Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

DŮVODOVÁ ZPRÁVA

A. Obecná část

B. Zvláštní část

K § X – Předmět úpravy

Věcná působnost návrhu zákona je vymezena obecně pro oblast kybernetické bezpečnosti s výjimkou informačních a komunikačních systémů nakládajících s utajovanými informacemi.

Pojmu kybernetické bezpečnosti je v souladu s dosavadní právní úpravou kontinuálně užito k odlišení od pojmu informační bezpečnosti, resp. počítačové bezpečnosti a ke zdůraznění specifického zaměření zákona na ochranu regulovaných služeb z pohledu zajištění všech relevantních aktiv sloužících ve svém důsledku pro shromáždění, zpracování, uchování, užití, sdílení, rozšiřování nebo jiné nakládání s informacemi a daty v elektronické podobě. Tento postup je zvolen s ohledem na skutečnost, že zajišťování kybernetické bezpečnosti výrazně přesahuje technologickou rovinu a vyžaduje ucelený přístup, jak uvádí také Národní strategie kybernetické bezpečnosti České republiky na období let 2021 až 2025, čímž navazuje na shrnutí pojmu kybernetické bezpečnosti, kterou Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 uváděla jako souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost. Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby a zranitelnosti v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury.

Návrh zákona současně blíže stanovuje pravomoci orgánů veřejné moci v této oblasti, především Národního úřadu pro kybernetickou a informační bezpečnost a pracovišť CERT.

Návrh zákona je téměř zcela transpozičním předpisem 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 (tzv. „směrnice NIS2“).

Je-li právním předpisem prováděno přizpůsobení právního řádu přímo použitelnému předpisu Evropské unie a je-li jím souběžně promítána do právního předpisu celá směrnice Evropské unie nebo její podstatná část, je nezbytné, aby tyto předpisy Evropské unie byly uvedeny v referenčním ustanovení, jak stanoví Legislativní pravidla vlády. Spolu se směrnicí NIS2 je tento zákon také adaptačním zákonem pro 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 (tzv. „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 a dále se jeho prostřednictvím realizuje obsah 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.

Specifické omezení působnosti návrhu zákona vztahující se k informačním a komunikačním systémům nakládajícím s utajovanými informacemi je důsledkem toho, že úprava povinných bezpečnostních parametrů těchto systémů včetně navazujících právních povinností, kompetencí orgánů veřejné moci, kontroly, sankcí apod. je komplexně provedena zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Toto rozdělení navazuje a zachovává dosavadní regulační rámec a není v současné době důvod do něj zasahovat, neboť uvedené systémy podléhají certifikaci, tj. vyšší formě regulace.

K § X – Vymezení pojmů

Návrh zákona přináší sadu nových pojmů, a to ať už z důvodu jejich převzetí z obsahu směrnice NIS2, nebo z toho důvodu, že návrh zákona svým obsahem navazuje na přístup a pojmosloví obsažené v dosavadním znění zákona o kybernetické bezpečnosti, avšak tento přístup prohlubuje. Nová právní úprava také přichází s použitím některých obecných pojmů, doposud definovaných v některém z prováděcích právních předpisů, ve více prováděcích právních předpisech. Z tohoto důvodu došlo například k přesunutí celé řady pojmů definovaných ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, již na úroveň nového zákona o kybernetické bezpečnosti.

Ustanovení o vymezení pojmů je rozděleno do dvou odstavců, přičemž v rámci prvního odstavce jsou definovány pojmy stanovující základ nové právní úpravy a prostupující napříč celým návrhem zákona a v rámci druhého je pojmový aparát doplněn o další potřebné definice.

V rámci odstavce 1 jsou definovány následující pojmy – aktivum, regulovaná služba, poskytovatel regulované služby a řízení kybernetické bezpečnosti. Vztah mezi těmito pojmy je velmi úzký; poskytovatel regulované služby zajišťuje prostřednictvím řízení kybernetické bezpečnosti aktiva regulované služby.

Aktiva jsou pojem převzatý z dosavadní právní úpravy obsažené ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, přičemž však došlo k jejich přesunutí z úrovně vyhlášky do úrovně zákona. Aktiva tvoří naprostý základ úvah o kybernetické bezpečnosti, resp. jejím řízení, v rámci jakékoliv organizace, a tento pojem tak slouží jako základní stavební kámen pro celý obsah návrhu zákona. Aktivem může být prakticky cokoliv 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 doplněním *„*[...] *relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě“*. Na tomto místě je potřeba zdůraznit, že vyjmenování jednotlivých činností je zde uvedeno pro návodnější orientaci adresáta normy a také, že zastřešující pojem „zpracování“ je v tomto cíleně bezrozporný s definicí zpracování podle obecného nařízení o ochraně osobních údajů, byť zde se samozřejmě nebude jednat jen o zpracování osobních údajů, ale jakýchkoliv informací a dat.

Právě informace a data, stejně tak služby a procesy jsou obsahem definice primárních aktiv. S ohledem na praktické zkušenosti s použitím tohoto zcela stěžejního pojmu se tato definice nově doplňuje také o výslovné uvedení procesů jakožto součástí služby. Toto chápání procesů bylo sice součástí praxe již v rámci dosavadní právní úpravy, a odpovídalo tak běžné praxi na poli kybernetické bezpečnosti, nicméně výslovné uvedení by mělo vést k posílení právní jistoty adresátů.

Vedle primárních aktiv se tímto návrhem nic nemění ani ve vymezení dosavadního pojmu podpůrných aktiv. Právě v případě podpůrných aktiv je nejlépe vidět, že v případě řešení kybernetické bezpečnosti není možné na tento problém pohlížet jen technickým pohledem – nepominutelnou roli mají zaměstnanci a dodavatelé, se kterými je potřeba v rámci řízení

bezpečnosti informací také počítat (dokonce se jedná o jeden z nejčastějších problémů v řešení kybernetické bezpečnosti), a proto mají své zvláštní místo jako jednotlivá aktiva. Dalším typem podpůrného aktiva jsou objekty.

Podmnožinou podpůrných aktiv jsou aktiva technická. Ani zde nedochází oproti dosavadní právní úpravě ke změnám, nicméně po aplikaci poznatků z praxe i v tomto případě dochází k výslovnému uvedení některých typických technických aktiv, jejichž interpretace jako technického aktiva nemusela být vždy na první pohled zřejmá.

Regulovaná služba je stěžejním institutem zákona, od kterého se odvíjí podstatná část činností regulovaných subjektů. Definičním znakem regulované služby je skutečnost, že její narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností. Principiálně tedy musí jít o službu, která je určitým způsobem významná pro celospolečenské fungování a zajištění důležitých společenských nebo ekonomických činností.

Odvětví, ve kterých je třeba regulované služby hledat, stejně jako kritéria pro stanovení regulované služby (ať již její stanovení vyvěrá přímo z právního předpisu, tj, kritéria pro identifikaci regulované služby, nebo je stanovena rozhodnutím Úřadu, tj. kritéria pro určení regulované služby), jsou uvedena v prováděcí vyhlášce k zákonu. Uvedení regulovaných odvětví přímo v textu zákona, jako tomu bylo za předchozí právní úpravy, se v praxi neosvědčilo, neboť neumožňovalo zákonodárci ani Úřadu pružně reagovat na dynamický vývoj společnosti a změny v důležitosti a vlivu jednotlivých odvětví na její fungování. Potřebu této flexibility lze dokumentovat na procesu vyjednávání samotného textu směrnice NIS2, při němž docházelo k živým diskuzím nad okruhem odvětví, která by do její působnosti měla spadat, a výsledný text je třeba chápat především jako kompromis balancující mezi potřebou regulovat všechna podstatná odvětví a objektivní schopností členských států zajistit reálný výkon pravidel obsažených v transpozičních národních předpisech. Okruh odvětví, která mají být tímto zákonem regulována, je tak potřeba do budoucna přizpůsobovat aktuálním společenským potřebám a rovněž potřebám České republiky. Z toho důvodu není vhodné stanovit taxativní výčet regulovaných odvětví zákonem, ale jako přiléhavější se jeví ponechat jejich konkrétní vymezení na prováděcím právním předpisu. Druhým definičním znakem regulované služby je skutečnost, že je poskytována za použití aktiv (viz výše). V dalších částech zákona a v navazujícím prováděcím předpisu pak dochází k definičnímu zpřesnění pojmu a k vydefinování kritérií, při naplnění kterých lze službu považovat za regulovanou.

V neposlední řadě je potřeba na tomto místě uvést, že Úřad vykonává v rámci své činnosti vedle regulace poskytovatelů regulované služby také z evropské legislativy vyplývající funkci tzv. příslušného orgánu PRS v souladu s 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. Tato zkratka „PRS“ je vytvořena z anglických slov „Public Regulated Service“, což je do českého jazyka překládáno jako „veřejně regulovaná služba“. Přestože tedy i tento pojem pracuje se souslovím „(veřejně) regulovaná služba“, je potřeba mít na paměti že se jedná o zcela odlišné instituty a „veřejně regulovaná služba“ souvisí jako pojem výhradně s programem Galileo.

Poskytovatelem regulované služby se orgán nebo osoba stává k okamžiku, kdy se služba, kterou poskytuje, stane regulovanou službou. Ve většině případů se orgán nebo osoba stane poskytovatelem regulované služby okamžikem naplnění kritérií pro identifikaci regulované služby (stanovených prováděcí vyhláškou k zákonu), ve zbylých případech pak dojde k naplnění definičních znaků poskytovatele regulované služby nabytím právní moci rozhodnutí Úřadu o určení regulované služby.

Posledním ze základní čtveřice pojmů uvedených v odstavci 1 je pojem řízení kybernetické bezpečnosti. Tato definice je zastřešujícím pojmem pro činnost směřující k zajištění kybernetické bezpečnosti regulované služby v případě obou režimů poskytovatele regulované služby. Návrh dále počítá s tím, že pokud je řízení kybernetické bezpečnosti vykonáváno poskytovatelem regulované služby v režimu vyšších povinností, označuje se jako systém řízení kybernetické bezpečnosti (zde opět zcela navazuje na dosavadní právní úpravu) a nově zavádí, že pokud je řízení kybernetické bezpečnosti vykonáváno poskytovatelem regulované služby v režimu nižších povinností, označuje se jako zajišťování minimální úrovně kybernetické bezpečnosti. Podstatou tohoto nadřazeného pojmu je tedy označit jednotícím pojmem sadu činností, které podle návrhu zákona poskytovatel regulované služby vykonává, především pro potřeby stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby podle návrhu zákona, což je zcela klíčová povinnost pro plnění navazujících povinností poskytovatelem regulované služby v obou režimech.

Na vymezení pojmů v rámci odstavce 1 navazují v odstavci 2 další doplňující definice.

