásadní služby). Primární aktiva, která nesouvisí s regulovanou službou není potřeba hodnotit (nZKB to nepožaduje). Nepovažujeme tuto změnu při identifikaci aktiv za nepřiměřenou. Je pravda, že v tomto ustanovení se projevují zkušenosti Úřadu z kontrolní činnosti, kdy správně stanovit rozsah ISMS organizací způsobuje značné problémy. Oproti platné právní úpravě došlo k otočení způsobu identifikace primárních aktiv, na které se nyní pohlíží z pohledu celé organizace a určují se ty, které souvisejí s regulovanou službou. Nesouhlasíme s tím, že pro zajištění kybernetické bezpečnosti současné znění předmětného ustanovení nebude mít vliv, a že se jedná o nepřiměřený zásah do práv povinných subjektů. Naopak, naší snahou je zmírnění požadavku NIS2 zavádět opatření na celou organizaci v tom smyslu, že se prvně hledí na celou organizaci, ale opatření se zavádí na těch aktivech, které se přímo dotýkají poskytování regulované služby. Připomínky byly vysvětlením vypořádány.
859. Český úřad zeměměřický a katastrální	Z	K § 17 odst. 3 písm. c) Požadují zde stanovenou lhůtu pro předložení závěrečné zprávy pro zvlášť složité kybernetické bezpečnostní incidenty prodloužit na 60 dní. Zároveň požadují, aby lhůta byla počítána od vyřešení incidentu, nikoliv od prvního hlášení.	Neakceptováno Proces hlášení kybernetických bezpečnostních incidentů je podrobně upraven přímo směrnici NIS2, tzn. pokud by do zákona nebyla tato úprava zahrnuta, jednalo by se o rozpor se směrnicí a Česká republika

			by mohla čelit sankcím za nesprávnou transpozici unijního předpisu. Lhůta pro předložení závěrečné zprávy o vyřešení incidentu je podle čl. 23 odst. 4 písm. d) směrnice NIS2 „nejpozději do jednoho měsíce od předložení oznámení incidentu podle písmene b)“. Z výše uvedeného důvodu národní právní úprava tento požadavek kopíruje. V případě, že po uplynutí této lhůty incident stále trvá, což se může stát v případě zvláště složitého incidentu, je stanovena lhůta na předložení závěrečné zprávy o vyřešení kybernetického bezpečnostního incidentu na 30 dnů od vyřešení tohoto incidentu. Připomínky byly vysvětlením vypořádány.
860. Český úřad zeměměřický a katastrální	D	K § 30 až 33 Doporučuji doplnit, že Národní úřad pro kybernetickou a informační bezpečnost bude na žádost poskytovatele strategicky významné služby při vyhodnocování rizik dodavatele, resp. dodavatelského řetězce, poskytovat součinnost.	Neakceptováno - nyní § 31 až 34 Návrh vznesený v připomínce považujeme za nedůvodný. V rámci procesu prověřování rizik spojených s dodavatelem, který je součástí mechanismu prověřování bezpečnosti dodavatelského řetězce, je povinností poskytovatele strategicky významné služby toliko zjišťovat s vynaložením přiměřeného úsilí základní informace o všech dodavatelích bezpečnostně významných dodávek a zjištěné informace nahlásit Úřadu v zákonem stanovené lhůtě. Samotné vyhodnocení rizikovosti těchto dodavatelů je úkolem Úřadu. Pro navrhované poskytování součinnosti Úřadem poskytovateli strategicky významné služby tedy není důvod, neboť poskytovatel strategicky významné služby v rámci mechanismu prověřování bezpečnosti dodavatelského řetězce rizika spojená s dodavatelem nevyhodnocuje. To činí Úřad. Nad rámec výše uvedeného doplňujeme, že řízení dodavatelů je samostatnou povinností poskytovatele regulované služby vyplývající ze zcela