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 aktivy 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. I zde nicméně dochází k drobné úpravě reflektující používání pojmu „zpracování“ v kontextu předpisů regulujících ochranu osobních údajů, který je obecně přejímán a využíván i v tomto návrhu zákona v případě zákonné definice aktiv (nicméně i zde platí výše uvedené, tedy že tento pojem se nepoužije jen vůči osobním údajům, ale aktivům obecně). Nově je tedy jednoznačně deklarováno, že i vznik a výměna informací a dat je součástí širšího pojmu zpracování.

Bezpečnost informací je běžně užívaný pojem, který v rámci tohoto návrhu nedoznal žádných praktických změn oproti dosavadní právní úpravě a opět se jedná o jeho převzetí z původního zákona o kybernetické bezpečnosti. Pojem bezpečnosti informací vychází ve své definici z významu tohoto pojmu v odvětví informačních věd a týká se důvěrnosti (tj. diskrece), jednoty (tj. integrity) a dostupnosti informace. Pojem se netýká obsahu informace, ale pouze funkčnosti prostředí, v němž je informace tvořena, zpracovávána, uchovávána a komunikována. To odpovídá také principu technologické neutrality.

V případě pojmu kybernetická hrozba a významná kybernetická hrozba se jedná o pojmy převzaté zcela z obsahu směrnice NIS2. Jejich význam v rámci návrhu zákona spočívá především pro jejich využití v rámci ustanovení o dobrovolném hlášení a v případě významné kybernetické hrozby pro významové odlišení od běžných hrozeb pro potřeby plnění informační povinnosti poskytovatele regulované služby vůči uživatelům.

Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident jsou definicemi, které byly převzaty z dosavadní právní úpravy a s ohledem na zavedení pojmu aktiva na úroveň zákona doznaly jazykových úprav. Rozdělení skutkových stavů, na něž zákon reaguje konstrukcí specifických povinností, na kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty, sleduje účel odlišení potenciálně problematických situací vykazujících stanovené formální znaky a situací, které na základě vyhodnocení formálních podmínek v kontextu aktuálních okolností, představují reálné bezpečnostní riziko. Zatímco kybernetickou bezpečnostní událostí je událost bez reálného negativního následku, kybernetickým bezpečnostním incidentem je pak samotné narušení bezpečnosti informací s negativním

dopadem. Cizojazyčný pojem „incident“ byl použit z důvodu zachování kontinuity a souladu zákonného pojmového aparátu s mezinárodní technickou terminologií. Nově se zavádí pojem významná kybernetická bezpečnostní událost, která je za prvé zohledněním obsahu směrnice NIS2, ale za druhé také zohledněním požadavků z praxe.

Poslední definicí obsaženou v odstavci 2 a týkající se kybernetických bezpečnostních incidentů je pojem zvládání kybernetického bezpečnostního incidentu. S tímto pojmem sice dosavadní právní úprava pracovala, nicméně jej definovala opisem různých činností bez zakotvení jednotné definice. Návrh zákona tak tento pojem přebírá a nově jednotně definuje jako soubor činností k zajištění všech dílčích kroků před, během i po výskytu incidentu. Tento pojem se vztahuje jak na činnosti poskytovatele regulované služby, resp. jakéhokoliv orgánu nebo osoby u které se vyskytl kybernetický bezpečnostní incident, ale také na zapojení dalších organizací do řešení dané situace – typicky např. Vládního nebo Národního CERT.

Definice významného dodavatele je dalším z pojmů převzatých z dosavadní právní úpravy a dalším z pojmů, které jsou tímto návrhem zákona přeneseny z prováděcích právních předpisů na zákonnou úroveň. Význam této změny je především ten, že dochází ke zrušení pojmu „provozovatel informačního nebo komunikačního systému“ a je tedy nutné již na úrovni zákona pracovat s pro kybernetickou bezpečnost relevantními dodavateli povinných osob. Významnými dodavateli jsou tak ti dodavatelé, kteří jsou s poskytovatelem regulované služby v právním vztahu a plněním z něj vyplývajících povinností mají vliv na kybernetickou bezpečnost. V praxi se může jednat o poskytovatele klíčových služeb, ale i o dodavatele primárních nebo podpůrných (především technických) aktiv. Na základě poznatků praxe je potřeba na tomto místě deklarovat, že z povahy věci se v případě zmíněného „právního vztahu“ jedná o právní vztah dodavatelský a nikoli zaměstnanecký. Zaměstnanec v daném vztahu k poskytovateli regulované služby není významným dodavatelem.

K § X – Kritéria regulované služby

Službu lze považovat za regulovanou při splnění kritérií regulované služby. Tato kritéria rozvíjí definici regulované služby obsaženou v ustanovení zákona věnovaném definicím a vymezují, které služby a ve kterých odvětvích jsou považovány za takové, jejichž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností. Pojetí kritérií regulovaných služeb vychází z předchozí úpravy identifikace provozovatelů základních služeb a prováděcí vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, oproti předchozí úpravě je však stanoven odlišný způsob použití těchto kritérií při zařazování orgánů a osob do regulace. Cílem nového pojetí identifikace povinných subjektů vycházejícího ze směrnice NIS2 je odstranit značné rozdíly mezi členskými státy v určování povinných subjektů a zajistit právní jistotu pro všechny regulované orgány a osoby, pokud jde o opatření k řízení kybernetických bezpečnostních rizik a oznamovací povinnosti. Za tím účelem stanoví směrnice NIS2 základní jednotné kritérium (velikost podniku), které určí subjekty, jež spadají do oblasti působnosti této směrnice. Subjekty, které naplňují definovaná velikostní kritéria (tedy jsou středními a velkými podniky) a které působí v odvětvích nebo poskytují druhy služeb nebo vykonávají činnosti, na něž se vztahuje směrnice NIS2, mají být do regulace zařazeny automaticky. Členské státy by pak měly rovněž stanovit, že do oblasti působnosti směrnice NIS2 spadají některé malé podniky a mikropodniky, které splňují zvláštní kritéria poukazující na klíčovou úlohu pro společnost, ekonomiku, nebo pro konkrétní odvětví či druhy služeb.

Návrh zákona v návaznosti na požadavky směrnice NIS2 rozlišuje dva druhy kritérií regulované služby – kritéria pro identifikaci regulované služby a kritéria pro určení regulované služby. Kritéria pro identifikaci regulované služby slouží pro potřeby tzv. samoidentifikace, tedy procesu, při kterém orgán nebo osoba sama posoudí, zda kritéria naplňuje či nikoli,

a v případě kladného posouzení se registruje u Úřadu jako poskytovatel regulované služby a začne plnit své zákonné povinnosti. Regulovanou službou se služba naplňující kritéria pro identifikaci regulované služby stává ze zákona, bez nutnosti dalšího jednání ze strany Úřadu. S ohledem na široký záběr kritérií (která vycházejí z příloh směrnice NIS2) lze předpokládat, že většina poskytovatelů regulované služby bude do regulace kybernetické bezpečnosti zařazena právě na základě naplnění kritérií pro identifikaci regulované služby.

Kritéria pro určení regulované služby představují dodatečná kritéria, na základě kterých může Úřad určit svým rozhodnutím službu jako regulovanou. Principiálně půjde o kritéria zohledňující důležitost subjektu pro celou společnost nebo určité odvětví. Naplnění kritérií pro určení regulované služby bude zkoumáno v rámci správního řízení, obdobně jako tomu bylo za účinnosti zákona č. 181/2014 Sb. při určování provozovatelů základní služby. Povinnosti pak poskytovateli regulované služby plynou až od pravomocného skončení řízení a zavedení orgánu nebo osoby do evidence poskytovatelů regulované služby.

Ačkoli to není v návrhu zákona výslovně stanoveno, tento zákon se vztahuje na poskytovatele regulované služby a subjekty poskytující služby registrace doménových jmen usazené v rámci České republiky nebo poskytující na území České republiky své služby. Uplatní se tak obecné pravidlo, že subjekt, který operuje na území České republiky, je povinen se při poskytování svých služeb na tomto území řídit českými platnými právními předpisy.

Pojem usazení byl zaveden již předchozí směrnicí NIS, 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 Evropské unie 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 Evropské unie za současného zachování původního sídla v jiném členském státě. Směrnice NIS2 zavedený pojem usazení bez dalšího přejímá. I pro potřeby tohoto 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 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 Evropské unie k výkladu svobody usazování přesně definována, může se tak jednat o kancelář, provozovnu, pobočku apod. Stěžejním je požadavek na fyzickou přítomnost daného subjektu na území předmětného státu.

V praxi pak bude běžné, že jedna osoba bude usazena ve více státech Evropské unie současně.

Speciální režim je stanoven pro poskytování služeb systému doménových jmen na internetu (DNS), správy a provozu registru internetových domén nejvyšší úrovně, cloud computingu, služeb datového centra, sítí pro doručování obsahu (CDN), on-line tržiště, internetového vyhledávače, služby platformy sociální sítě, poskytování řízené služby (MSP) a řízené bezpečnostní služby (MSSP) a služby registrace doménových jmen v případě, že jsou poskytovány fyzickou nebo právnickou osobou se sídlem v jiném členském státě. Pro tyto subjekty platí, že spadají do plné dozorové pravomoci dozorového orgánu toho členského státu, ve kterém mají umístěnu svou hlavní provozovnu. Pokud mají tyto subjekty umístěnu svou hlavní provozovnu v jiném členském státě, platí, že jsou poskytovateli regulované služby v příslušných odvětvích, resp. osobami, kterým se ukládají povinnosti v souvislosti s poskytováním služeb registrace doménových jmen, podle tohoto zákona, nicméně dozorová

pravomoc Úřadu je omezena pouze na situace, kdy je Úřad o výkon dozorových pravomocí dožádán dozorovým orgánem členského státu, ve kterém má osoba umístěnu hlavní provozovnu nebo ve které má ustaveného svého zástupce.

K § X – § Y – Režim poskytovatele regulované služby a Režim poskytovatele regulované služby v případě poskytování více regulovaných služeb jedním poskytovatelem

Návrh zákona zavádí nový institut, který je stěžejní pro plnění povinností poskytovatele regulované služby, a tím je institut tzv. režimů poskytovatele regulované služby.

Jeho podstatou je, že všichni poskytovatelé regulované služby, ať už se poskytovateli stanou pro jakoukoliv z regulovaných služeb nebo pro jakékoliv množství regulovaných služeb, jsou následně rozděleni do dvou skupin a každému z nich je přiřazen jeden režim. Režim podle prvního odstavce tohoto ustanovení následně určuje, jaké povinnosti budou muset poskytovatelé regulované služby plnit vůči všem službám, pro které naplnili kritéria. V souladu s druhým odstavcem tohoto ustanovení jsou předmětné režimy označeny jako tzv. režim vyšších povinností a režim nižších povinností.

Koncept režimů má svůj základ ve směrnici NIS2, která povinné osoby rozděluje do dvou skupin, tzv. „základních subjektů“ a „důležitých subjektů“. K tomuto rozdělení z pohledu povinností směrnice uvádí zejména: *„Subjekty spadající do oblasti působnosti této směrnice pro účely dodržování opatření k řízení kybernetických bezpečnostních rizik a oznamovacích povinností by měly být zařazeny do dvou kategorií: základní subjekty a důležité subjekty, s přihlédnutím k míře kritické důležitosti, pokud jde o odvětví nebo druh služby, kterou poskytují, a také k jejich velikosti. V této souvislosti by se v případě potřeby měla náležitě zohlednit veškerá relevantní odvětvová posouzení rizik nebo pokyny příslušných orgánů. Dohledové a donucovací režimy pro tyto dvě kategorie subjektů by se měly odlišovat, aby byla zajištěna spravedlivá vyváženost mezi požadavky a povinnostmi založenými na riziku na jedné straně a správní zátěží vyplývající z dohledu nad dodržováním směrnice na druhé straně.“.* Zmíněná potřeba zohlednit výše uvedené skutečnosti vede k tomu, že návrh zákona rozděluje poskytovatele regulovaných služeb do dvou skupin – režimů. Ve vyšším režimu jsou subjekty, které poskytují alespoň jednu z regulovaných služeb odpovídající povaze regulace „základních subjektů“ v souladu se směrnicí, případně další subjekty, o kterých tak v souladu se směrnicí nebo nad rámec směrnice stanoví národní právní úprava. V režimu nižších povinností jsou pak subjekty, které neposkytují žádnou službu ve vyšším režimu a u nichž ani na základě žádného dalšího pravidla uvedeného v návrhu zákona nedošlo k jejich převedení do režimu vyšších povinností. Zpravidla se tak bude jednat o subjekty odpovídající povaze regulace „důležitých subjektů“ v souladu se směrnicí NIS2.

Návrh zákona zohledňuje výše uvedené tím způsobem, že podle odstavce tři jsou režimy přiřazeny jednotlivým regulovaným službám tak, jak je dále upřesněno prováděcím právním předpisem.

Pokud by tedy poskytovatel regulované služby vykonával jen jednu regulovanou službu ze všech služeb, které jsou uvedeny v prováděcím právním předpise, je jeho režim dán režimem, který na základě prováděcího právního předpisu vyhodnotí.

Nad rámec základního rozdělení režimů stanoveného prováděcím předpisem může Úřad svým rozhodnutím změnit režim poskytovatele regulované služby a převést jej do režimu vyšších povinností, pokud jsou pro to dány důvody spočívající zejména ve zvláštní důležitosti organizace pro celou Českou republiku nebo konkrétní odvětví. Kritéria pro zařazení organizace do vyššího režimu jsou dány prováděcím právním předpisem a odpovídají kritériím pro určení regulované služby. Jakmile důvody pro zvýšení režimu pominou, Úřad vydá rozhodnutí o pominutí důvodů pro změnu režimu.

Pokud by poskytovatel regulované služby vykonával dvě a více regulovaných služeb podle prováděcího právního předpisu, je pro stanovení jeho režimu nutno zohlednit ještě obsah ustanovení v zákoně, které takovou situaci řeší. Předmětné ustanovení upravující režim poskytovatele regulované služby v případě poskytování více regulovaných služeb říká, že poskytovatel regulované služby, jehož regulované služby neodpovídají všechny stejnému režimu (tj. nestanovují všechny jen režim nižších povinností, nebo jen režim vyšších povinností), a tudíž alespoň jedna regulovaná služba odpovídá podle prováděcího právního předpisu režimu vyšších povinností a alespoň jedna odpovídá režimu nižších povinností, musí ke všem regulovaným službám přistupovat z pohledu režimu vyšších povinností.

Praktický příklad přibližující výše popsanou situaci: Společnost X po vyhodnocení kritérií v prováděcím právním předpisu zjistí, že se jí týká regulace tří služeb – služby A, služby B a služby C. Prováděcí právní předpis stanovil, že kritériím, které ve vyhlášce společnost X naplňuje, odpovídá u služeb A a B režim nižších povinností, ovšem u služby C zařazuje společnost do režimu vyšších povinností. Výše popsané ustanovení v návrhu zákona však stanoví, že společnost X může mít stanoven pouze jeden režim povinností, společnost proto bude postupovat a zavádět povinnosti vůči službám A, B i C tak, jako by byly všechny v režimu vyšších povinností již podle prováděcího právního předpisu. Pokud by společnost X službu C neposkytovala, poskytování služeb A a B by vedlo ke stanovení jejího režimu na režim nižších povinností.

Právní fikce zavádějící výše zmíněné pravidlo je zásadní pro správné fungování pravidel plynoucích ze zákona, především pro zavádění a provádění bezpečnostních opatření, ale i hlášení kybernetických bezpečnostních incidentů v regulovaném subjektu. Tato pravidla se totiž použijí napříč organizací a v rámci obou režimů jsou odlišná. Pokud by se režim v organizaci nesjednotil na úrovni zákona, došlo by k tomu, že by organizace měla povinnost postupovat podle dvojí sady pravidel a zavádět na různé množiny různě se překrývajících aktiv různé povinnosti, které by se zdvojovaly či si dokonce odporovaly. Nezavedení jednotného režimu dané organizace by ztížilo praktické zavádění uložených povinností a plnění zákonných požadavků by v praxi výrazně zkomplikovalo či učinilo nepoužitelným. Doporučení „best practice“ navíc především v případě bezpečnostních opatření ukazují, že nejlepším přístupem je zavádět jednotná pravidla napříč organizací, neboť obecně platí, že čím více pravidel a výjimek je stanoveno, tím nižší bezpečnost potenciálně je.

K § X – Registrace poskytovatele regulované služby

Návrh rozlišuje tři samostatné úkony vedoucí k zařazení poskytovatele regulované služby do regulace a zahájení plnění jeho povinností – registraci poskytovatele regulované služby, zápis do evidence poskytovatelů regulovaných služeb a vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb. Každý z těchto úkonů má svůj specifický význam a napomáhá k lepšímu fungování celé regulace.

Jakmile orgán nebo osoba naplní definiční znaky poskytovatele regulované služby, je potřeba jej jako poskytovatele regulované služby zaregistrovat u Úřadu. V závislosti na způsobu zařazení do regulace, tedy zda došlo k naplnění kritérií pro identifikaci regulované služby a samoidentifikaci poskytovatelem regulované služby, nebo k určení regulované služby rozhodnutím Úřadu na základě naplnění kritérií pro určení regulované služby, provede registraci buďto sám poskytovatel regulované služby, nebo Úřad.

Provedení registrace navazující na naplnění kritérií pro identifikaci regulované služby (samoidentifikaci) je zákonnou povinností poskytovatele regulované služby, která není vázána na žádnou notifikaci ze strany Úřadu. Orgán nebo osoba si tak musí aktivně posoudit, zda kritéria naplňuje či nikoli, a podle toho dále jednat. Kritéria pro identifikaci regulované služby budou stanovena prováděcím předpisem a ve většině případů půjde o jednoduše vyhodnotitelná

binární kritéria (mnohdy vázaná na držení licence nebo povolení k poskytování služby). V komplikovanějších případech bude možné využít podpůrných materiálů Úřadu a *ad hoc* konzultací. Posouzení naplnění kritérií pro identifikaci regulované služby by měly orgány a osoby provést (či alespoň zahájit) nejlépe ihned po zveřejnění platného znění zákona a prováděcího předpisu ve Sbírce zákonů, tedy v době určené pro seznámení se s novou právní úpravou. Pro vlastní provedení registrace návrh zákona stanoví subjektivní lhůtu 30 dnů ode dne, kdy poskytovatel regulované služby zjistí, že jím poskytovaná služba naplňuje kritéria pro identifikaci regulované služby, resp. objektivní lhůtu 90 dnů ode dne, kdy k naplnění kritérií pro identifikaci regulované služby došlo (pro mnoho subjektů tato lhůta začne běžet okamžikem nabytí účinnosti zákona). Vzhledem k relativní jednoduchosti kritérií pro identifikaci regulované služby a nenáročnosti navrhovaného procesu registrace by měly být navrhované registrační lhůty plně dostačující i pro subjekty s komplikovanější organizační strukturou.

Úřad může registraci provést sám v případě, že poskytovatel regulované služby naplňující kritéria pro identifikaci regulované služby nesplní svou zákonnou povinnost zaregistrovat se v zákonné lhůtě a Úřad se o naplnění kritérií dozví z vlastní činnosti (čímž není dotčena odpovědnost poskytovatele regulované služby za spáchání přestupku, kterým nesplnění registrační povinnosti je). Úřad k tomuto kroku přistoupí ve chvíli, kdy bude zřejmé naplnění kritérií pro identifikaci regulované služby.

Povinnost provést registraci se vztahuje i na orgány a osoby naplňující kritéria pro identifikaci regulované služby, které byly před nabytím účinnosti zákona povinnými osobami podle § 3 písm. c) až g) zákona č. 181/2014 Sb (dosavadního zákona o kybernetické bezpečnosti). Úřad sice disponuje kontaktními údaji těchto osob, jejich rozsah je nicméně odlišný od požadavků navrhovaného zákona a nadto může u těchto osob dojít k rozšíření regulovaných služeb oproti službám, pro které byly určeny nebo identifikovány povinnou osobou podle zákona č. 181/2014 Sb. (další významnou změnou bude i přechod od regulace konkrétních informačních systémů k regulaci celé organizace). Z toho důvodu tyto osoby nepřechází do regulace nového zákona automaticky, ale stejným způsobem jako dosud neregulované subjekty. Pro dosavadní povinné osoby je nicméně stanoveno přechodné ustanovení zajišťující kontinuitu zajišťování kybernetické bezpečnosti po dobu plynutí lhůty pro zahájení plnění povinností podle nového zákona.

Registraci orgánů a osob, u nichž došlo rozhodnutím Úřadu k určení regulované služby na základě naplnění kritérií pro určení regulované služby, zajišťuje sám Úřad. S těmito subjekty bylo vedeno správní řízení o určení regulované služby a Úřad tak již všemi informacemi nezbytnými pro registraci poskytovatele registrované služby disponuje. Z toho důvodu není třeba poskytovatele regulované služby dále zatěžovat a vyžadovat po nich duplicitní hlášení informací. Tím však není dotčena povinnost určeného poskytovatele regulované služby nahlásit Úřadu kontaktní a další údaje, neboť těmi Úřad po provedení řízení o určení zpravidla disponovat nebude (nebo nebudou předmětem jeho zkoumání).