			jiné části návrhu zákona, než na kterou připomínka směřuje, a dále z návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. Řízení dodavatelů je přitom povinností, kterou si musí plnit sám poskytovatel regulované služby. Připomínky byly vysvětlením vypořádány.
861. Český úřad zeměměřický a katastrální	Z	K § 34 odst. 3 Zde stanovená doba jednoho roku na splnění povinností poskytovatele je i s ohledem na lhůty vyplývající ze zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zcela nerealizovatelná. Pro naplnění podmínek stanovených zákonem je nezbytné zajistit dobudování infrastruktury a navýšení personálních kapacit i finančního pokrytí zvýšených nákladů, což není možné ve stanovené lhůtě a v rámci stávajícího státního rozpočtu splnit.	Neakceptováno - nyní § 35 Připomínkované ustanovení § 34 bylo v odst. 1 upraveno tak, že „Poskytovatel strategicky významné služby je povinen zajistit její dostupnost v nezbytném rozsahu, v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky.“. Tento nezbytný rozsah pak bude stanoven vyhláškou o nezbytném rozsahu dostupnosti strategicky významných služeb. V případě veřejné správy budou stanovena kritéria dopadu kybernetického bezpečnostního incidentu v podobě narušení dostupnosti služby a nezbytným rozsahem pak budou jen ty služby veřejné správy, které budou naplňovat tato kritéria dopadu. Přičemž ta budou zhruba odpovídat kritériím dopadu na úrovni kritická podle vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy pak v § 6m odst. 2 stanoví, že „Poskytovatelem cloud computingu poskytujícím orgánu veřejné správy cloud computing zařazený do nejvyšší bezpečnostní úrovně může být pouze poskytovatel státního cloud computingu.“ Připomínkou namítaný dopad na veřejné zadavatele se tak vzhledem k výše uvedenému předkladatel neočekává.

			Připomínky byly vysvětlením vypořádány.
862. Sdružení CZ.NIC	Z	<u>K návrhu zákona o kybernetické bezpečnosti</u> K § 36 Navrhujeme v § 36 vložit nové odstavce (4) a (5) a zbylé odstavce přečíslovat. Znění nových odstavců je následující: (4) Subjekt spravující a provozující registr internetových domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén mohou při zavedení postupů pro ověření totožnosti držitele jména domény využít prostředek pro elektronickou identifikaci vydaný v rámci kvalifikovaného systému elektronické identifikace. Subjekt poskytující služby registrace jmen domén může přistupovat ke kvalifikovanému systému elektronické identifikace prostřednictvím subjektu spravujícího a provozujícího registr internetových domén nejvyšší úrovně na základě uzavřené smlouvy. (5) Subjekt spravující a provozující registr internetových domén nejvyšší úrovně může s cílem zajistit přesnost a úplnost informací vedených v databázi doručovat elektronicky prostřednictvím datové schránky podle jiného právního předpisu.³ Tuto připomínku považujeme za zásadní. Odůvodnění: Odůvodnění návrhu zákona správně uvádí, že pro ověření totožnosti držitele jména domény může subjekt spravující a provozující registr internetových domén nejvyšší úrovně („registr TLD“) a registrátoři domén využívat prostředky pro elektronickou identifikaci vydané v rámci kvalifikovaného systému elektronické identifikace. Nicméně je klíčové, aby se tato možnost objevila přímo v legislativním textu. Zákon č. 250/2017 Sb. o elektronické identifikaci v ustanovení § 2	Akceptováno jinak - nyní § 37 Do ustanovení § 37 byl doplněn odstavec 4 následujícího znění: „Subjekt spravující a provozující registr domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén mohou při zavedení postupů pro ověření totožnosti držitele jména domény využít prostředek pro elektronickou identifikaci podle zákona upravujícího elektronickou identifikaci. Subjekt poskytující služby registrace jmen domén může přistupovat ke kvalifikovanému systému elektronické identifikace prostřednictvím subjektu spravujícího a provozujícího registr domén nejvyšší úrovně na základě uzavřené smlouvy.“ Pokud jde o možnost doručování do datové schránky, platí, že zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, v účinném znění, upravuje povinnost doručit dokument do datové schránky pouze orgánu veřejné moci. Způsob komunikace mezi soukromoprávními subjekty je zcela v jejich dispozici. Doplnění § 37 návrhu zákona v tomto smyslu máme tedy za neopodstatněné, uvedenou možnost komunikace jsme nicméně nově doplnili do důvodové zprávy. Připomínkové místo s vypořádáním souhlasí.

³ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

	uvádí: „Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace (dále jen „kvalifikovaný systém“).“ Pro možnost využití kvalifikovaného systému elektronické identifikace je tedy podstatné, zda-li lze nalézt důvod pro toto využití v nějakém právním předpisu. V tomto duchu odkazujeme i na připomínku Digitální a informační agentury ze dne 12. července 2023 k návrhu zákona o kybernetické bezpečnosti. Využívání národních systémů pro elektronickou identifikaci uvádí také agentura ENISA jako příklad dobré praxe ve své nedávno vydané publikaci „<i>DNS Identity – Verification and Authentication of Domain Name Owners</i>“). Příkladem takové dobré praxe může být Dánsko, kde je verifikace držitele domény prostřednictvím národního systému e-identifikace, obsaženo přímo v legislativě. Domníváme se, že pokud stát má zájem o co největší úplnosti a přesnosti souboru registračních údajů, mělo by být také v jeho zájmu umožnit maximální možné použití již existujících prostředků, ať už je to prostřednictvím zákonného zmocnění k využití kvalifikovaného systému elektronické identifikace, nebo v případě registru TLD prostřednictvím systému datových schránek. Z věcné povahy věci se jedná o kvazi veřejnoprávní agendu, která opodstatňuje využití těchto prostředků ze zákona. Významná skupina subjektů poskytujících registrace domén již má nastavené technické propojení na provozovatele registru internetových domén nejvyšší úrovně a z důvodu zjednodušení realizace by tak mohl registr přístup ke kvalifikovanému systému pro tyto subjekty zprostředkovávat na základě smlouvy. Oceňujeme, že tato možnost je zmíněna v odůvodnění návrhu, nicméně bez příslušného legislativního ukotvení není pro možnost tohoto postupu opora. Navrhované ustanovení je také navrhováno s cílem implementovat zásadu z NIS 2, podle které nemají nově zavedené postupy vést ke zdvojování shromažďovaných dat.	

863. Sdružení CZ.NIC	Z	K § 36 Na konci odstavce 3 navrhujeme doplnit následující větu: „<u>Tyto zásady a postupy nesmí vést ke zdvojování shromažďovaných dat. Za tímto účelem registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén musí vzájemně spolupracovat.</u>“ Tuto připomínku považujeme za zásadní. Odůvodnění: Navrhované ustanovení implementuje čl. 28 odst. 6 směrnice NIS 2. Tento článek je významný pro garanci toho, že i subjekty poskytující služby registrace jmen domén budou na implementaci požadavků v bodech 1.-5. NIS 2 s registrem domén nejvyšší úrovně spolupracovat a bude tak zaručeno, že nedojde ke zdvojování shromažďovaných dat.	Akceptováno jinak - nyní § 37 Dotčené ustanovení bylo v zásadě doplněno požadovaným způsobem, místo „musí vzájemně spolupracovat“ byla zvolena formulace „vzájemně spolupracují“, jak je uvedeno např. v § 8 odst. 2 zákona č. 500/2004 Sb., správního řádu, v účinném znění, či v § 2 odst. 7 a v § 7 odst. 2 zákona č. 141/1961 Sb., trestního řádu, v účinném znění. Připomínkové místo s vypořádáním souhlasí.
864. Sdružení CZ.NIC	Z	K § 40 V § 40 odst. 1 písm. c) za slovo „vyhovět,“ požadujeme doplnění slov „pokud to neohrozí plnění jejich úkolů při řešení stavu kybernetického nebezpečí,“ Tuto připomínku považujeme za zásadní. Odůvodnění: Tuto připomínku jsme uplatnili již ve veřejné konzultaci, kterou NÚKIB uspořádal k předchozímu návrhu zákona. I když měla být tato připomínka akceptována, bohužel v návrhu zákona, který byl rozeslán do meziresortního připomínkového řízení se akceptace této připomínky neprojevila. I když bude povinnost vypomoci pracovními kapacitami stanovena smlouvou, je podle našeho názoru vhodné, aby zákon tuto povinnost limitoval.	Akceptováno - nyní § 41 Připomínkové místo s vypořádáním souhlasí.

V Brně 20. 12. 2023

Vypracoval: Národní úřad pro kybernetickou a informační bezpečnost (kontaktní osoba Mgr. Prokop Lang, tel. 541 110 610 e-mail: legislativa@nukib.cz)