Registrace se provádí prostřednictvím Portálu NÚKIB vyplněním registračních údajů. Podrobnosti k fungování Portálu NÚKIB, ke způsobu přihlášení do portálu a k rozsahu informací, které se v rámci registrace vyplňují, stanoví prováděcí právní předpis.

Registrace slouží primárně jako prostředek identifikace povinné osoby vůči Úřadu (většina poskytovatelů regulované služby bude do regulace zařazena na základě naplnění kritérií pro identifikaci regulované služby, a Úřad tak s většinou regulovaných osob nepovede žádné řízení o určení) a představuje transpozici notifikační povinnosti podle čl. 3 odst. 4 směrnice NIS2. Provedení registrace není okamžikem rozhodným pro zahájení běhu lhůt pro plnění povinností poskytovatele regulované služby, tím je až vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb. Předmětem registračních údajů tak budou především

základní informace o povinné osobě a informace o poskytovaných regulovaných službách. Další informace, zejména o používaných informačních systémech, budou předmětem navazujícího hlášení údajů (není však vyloučeno, aby poskytovatel regulované služby v rámci registrace poskytl i informace vyžadované v rámci hlášení údajů).

V případě, kdy dojde k naplnění kritérií pro samoidentifikaci poskytovatele regulované služby, se registrace provádí u prvního naplnění definičních znaků poskytovatele regulované služby, resp. za situace, kdy poskytovatel regulované služby dosud není veden v evidenci poskytovatelů regulované služby pro žádnou regulovanou službu (ať již z důvodu, že dosud žádnou neposkytoval, nebo z důvodu, že byl z evidence v minulosti vymazán). V případě, že je poskytovatel regulované služby v evidenci již veden a naplní kritéria regulované služby pro další službu, která dosud nebyla zaregistrována, postupuje se podle ustanovení upravujícího změnu registrace poskytovatele regulované služby.

V případě, kdy dojde k určení první či další regulované služby rozhodnutím Úřadu na základě naplnění kritérií pro určení regulované služby, provádí registraci podle odst. 4 samotný Úřad. Není proto třeba rozlišovat mezi registrací a změnou registrace.

Pokud na základě rozhodnutí Úřadu dojde ke změně režimu, provede tuto změnu režimu podle odst. 5 Úřad. V případě, že v důsledku rozhodnutí Úřadu dojde ke zrušení povýšení režimu poskytovatele regulované služby, a tedy ke změně režimu povinností z vyššího na nižší, nové lhůty běžet nepočínají, neboť poskytovateli regulované služby povinnosti ubývají, nikoli přibývají (požadavky nižšího režimu budou vždy součástí množiny požadavků vyššího režimu, poskytovatel regulované služby tedy jen omezí rozsah svých bezpečnostních opatření a dalších povinností na tuto nižší úroveň).

K § X – Změna registrace poskytovatele regulované služby

Proces změny registrace poskytovatele regulované služby slouží pro změnu registrovaných údajů, resp. pro zaregistrování nových regulovaných služeb u již evidovaného poskytovatele regulované služby nebo změnu režimu zaregistrovaných regulovaných služeb, kteří se do regulace dostali na základě naplnění kritérií pro samoidentifikaci poskytovatele regulované služby.

Důvodem pro oddělení změny registrace od samotné registrace je praktické zjednodušení fungování Portálu NÚKIB. Proces změny registrace je v zásadě totožný s procesem prvotní registrace, i zde tak platí subjektivní 30-denní, resp. objektivní 90-denní lhůta pro nahlášení registračních údajů a rozdělení odpovědností za nahlášení registračních údajů. Rozdíl je však v tom, že změnu registrace provádí samotný poskytovatel regulované služby jakožto přihlášený uživatel Portálu NÚKIB, přičemž k tomu využije zjednodušený formulář pro změnu registrace. Vyplnění registračních údajů v rozsahu potřebném pro prvotní registraci v tomto případě není nutné, vzhledem k tomu, že poskytovatel regulované služby je v evidenci již zapsán. Obdobně je pak rozdělena povinnost provést změnu registrace v případě změny režimu poskytovatele regulované služby. Změna se provádí prostřednictvím Portálu NÚKIB. Na změnu registrace navazuje povinnost vůči novým službám a novým režimům nahlásit kontaktní údaje.

Registrací nové regulované služby nebo změny režimu u již registrované regulované služby z nižšího na vyšší počínají vůči těmto službám běžet nové lhůty pro zahájení plnění povinností. Naopak při změně režimu poskytovatele regulované služby z vyššího na nižší nové lhůty běžet nepočínají, neboť poskytovateli regulované služby povinnosti ubývají, nikoli přibývají (požadavky nižšího režimu budou vždy součástí množiny požadavků vyššího režimu, poskytovatel regulované služby tedy jen omezí rozsah svých bezpečnostních opatření a dalších povinností na tuto nižší úroveň).

K § X – Zápis do evidence poskytovatelů regulované služby

Jakmile je poskytovatel regulované služby zaregistrován prostřednictvím Portálu NÚKIB, Úřad jej a jím poskytované regulované služby bezodkladně zapíše do evidence poskytovatelů regulovaných služeb. Obdobně Úřad postupuje i po provedení změny registrace. Evidence poskytovatelů regulovaných služeb slouží jako databáze regulovaných osob, obdobně jako tomu bylo u evidence kontaktních údajů podle zákona č. 181/2014 Sb. Evidence je neveřejná, slouží potřebám Úřadu a informace v ní vedené se neposkytují ani podle předpisů upravujících svobodný přístup k informacím (viz odůvodnění k ustanovení o výjimce z práva na informace a evidencím vedených Úřadem).

Zápis do evidence bude v zásadě automaticky prováděným úkonem, Úřad bude provádět pouze formální kontrolu registrovaných údajů (např. duplicity hlášení, zjevných chyb v registrovaných údajích, nesouladů s informacemi z registrů apod.). Prodlení mezi registrací a zápisem do evidence by tedy mělo být minimální. O provedení zápisu do evidence poskytovatelů regulovaných služeb Úřad zapsaného poskytovatele písemně vyrozumí. Písemné vyrozumění o zápisu do evidence musí být poskytovateli regulované služby doručeno. Těm poskytovatelům regulované služby, kteří mají zřízenu datovou schránku, bude vyrozumění doručeno do datové schránky. Zbylým subjektům bude doručováno v souladu s pravidly zákona č. 500/2004 Sb., správního řádu.

Vyrozumění je stěžejním dokumentem pro počítání lhůt pro zahájení plnění zákonných povinností. Teprve od tohoto okamžiku poskytovateli počínají běžet lhůty pro zavádění bezpečnostních opatření, hlášení incidentů, plnění protiopatření Úřadu a dalších povinností upravených zákonem pro jednotlivé zapsané regulované služby. Od tohoto okamžiku je také poskytovatel regulované služby odpovědný za případné přestupky proti tomuto zákonu, kterých se neplněním svých povinností dopustí (s výjimkou odpovědnosti za přestupek spočívající v nesplnění povinnosti registrace nebo změny registrace, která nastupuje uplynutím lhůt pro registraci nebo změnu registrace). Jednoznačné určení okamžiku, od kterého je poskytovatel regulované služby odpovědný za plnění svých zákonných povinností, má za cíl odstranit problémy spojené s předchozí regulací významných informačních systémů (u nichž se také uplatnila samoidentifikace), kdy bylo v mnoha případech obtížné určit, ke kterému okamžiku se informační nebo komunikační systém stal významným informačním systémem a jeho správce nebo provozovatel povinnou osobou podle § 3 písm. e) zákona č. 181/2014 Sb. Úřad tak bude díky navrhované úpravě schopen zejména v přestupkových řízení zcela jednoznačně stanovit, od kterého okamžiku poskytovateli regulované službě vznikla povinnost řídit se zákonem a plnit povinnosti v něm obsažené a kdy byl projednávaný přestupek spáchán.

Za účelem zachování právní jistoty adresátů normy i dalších osob, které jsou s nimi v právních vztazích relevantních z hlediska regulovaných služeb, je stanoveno, že poskytovatelé regulované služby jsou povinni plnit povinnosti dané zákonem po celou dobu svého zápisu v evidenci poskytovatelů regulovaných služeb, a to až do okamžiku doručení vyrozumění o výmazu z evidence poskytovatelů regulovaných služeb. Prakticky tak jde o nevyvratitelnou právní domněnku, že poskytovatel regulované služby zapsaný v evidenci poskytovatelů regulovaných služeb naplňuje definiční znaky poskytovatele regulované služby (jím poskytované zapsané regulované služby naplňují kritéria regulované služby), dokud není Úřadem deklarován opak. Navrhované ustanovení má za cíl zajistit, že osoby, které se nesprávně domnívají, že jimi poskytované služby nenaplňují kritéria regulované služby, nepřestanou i přes svůj zápis v evidenci plnit povinnosti dané zákonem. Současně je i v zájmu Úřadu, aby v evidenci poskytovatelů regulované služby nebyly zapsány orgány a osoby nebo jimi poskytované služby, které skutečně kritéria pro zařazení do regulace nesplňují. U takových služeb a orgánů a osob Úřad bez zbytečného odkladu zahájí kroky vedoucí k výmazu orgánů a osob nebo jednotlivých služeb z evidence poskytovatelů regulované služby.

K § X – Hlášení údajů poskytovatelem regulované služby

Tato povinnost spolu s registrací poskytovatelů regulovaných služeb v zásadě odpovídá hlášení kontaktních údajů dle § 16 původního zákona o kybernetické bezpečnosti. Kromě tvorby znalostní báze Úřadu a získávání přehledu o jednotlivých množinách regulovaných entit jde také o nastavení nezbytných komunikačních kanálů s jednotlivými poskytovateli regulovaných služeb tak, aby s nimi Úřad případně mohl řešit potenciální hrozby či incidenty a obracel se přitom v rámci dané organizace na relevantní osoby. Hlášení relevantních údajů přitom bude probíhat prostřednictvím Portálu NÚKIB (viz blíže ustanovení o Portálu NÚKIB.

Odst. 2 specifikuje jednotlivé množiny hlášených údajů, které jsou blíže specifikovány ve vyhlášce o Portálu NÚKIB. K hlášení registračních údajů přitom dochází již při prvotní registraci poskytovatele regulované služby, k hlášení ostatních údajů musí dle odst. 3 dojít nejpozději do 30 dnů od doručení vyrozumění o zápisu relevantní regulované služby do evidence poskytovatelů regulovaných služeb, tedy od dokončení registrace.

Odst. 4 pak zakotvuje povinnost hlášení veškerých změn ve lhůtě 10 dní, tak aby byly hlášené údaje udržovány úplné a aktuální, u referenčních údajů vedených v základních registrech se přitom předpokládá automatická aktualizace. Odpovědnost poskytovatele regulované služby za úplnost a aktuálnost nahlášených údajů je dále akcentována v odst. 6.

Odst. 5 pouze zdůrazňuje důležitost dostupnosti poskytovatele regulovaných služeb, nemělo by tak docházet k situacím, kdy budou pověřené kontaktní osoby nedostupné a bez jakéhokoliv zástupu. Takový stav by komplikoval, resp. znemožňoval, efektivní komunikaci ze strany Úřadu vůči danému poskytovateli regulovaných služeb, což by například v souvislosti s probíhajícím incidentem mohlo mít závažné důsledky. Konkrétní počet kontaktních osob není určen, jelikož bude souviset s velikostí a kapacitami regulované organizace, případně počtem regulovaných služeb. Absolutním minimem by však vždy měly být dvě až tři kontaktní osoby.

Odst. 7 pak odkazuje na vyhlášku o Portálu NÚKIB, kde jsou podrobně upraveny jednotlivé kategorie hlášených údajů, včetně způsobu provádění souvisejících úkonů.

K § X – Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby

Základem řízení kybernetické bezpečnosti je správné stanovení jeho rozsahu pomocí identifikace organizačních částí a aktiv. Na tuto povinnost jsou navázány další požadavky zákona o kybernetické bezpečnosti a jeho prováděcích právních předpisů. Stěžejní je především to, že stanovený rozsah definuje, kde mají být zaváděna bezpečnostní opatření. Neplnění požadavku na stanovení rozsahu nebo jeho nedostatečné stanovení již podle dosavadní právní úpravy představuje zásadní problém, který Úřad při kontrolách prováděných dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, identifikoval. Z toho důvodu v rámci návrhu zákona došlo k podrobné úpravě postupu identifikace rozsahu. Cílem je zpřesnit a v praxi zjednodušit poskytovateli regulované služby stanovení rozsahu, přičemž poskytovatelé regulované služby, kteří měli rozsah stanoven správně v souladu s požadavky dosavadního zákona č. 181/2014 Sb., o kybernetické bezpečnosti, by měli při stanovení rozsahu dle tohoto zákona dojít ke stejnému výsledku.

Dle odst. 1 poskytovatel regulované služby nejprve pohlíží na organizaci jako na celek, identifikuje všechna primární aktiva (neboli jím zpracovávané a poskytované služby a informace), díky čemuž o nich získá přehled. Následně z nich určí ta primární aktiva, která souvisejí s poskytováním regulované služby (a pro tuto množinu primárních aktiv dále identifikuje a určí organizační části a podpůrná aktiva). Organizační části představují vybrané organizační celky poskytovatele regulované služby, které se např. podílí na zajišťování fungování regulované služby či jsou její uživatelé. V praxi se tak může jednat o celou organizaci

nebo o vybrané relevantní části organizace např. specifické úseky či oddělení. Ostatní primární aktiva, která s regulovanou službou nesouvisejí, může z rozsahu vyjmout, avšak toto své rozhodnutí musí řádně zdůvodnit. Dále toto ustanovení ukládá povinnost vést o všech krocích dokumentovaný záznam, tedy o stanovení rozsahu vč. primárních aktiv, která byla z rozsahu vyjmuta, a odůvodnění jejich vyjmutí. Dokumentování rozsahu je důležité z hlediska jeho zpětného přezkoumání a zároveň je tím zajištěno, že rozsah bude vnímán jednotně napříč celou organizací.

Vzhledem k tomu, že je stanovení rozsahu řízení kybernetické bezpečnosti zcela klíčovou povinností, jelikož je nutnou prerekvizitou pro řádné plnění dalších požadavků podle tohoto zákona a jeho prováděcích právních předpisů, a také proto, že byly identifikovány časté nedostatky při stanovení rozsahu, došlo k doplnění odst. 4, který popisuje výchozí stav rozsahu řízení kybernetické bezpečnosti. Výchozí stav do rozsahu řízení kybernetické bezpečnosti zahrnuje, jak regulovanou službu poskytovatele regulované služby, tak podpůrná aktiva celé organizace a další aktiva související s poskytováním regulované služby. Přičemž je zdůrazněno, že kromě aktiv organizace do rozsahu řízení kybernetické bezpečnosti patří i externí aktiva jako např. dodavatelé, která je nutné do rozsahu řízení kybernetické bezpečnosti rovněž zahrnout. Tento výchozí stav může budit dojem, že je nastaven příliš široce, je však pouhou fikcí, která se při plnění požadavku odst. 1 zákona nepoužije. Navíc bez identifikace primárních aktiv a organizačních částí včetně určení těch, které souvisí s poskytováním regulované služby nelze žádná primární aktiva a organizační části z rozsahu vyloučit. Podpůrná aktiva (kterými se rozumí zaměstnanci, dodavatelé, objekty a technická aktiva) mají na rozdíl od zbylých aktiv fyzickou příp. hmatatelnou podobu, jejich existence je tedy jednoznačná. Avšak bez identifikovaných primárních aktiv a určení souvislostí mezi regulovanou službou, primárními a podpůrnými aktivy rovněž nelze žádná podpůrná aktiva z rozsahu řízení kybernetické bezpečnosti vyloučit. Přímo na identifikaci aktiv kromě stanovení rozsahu řízení kybernetické bezpečnosti navazuje celá řada dalších povinností, a proto je v praxi podmíněno plnění těchto navazujících povinností provedením činností popsaných v odst. 1. V případě správného plnění alespoň jedno z těchto navazujících požadavků, by vždy mělo dojít k tomu, že budou povinnosti podle odst. 1 splněny – tzv. fikce uvedená v odst. 4 se tedy nepoužije.

Za úplné stanovení rozsahu řízení kybernetické bezpečnosti je považován okamžik, kdy je jeho stanovení řádně a prokazatelně dokumentováno a evidováno dle odst. 3.

Obdobným způsobem je fikce uplatněna v odst. 5, který stanovuje, že všechna nově pořízená či nabytá aktiva organizace (tedy primární či podpůrná aktiva pořízená či nabytá po splnění povinnosti dle odst. 1 nebo uplatnění fikce dle odst. 4), jsou součástí rozsahu řízení kybernetické bezpečnosti, dokud nejsou provedeny činnosti popsané v odst. 1, tedy identifikace a určování organizačních částí a aktiv tvořících rozsah řízení kybernetické bezpečnosti. Cílem tohoto odstavce bylo pokrýt následný rozvoj organizace, který je nedílnou součástí jejího fungování. Důvody pro stanovení takto širokého záběru jsou shodné s důvody uvedenými v odstavci výše. Za úplné stanovení rozsahu řízení kybernetické bezpečnosti je považován okamžik, kdy je jeho stanovení řádně a prokazatelně dokumentováno v souladu s odst. 3.

K § X – Bezpečnostní opatření poskytovatele regulované služby

Navrhovaná právní úprava vychází z předpokladu, že zabezpečení regulované služby před negativními následky kybernetických bezpečnostních incidentů může být efektivní pouze v případě, jsou-li jednotlivé jeho prvky aplikovány systematicky a ve vzájemných souvislostech. Jedním z předpokladů navrhované právní úpravy je rovněž faktická důležitost nejen technických opatření, ale též s nimi souvisejících organizačních opatření. Teprve kombinace kvalitních technologických nástrojů s náležitě zorganizovaným personálním zajištěním a jasně nastavenými pravidly totiž může ve výsledku poskytnout kýženou efektivitu.

Navrhovaná právní úprava počítá se zavedením povinnosti definovat a aplikovat systém opatření a postupy pro vybrané skupiny poskytovatelů regulovaných služeb souhrnně označovaný jako bezpečnostní opatření. Cílem bezpečnostních opatření je zajistit řádné poskytování regulované služby a kybernetické bezpečnosti aktiv. Navrhovaná právní úprava předpokládá, že poskytovatelé regulovaných služeb provedou zhodnocení bezpečnostních charakteristik jimi poskytovaných služeb a na tomto základě si vytvoří a zdokumentují vlastní systém bezpečnostních opatření sestávajících z opatření organizačních a technických v intencích navrhované právní úpravy. Poskytovatel regulované služby zavádí taková bezpečnostní opatření, která odpovídají jeho režimu, přičemž na poskytovatele regulované služby v režimu vyšší jsou kladeny vyšší nároky než na poskytovatele regulované služby v režimu nižším. Protože je návrh zákona transpozičním předpisem evropské směrnice NIS2, která bezpečnostní opatření také upravuje, je v obou případech, tedy jak v případě poskytovatele regulované služby v režimu vyšších povinností, tak v režimu nižších povinností, potřeba aby bezpečnostní opatření splňovala alespoň požadavky dané čl. 20 a 21 této směrnice.

Je potřeba také uvést, že pokud směrnice NIS2 hovoří vedle organizačních a technických bezpečnostních opatřeních také o provozních opatřeních, jedná se jen o použití jiných termínů vůči tomu, co je ve výsledku stejnou množinou opatření. Tento návrh zákona tedy zachovává dosavadní dělení na organizační a technická opatření, přičemž ale směrnici NIS2 v tomto ohledu plně transponuje.

Dále je potřeba uvést, že směrnice NIS2 uvádí následující:

„Článek 21.

Odstavec 1: Členské státy zajistí, aby základní a důležité subjekty přijaly vhodná a přiměřená technická, provozní a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, jež tyto subjekty používají pro svůj provoz nebo poskytování svých služeb, a k předcházení incidentům nebo minimalizaci jejich dopadů na příjemce jejich služeb a na další služby. S ohledem na nejnovější technický vývoj a případně na příslušné evropské a mezinárodní normy a na náklady na provádění musí opatření uvedená v prvním pododstavci zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika. Při posuzování přiměřenosti těchto opatření je třeba náležitě zohlednit míru vystavení subjektu rizikům, jeho velikost a pravděpodobnost výskytu incidentů, jejich závažnost a společenský a ekonomický dopad.

Odstavec 2: Opatření uvedená v odstavci 1 jsou založena na přístupu zohledňujícím všechny druhy rizik, jehož cílem je chránit sítě a informační systémy a fyzické prostředí těchto systémů před incidenty, a zahrnují alespoň:

a) politiku analýzy rizik a politiku bezpečnosti informačních systémů;

(...)“

Směrnice NIS2 však na tomto místě nestanovuje, že podmínka provedení analýzy rizik musí bezpodmínečně nutně vycházet z hodnocení provedeného samotnými subjekty. Z tohoto důvodu předkládá tento návrh zákona přístup, který v případě poskytovatelů regulovaných služeb v režimu vyšších povinností nechává řízení rizik na těchto subjektech, avšak v případě poskytovatelů regulované služby v režimu nižších povinností má za cíl těmto subjektům s ohledem na jejich počet, nižší význam a obecně nižší maturitu odlehčit z nutnosti provádět plný balík povinností, především těch nejnáročnějších a v praxi nejobtížněji proveditelných – tedy detailního analyzování rizik. V jejich případě tedy návrh zákona stanovuje sadu pravidel, která reagují na provedení analýzy rizik provedené navrhovatelem. Tím, že je poskytovatelé regulovaných služeb provedou dojde také k naplnění cílů směrnice NIS2.

Seznam bezpečnostních opatření pro oba typy poskytovatelů regulovaných služeb je stanoven v následujícím paragrafu a jejich detail je pak stanoven prováděcími právními předpisy.

K § X – Seznam bezpečnostních opatření poskytovatele regulované služby

Seznam bezpečnostních opatření je v navrhované právní úpravě, včetně prováděcích předpisů, proveden genericky resp. teleologicky a předpokládá, že jednotlivá konkrétní řešení bezpečnostních opatření se mohou při současném splnění zákonných požadavků vzájemně odlišovat. Povinnosti týkající se zavedení systému bezpečnostních opatření vycházejí z mezinárodně uznaných standardů a týkají se nejen kategorií a funkčních parametrů jednotlivých typů bezpečnostních technologií (zejména zavedení bezpečnosti komunikačních sítí, řízení identit a přístupových oprávnění, detekčních nástrojů, kryptografických nástrojů), ale rovněž organizace jednotlivých souvisejících procesů (zejména řízení aktiv, příp. rizik v případě poskytovatele regulovaných služeb v režimu vyšších povinností, lidských zdrojů, řízení akvizic nových technologií, organizační postupy pro zvládání kybernetických bezpečnostních událostí a incidentů, řízení kontinuity činností a dalších).

Vzhledem k rozdílným nárokům na poskytovatele regulované služby v režimu vyšších povinností a poskytovatele regulované služby v režimu nižších povinností, jak je uvedeno také výše, je i seznam bezpečnostních opatření rozdělen pro tyto režimy a odráží rozdílnost požadavků na ně.

K § X – Hlášení kybernetických bezpečnostních incidentů

Ustanovení zakládá poskytovatelům regulované služby povinnost hlásit kybernetické bezpečnostní incidenty. Účelem je umožnit Úřadu, resp. Vládnímu CERT a Národnímu CERT vykonávat jejich primární funkci, tj. koordinovat ochranu kybernetického prostoru České republiky.

Primárně mají poskytovatelé regulovaných služeb povinnost hlásit incidenty s původem v kybernetickém prostoru, což vylučuje z hlášení tzv. provozní incidenty, které z povahy věci pod působnost Úřadu nespadají a nemají pro vyhodnocování ze strany Úřadu a další mapování situace v kybernetickém prostoru zásadnější význam. Respektive jejich význam dostatečně nevyrovnává administrativní náročnost zpracování jejich hlášení jak ze strany Úřadu, tak ze strany poskytovatelů regulovaných služeb, nadto Úřad nemůže u těchto incidentů nabídnout relevantní podporu pro jejich zvládání. Toto omezení je v souladu s cílem směrnice zajistit vysoké společné úrovně kybernetické bezpečnosti v Unii, hlášení incidentů s původem mimo kybernetický prostor by reálně ke zvýšení kybernetické bezpečnosti nepřispívalo. Poskytovatelé regulovaných služeb v režimu vyšších povinností hlásí Úřadu všechny kybernetické bezpečnostní incidenty s původem v kybernetickém prostoru. V tomto případě je navržena přísnější úprava nad rámec směrnice, podle které by měly regulované subjekty hlásit pouze incidenty s významným dopadem. 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.

Poskytovatelé regulovaných služeb v režimu nižších povinností hlásí provozovateli Národního CERT pouze incidenty s významným dopadem. Tito poskytovatelé si, na rozdíl od režimu vyšších povinností, sami určí závažnost dopadu na chod organizace a hlásí pouze ty

incidenty, které mají významný dopad. Toto rozložení míry incidentů, které zákon o kybernetické bezpečnosti požaduje po subjektech hlásit, je odrazem proporčního posouzení významnosti všech incidentů povinných osob v režimu nižších povinností a administrativní náročnosti pro jejich zpracování, a to jak na straně samotných povinných osob, tak na straně Úřadu. To společně s aspektem markantního početního nárůstu povinných osob, a to zejména právě v okruhu poskytovatelů regulovaných služeb v režimu nižších povinností a s tím, že primárně jsou v režimu nižších povinností zahrnuty ty osoby, které doposud nebyly povinnými osobami dle zákona o kybernetické bezpečnosti vedlo k výše uvedenému rozložení povinnosti mezi tyto dva režimy povinností poskytovatelů regulovaných služeb.

Vzhledem k tomu, že je potřeba upravit způsob stanovení významného dopadu, je v tomto ustanovení rovněž provedeno zákonné zmocnění Úřadu k vydání prováděcího předpisu, který bude kritéria pro stanovení významnosti obsahovat.

Lhůta pro plnění této povinnosti je stanovena tak, aby měli poskytovatelé regulovaných služeb dostatečnou časovou rezervu k organizačním opatřením umožňujícím správné stanovení rozsahu, ze kterého se incidenty mají hlásit.

Dále je v ustanovení zakotvena možnost dobrovolného hlášení incidentů, událostí a hrozeb v oblasti kybernetické bezpečnosti i od subjektů, které nespadají do působnosti zákona. Tyto subjekty jsou motivovány k tomu, aby společně využívaly svých individuálních znalostí a praktických zkušeností na strategické, taktické a operativní úrovni s cílem zlepšit své schopnosti předcházet incidentům, odhalovat je, reagovat na ně, zotavovat se z nich nebo zmírňovat jejich dopad. Sdílení informací o incidentech, událostech a hrozbách by mělo ve výsledku přispět k lepšímu povědomí o bezpečnostní situaci v kybernetickém prostoru, což následně posiluje schopnost subjektů předcházet incidentům. Stejně tak hlášení zranitelností pro účely koordinovaného zveřejňování zranitelností výrazně zvyšuje schopnost subjektů snižovat rizika vyplývající z těchto zranitelností.

Toto ustanovení je komplementární úpravou k existujícím informačním a ohlašovacím povinnostem, splnění ohlašovací povinnosti podle tohoto ustanovení se orgány a osoby nezbavují informačních povinností založených jinými právními předpisy, např. zákonem č. 127/2005 Sb., o elektronických komunikacích nebo 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 (obecné nařízení o ochraně osobních údajů).

K § X – Náležitosti hlášení kybernetických bezpečnostních incidentů

Směrnice NIS2 ve svém čl. 23 klade požadavky na postup hlášení incidentů, který zahrnuje vícefázové hlášení vztahující se k jednotlivým etapám v rámci řešení incidentu.

V souvislosti s výše uvedeným tak toto ustanovení vytyčuje vícefázový přístup k hlášení incidentů tak, aby bylo dosaženo správné rovnováhy mezi rychlým oznamováním, které pomáhá snížit potenciální šíření významných incidentů a umožňuje poskytovatelům regulovaných služeb žádat Úřad a Národní CERT o podporu, a podrobným oznamováním, které čerpá cenná poučení z jednotlivých incidentů a s postupem času zvyšuje kybernetickou odolnost jednotlivých subjektů a celých odvětví.

Poskytovatelé regulovaných služeb v obou režimech hlásí kybernetické bezpečnostní incidenty bez zbytečného odkladu, nejpozději do 24 hodin od detekce incidentu. Vzhledem ke skutečnosti, že poskytovatelé regulovaných služeb v režimu vyšších povinností hlásí všechny incidenty, posoudí významnost dopadu Úřad na základě informací obsahu hlášení a dalších relevantních informací, a poskytovatele regulované služby informuje o výsledku. V případě incidentů s významným dopadem poskytovatel regulované služby v režimu vyšších povinností následně doplňuje zbylé fáze hlášení ve stanovených časových rozmezích.

Prvotní hlášení by mělo zahrnovat pouze informace nezbytné k tomu, aby se Úřad, příp. Národní CERT dozvěděly o významném incidentu a aby dotčený poskytovatel regulované služby mohl v případě potřeby požádat o pomoc. Prvotní hlášení by mělo případně uvádět, zda existuje podezření, že významný incident byl způsoben nezákonným nebo svévolným zásahem, a zda je pravděpodobné, že bude mít přeshraniční dopad. Povinnost podat prvotní hlášení nebo následné oznámení incidentu by měla být splněna v takové míře, aby neodváděla zdroje oznamujícího poskytovatele regulované služby od činností souvisejících s řešením incidentu, které by měly být upřednostněny.

Po prvotním hlášení incidentu předloží poskytovatel regulované služby oznámení s cílem aktualizovat informace předané v prvotním hlášení a uvést posouzení významného incidentu, včetně jeho dopadu, jakož i indikátory narušení, jsou-li k dispozici. Toto oznámení musí být Úřadu nebo Národnímu CERT doloženo bez zbytečného odkladu, v každém případě do 72 hodin (poskytovatel služby vytvářející důvěru do 24 hodin) od okamžiku, kdy se o významném incidentu subjekt dozvěděl. Nejpozději do 30 dnů po oznámení incidentu by měla být předložena závěrečná zpráva. V případě, že v okamžiku, kdy by měla být předložena závěrečná zpráva, incident stále trvá, předloží poskytovatel regulované služby v uvedené lhůtě zprávu o pokroku a poté nejpozději do 30 dnů po vyřešení významného incidentu závěrečnou zprávu.

Incidenty jsou hlášeny prostřednictvím Portálu NÚKIB. Celý proces bude v co nejvyšší míře automatizován a zjednodušen oproti původnímu hlášení prostřednictvím formuláře na internetových stránkách Úřadu, a jedná se o splnění požadavku směrnice na snížení administrativní zátěže subjektů. Zároveň zůstává zachována i možnost alternativního způsobu hlášení incidentů prostřednictvím elektronické pošty nebo datové schránky Úřadu, příp. Národního CERT v případě nedostupnosti Portálu NÚKIB.

K určení obsahu a způsobu hlášení kybernetických bezpečnostních incidentů a náležitostí závěrečné zprávy je v tomto ustanovení provedeno zákonné zmocnění Úřadu k vydání prováděcího předpisu.

K § X – Zvládání kybernetických bezpečnostních incidentů

Úřad, resp. Vládní CERT a Národní CERT, poskytují bez zbytečného odkladu poskytovatelům regulovaných služeb své vyjádření k nahlášenému kybernetickému bezpečnostnímu incidentu, a na vyžádání také podporu při jeho zvládání. Vládní a Národní CERT prioritizují poskytování svých služeb podle přístupu založeném na rizicích a podle dostupných kapacit.

Při zvládání kybernetických bezpečnostních incidentů je vyžadována součinnost všech orgánů a osob za účelem odstranění možných překážek zabraňujících zvládání těchto incidentů. Může se jednat například o zpřístupnění prostor, ve kterých se nachází napadená infrastruktura, a to i ze strany orgánů a osob, které nejsou poskytovateli regulovaných služeb, tedy například dodavatelů. Součinnost bude vyžadována pouze v nezbytných a důvodných případech tak, aby byl zásah do práv těchto osob proporční k míře nebezpečnosti a rizikovosti daného incidentu a důležitosti poskytované služby, která je tímto incidentem ohrožena.

Údaje o kybernetických bezpečnostních incidentech, událostech, hrozbách a zranitelnostech mají velkou vypovídací hodnotu o činnosti pracovišť CERT a o kybernetické bezpečnostní situaci České republiky a jejich analýza je vhodná k dalšímu zlepšování služeb pracovišť CERT a jako podklad pro další kroky Úřadu. Proto jsou shromažďovány v určené evidenci vedené Úřadem.

K § X – Informační povinnost poskytovatele regulované služby

Poskytovatel regulované služby sám posoudí potřebu oznámit kybernetický bezpečnostní incident s významným dopadem uživatelům napadené regulované služby. Ohlašování kybernetických bezpečnostních hrozeb má zásadní význam pro předcházení tomu, aby tyto hrozby přerostly do kybernetických bezpečnostních incidentů. Proaktivní přístup ke kybernetickým hrozbám je zásadní složkou opatření k řízení kybernetických bezpečnostních rizik. Pokud je nezbytná informovanost veřejnosti, zavádí se oprávnění Úřadu informovat veřejnost, nebo uložit poskytovateli regulované služby povinnost učinit tak sám. 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 či obchodních zájmů poskytovatele regulované služby, který incident ohlašuje.

V příslušných případech by poskytovatelé regulovaných služeb měli uživatelům svých služeb bez zbytečného odkladu sdělit veškerá opatření nebo nápravná opatření, která mohou přijmout ke zmírnění výsledných rizik vyplývajících z významné kybernetické hrozby. Poskytovatelé regulovaných služeb by měli podle potřeby, obzvláště pokud je pravděpodobné, že se významná kybernetická hrozba naplní, rovněž informovat uživatele svých služeb o samotné hrozbě. Požadavek na informování těchto uživatelů o významných kybernetických hrozbách by se měl splnit s vynaložením maximálního úsilí, ale neměl by tyto subjekty zbavovat povinnosti přijmout na vlastní náklady přiměřená a okamžitá opatření s cílem zamezit těmto hrozbám nebo je odstranit a obnovit běžnou úroveň bezpečnosti služby. Tyto informace o významných kybernetických hrozbách by měly být uživatelům služby poskytovány zdarma a měly by být formulovány ve snadno srozumitelném jazyce.

K § X - § Y – Protiopatření

Ustanovení upravuje definici protiopatření jako součásti systému k zajištění kybernetické bezpečnosti. Definice protiopatření je provedena za užití obsahového kritéria, tj. účelu ochrany kybernetického prostoru před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení kybernetického bezpečnostního incidentu, který již nastal.

Cílem takto stanovené struktury protiopatření je pokrýt jednak formou varování potřebu oficiálního preventivního působení NÚKIB vzhledem k aktuálním kybernetickým bezpečnostním hrozbám a zranitelnostem ještě před tím, než se tyto hrozby či zranitelnosti projeví v kybernetickém prostoru. Smyslem reaktivních protiopatření pak je působit k dosažení smyslu a účelu zákona v situaci trvajícího či bezprostředně hrozícího kybernetického bezpečnostního incidentu, či zpětně reagovat na proběhlý kybernetický bezpečnostní incident a využít zkušenosti z jeho řešení k prevenci dalších kybernetických bezpečnostních incidentů obdobného charakteru. Dále pak strukturu doplňuje výstraha, která umožňuje NÚKIB veřejně informovat o porušování zákona o kybernetické bezpečnosti či o probíhajícím kybernetickém bezpečnostním incidentu v případech, kdy je to nutné z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu.

Zákon ukládá poskytovatelům regulované služby povinnost provádět reaktivní protiopatření. Vzhledem k jejich povaze je pak reaktivní protiopatření jako prostředek ultima ratio NÚKIB povinné pro poskytovatele služeb jak v režimu vyšších povinností, tak i v režimu nižších povinností. Vzhledem k nastavení systému řízení bezpečnosti informací u poskytovatelů regulovaných služeb v režimu nižších povinností se na ně varování neaplikuje. Nicméně vzhledem k tomu, že se jedná o veřejně dostupnou informaci o existující hrozbě či zranitelnosti, a to společně s mírou její závažnosti, měly by se touto hrozbou či zranitelností, pokud je pro ně relevantní, zabývat i poskytovatelé regulovaných služeb v režimu nižších

povinností, nicméně není pro ně závazná. Rozdělení poskytovatelů regulované služby vzhledem k povinnostem provádět protiopatření odpovídá principu minimalizace zásahu do autonomie vůle poskytovatelů regulované služby a zakládá možnost NÚKIB autoritativně regulovat chování poskytovatelů regulované služby jen v nezbytně nutné míře.

Zákon dále ukládá poskytovatelům regulovaných služeb, kterých se protiopatření týká, aby informovali o jeho provedení ve lhůtě v něm uvedené, pokud v daném protiopatření nebude uvedeno jinak. To odráží fakt, že informace o stavu kybernetického prostředí státu a jejich zpracování jsou podstatnou součástí budování odolné společnosti a zajišťování bezpečnosti státu. NÚKIB pak provede správní uvážení, zda informace o splnění daného opatření a jejich následné zpracování bude představovat dostatečný benefit pro plnění účelu zákona o kybernetické bezpečnosti v porovnání s administrativní zátěží, kterou to na jednotlivé poskytovatele regulovaných služeb klade a zváží případně, že této povinnosti poskytovatele regulované služby v daném protiopatření zprostí. Pro zjednodušení této povinnosti a nezatěžování poskytovatelů regulované služby přílišnými administrativními povinnostmi pak NÚKIB stanoví prováděcím právním předpisem náležitosti a způsob tohoto oznámení, které bude NÚKIB podáváno prostřednictvím portálu NÚKIB.

Výstraha

Výstraha jako institut vychází z požadavků směrnice na členské státy. Jde o nástroj informování veřejnosti použitelný pouze v případě, že zveřejnění takové informace je nezbytné pro zajištění ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu. Benefit zveřejnění takovéto informace by měl převýšit možné negativní dopady zveřejnění těchto informací. NÚKIB v rámci správního uvážení vezme do úvahy potřebu zachování rovnováhy mezi zájmem veřejnosti být informovanou o hrozbách a mezi možným poškozením pověsti či obchodních zájmů poskytovatele regulované služby. Při tomto správním uvážení NÚKIB zároveň vyhodnotí možné další přímé dopady na veřejnost s přihlédnutím k zájmu o informace chráněné zákonem o kybernetické bezpečnosti.

Jedná se pak o zveřejnění dvou typů informace, a to buďto informace o tom, že některý poskytovatel regulované služby nedodržuje povinnosti, které mu ukládá zákon o kybernetické bezpečnosti, nebo že došlo ke kybernetickému bezpečnostnímu incidentu. NÚKIB může buďto nařídit poskytovateli regulovaných služeb, aby tuto informaci zveřejnil on, nebo tak učinit sám.

Varování

Účelem varování podle tohoto ustanovení je oficiální publikace informací o bezpečnostní hrozbě či zranitelnosti, tj. preventivní informování poskytovatelů regulované služby o míře závažnosti některé hrozby či zranitelnosti, která je následně povinným vstupem do analýzy rizik daného poskytovatele regulovaných služeb.Vzhledem k technickému charakteru některých kybernetických bezpečnostních hrozeb lze očekávat, že v některých případech bude možno takovou hrozbu či zranitelnost ze strany NÚKIB po obdržení informací o její existenci pro účely okamžitého vydání varování pouze popsat či ohodnotit. Bude-li mít NÚKIB k dispozici též informace o technickém řešení, může tyto informace připojit k varování a zvýšit tak návodnost pro poskytovatele regulovaných služeb.

Varování bude publikováno prostřednictvím internetových stránek NÚKIB, aby byla zajištěna informovanost dotčených subjektů, včetně široké veřejnosti. Poskytovatelům regulované služby bude varování rovněž oznamováno prostřednictvím kontaktních údajů, které mají povinnost hlásit do evidence kontaktních údajů. V případě, že by však zveřejnění tohoto varování mohlo vést k negativním dopadům na právem chráněné zájmy (konkrétně by tedy mohlo ohrozit zajišťování kybernetické bezpečnosti, účinnost protiopatření vydaného podle zákona o kybernetické bezpečnosti, jiné oprávněné zájmy státu nebo by na jeho základě bylo

možné identifikovat orgán nebo osobu, která kybernetickou hrozbu, zranitelnost nebo kybernetický bezpečnostní incident ohlásila), může NÚKIB od zveřejnění varování upustit a toto tak sdílet pouze s jím dotčenými poskytovateli regulovaných služeb. K tomu NÚKIB přistoupí po správním uvážení, zda je zde převažujícím zájmem právo veřejnosti na informace o zranitelnostech a hrozbách či převáží jiný chráněný zájem, který by byl zveřejněním varování narušen.

Varování je závazné pro poskytovatele regulovaných služeb v režimu vyšších povinností, jelikož ti v rámci svého systému řízení bezpečnosti informací jsou schopni zohlednit hodnotu dané hrozby či zranitelnosti v rámci svého řízení rizik. Poskytovatelé regulovaných služeb v režimu nižších povinností by měli k informacím obsaženým ve varování přistupovat jako k informaci, která může jejich bezpečnost rovněž ovlivnit, nicméně právně závazné vzhledem k postupům, kterými zajišťují svou kybernetickou bezpečnost, pro ně *per se* není.

Reaktivní protiopatření

Účelem reaktivního protiopatření je okamžitá reakce na výskyt kybernetického bezpečnostního incidentu. Obsahem protiopatření tedy mohou být povinnosti provést konkrétní úkony nutné k odvrácení kybernetického bezpečnostního incidentu nebo ke zmírnění jeho následků. Může nabývat, jak podoby preventivní, kdy kybernetický bezpečnostní incident hrozí, čistě reaktivní, kdy incident právě probíhá či následně preventivní, kdy incident proběhl, byl vyřešen a je vhodné provést úkony, které výskyt tohoto incidentu budou dostatečně preventovat u vymezeného dotčeného okruhu poskytovatelů regulovaných služeb.

Reaktivní protiopatření je zároveň v této podobě i nástrojem odrážejícím požadavek, který směrnice NIS2 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 NIS2.

Rovněž je rozsah reaktivního protiopatření dostatečně široký a procesně ukotvený na to, aby jím bylo možné provést krok doposud upravený ustanovením § 24 odst. 2 současného znění zákona o kybernetické bezpečnosti, a tedy nařídit prostřednictvím reaktivního protiopatření zákaz použití některých aktiv daného poskytovatele do doby odstranění nedostatků, které byly při kontrole nalezeny.

Zákon rozlišuje dvě formy reaktivních protiopatření, a to rozhodnutí a opatření obecné povahy. Smyslem tohoto dělení je pokrýt oba typické případy vyskytující se při ochraně před kybernetickými bezpečnostními incidenty. První možností je výskyt kybernetického bezpečnostního incidentu v rámci určité organizace. Reaktivní protiopatření lze v takovém případě vydat formou rozhodnutí konkrétně specifikujícím povinnosti pro určeného adresáta – poskytovatele regulované služby. Druhou možností je výskyt incidentu, jehož rozsah je větší nebo jehož rozsah nelze kvůli složitosti incidentu nebo jeho rychlému vývoji přesně určit – takový incident pak je možno řešit vydáním reaktivního protiopatření formou opatření obecné povahy, v němž budou specifikovány konkrétní povinnosti k jeho odvrácení neurčitému okruhu poskytovatelů regulovaných služeb definovanému za užití generických znaků odpovídajících jeho charakteru.

Charakter kybernetických bezpečnostních incidentů vyžaduje k úspěšnosti reaktivního protiopatření reakci v co nejkratším čase. Jakákoli časová prodleva, byť v řádu hodin, může znamenat exponenciální rozvoj kybernetického bezpečnostního incidentu a násobení jeho škodlivého účinku. Z tohoto důvodu je zákonem speciálně upravena vykonatelnost rozhodnutí jeho doručením poskytovatelům regulované služby, respektive vyvěšením na úřední desce NÚKIB a výslovně založena možnost vydání rozhodnutí v řízení na místě podle správního řádu.

Z téhož důvodu nelze přiznat odkladný účinek rozkladu podanému proti rozhodnutí a nelze vést ani přezkumné řízení, je-li reaktivní protiopatření vydáno opatřením obecné povahy.

Z důvodu naléhavé nutnosti reagovat na hrozící, probíhající nebo vyřešený kybernetický bezpečnostní incident v co nejkratším čase je upravena účinnost těchto opatření obecné povahy dnem zveřejnění na úřední desce NÚKIB, přičemž vydání těchto opatření obecné povahy nebude předcházet řízení o návrhu opatření obecné povahy podle § 172 správního řádu, při němž by mohly být proti návrhu podávány oprávněnými osobami námitky nebo připomínky. Poskytovatelům regulované služby je oprávnění uplatnit připomínky podle § 172 odst. 4 správního řádu modifikováno, a to tak, že budou oprávněni podat připomínky směřující přímo proti vydanému opatření obecné povahy, a to ve lhůtě 15 dnů od jeho zveřejnění na úřední desce NÚKIB. V případě vyhodnocení připomínek jako důvodných, lze příslušné opatření obecné povahy změnit nebo zrušit.

Současně z důvodu zajištění co možná nejrychlejšího a nejefektivnějšího informování poskytovatelů regulované služby o protiopatřeních vydaných formou opatření obecné povahy NÚKIB vyrozumí poskytovatele regulované služby o vydání těchto protiopatření prostřednictvím kontaktních údajů, které mají povinnost hlásit do evidence kontaktních údajů.

Vyloučení přezkumného řízení odůvodňuje potřeba reakce na nastalý kybernetický bezpečnostní incident v co nejkratším čase, jakož i potřeba zamezit prodlevě mezi získáním poznatků z řešení kybernetického bezpečnostního incidentu a jejich implementací poskytovateli regulované služby.

K § X – Řízení dodavatelů a vztah k zadávání veřejných zakázek

Navrhované ustanovení je přejato z předchozí právní úpravy a navazuje na povinnost poskytovatelů regulované služby zavádět a provádět bezpečnostní opatření. 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 NIS2, 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.

Druhá věta pak stejně jako v případě předchozí právní úpravy deklaruje slučitelnost požadavků vyplývajících z plnění povinností podle tohoto zákona s pravidly pro zadávání veřejných zakázek. Stejně jako v případě předchozí právní úpravy však platí, že za zákonné omezení hospodářské soutěže nebo odůvodněnou překážku hospodářské soutěži se automaticky považuje zohlednění pouze takových požadavků, které jsou nezbytné pro splnění povinností podle tohoto zákona (zejména tedy požadavky založené na výsledcích řízení rizik nebo vyvěrající z protiopatření Úřadu). Požadavky stanovené nad rámec této minimální úrovně je potřeba odůvodnit jiným způsobem.

K § X – Speciální úprava předání informací a dat od významného dodavatele

Řada poskytovatelů regulovaných služeb neprovozuje aktiva sloužící pro poskytování regulovaných služeb a v důsledku toho mnohdy nedisponují informacemi a daty, která s provozem těchto aktiv souvisejí. Při potřebě extrakce informací a dat ze systému (ať již v průběhu plnění smluvního vztahu, nebo při jeho končení a migraci informací a dat k jinému dodavateli) jsou tak závislí na součinnosti svého dodavatele. Poskytovatel regulované služby má ze zákona povinnost smluvně si ošetřit situace, kdy potřebuje mít tyto informace a data k dispozici, nicméně v krajních případech mohou nastat situace vyžadující autoritativní zásah ze strany Úřadu. Činnost Úřadu v tomto případě slouží k zabránění realizace kybernetického bezpečnostního incidentu v situaci, kdy soukromoprávní prostředky k vyřešení situace nepostačují a je dán veřejný zájem na ochraně regulované služby. 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. Vydání rozhodnutí Úřadu a splnění povinnosti v něm uložené smluvní strany nezbavuje odpovědnosti za řádné plnění závazku ze smlouvy.

Navrhované ustanovení reaguje na stav, kdy provozovatel regulované služby v režimu vyšších povinností nemá přes existenci smluvních ujednání stran předání dat přístup k informacím a datům, např. v důsledku neshod s významným dodavatelem, a zároveň hrozí kybernetický bezpečnostní incident, který může mít vliv na poskytování regulované služby. Pokud poskytovatel regulované služby v režimu vyšších povinností marně vyzval významného dodavatele k předání informací a dat souvisejících s provozem aktiv sloužících k poskytování regulované služby, Úřad může vydat rozhodnutí, kterým uloží významnému dodavateli povinnost tyto informace a data poskytovateli regulované služby předat. Zákon tak míří primárně na případy, kdy významný dodavatel nedostatečně plní své smluvní povinnosti směrem k poskytovateli regulované služby.

Současně však Úřad není vázán ustanoveními smlouvy mezi poskytovatelem regulované služby a jeho významným dodavatelem a může stanovit vlastní rozsah povinně předaných dat. Vždy však musí jít o informace a data související s provozem aktiv sloužících k poskytování regulované služby.

Navrhované ustanovení upravuje i situace, kdy v důsledku outsourcingu a řetězení dodavatelů postrádá přístup k informacím a datům i významný dodavatel. Ačkoli by předání dat mělo být mezi poskytovatelem regulované služby a jeho poddodavateli rovněž řešeno smluvně (resp. řetězením smluv), je z důvodu hrozby kybernetického bezpečnostního incidentu kladen důraz na rychlost řešení situace. Z toho důvodu může Úřad v rozhodnutí zavázat i další osoby než jen přímého smluvního partnera poskytovatele regulované služby k vydání informací a dat souvisejících s provozem aktiv sloužících k poskytování regulované služby, kterými tato osoba disponuje. Smluvní ujednání mezi významným dodavatelem poskytovatele regulované služby a jeho poddodavateli nejsou pro vydání rozhodnutí Úřadu rozhodná. K rozhodnutí o uložení povinnosti jiné osobě než významnému dodavateli může Úřad přistoupit buďto v situaci, kdy významný dodavatel požadovanými informacemi a daty objektivně nedisponuje, nebo jimi sice disponuje nebo by jimi disponovat měl, ale vzhledem ke skutkovým okolnostem není účelné po něm opatření a vydání informací a dat požadovat. To nastane typicky v situaci, kdy by trvání na splnění povinnosti významným dodavatelem vedlo k neúměrnému prodloužení doby předání informací a dat a tím k realizaci incidentu nebo k významnému zvýšení pravděpodobnosti jeho realizace. Uložením povinnosti předat informace a data jiné osobě není dotčena odpovědnost významného dodavatele za nesplnění jemu uložené povinnosti předat informace a data, pokud mu ji Úřad uložil.

Řízení o vydání rozhodnutí je zahajováno z moci úřední na základě podaného podnětu a na jeho zahájení není právní nárok. Úřad řízení zahájí pouze v případě, že jsou pro to splněny zákonné předpoklady. Podnět k zahájení řízení může podat pouze poskytovatel regulované služby v režimu vyšších povinností. Podnět kohokoli jiného Úřad zaeviduje, ale řízení nezahájí. Zákon v tomto ohledu míří na poskytovatele regulovaných služeb v režimu vyšších povinností z důvodu vyšších požadavků kladených na tyto subjekty. S ohledem na skutečnost, že služby těchto subjektů jsou stěžejní pro zajištění bezpečnosti státu, bude dopad kybernetických bezpečnostních incidentů v jejich aktivech obecně významnější než u subjektů zařazených do režimu nižších povinností.

Rozhodnutí o uložení povinnosti předat informace a data může být prvním úkonem v řízení zejména v případech, kdy je hrozba kybernetického bezpečnostního incidentu urgentní

a zároveň nejsou dány pochybnosti o skutkovém stavu. V ostatních případech Úřad zahájí standardní správní řízení umožňující účastníkům řízení vyjadřovat se k podkladům rozhodnutí či jinak ovlivňovat průběh správního řízení. Rozklad proti rozhodnutí ve věci nemá odkladný účinek z důvodu existence hrozícího incidentu, který by se v případě pozdržení předání informací a dat nad rámec stanoveného lhůty mohl realizovat. Rozhodnutí je tak předběžně vykonatelné dnem uplynutí lhůty stanovené ke splnění povinnosti (pokud lhůta není stanovena, pak dnem jeho doručení) a adresát povinnosti je povinen ji ve stanovené lhůtě splnit. V opačném případě se vystavuje jednak postihu za nesplnění povinnosti (pokuta za přestupek), jednak exekuci rozhodnutí Úřadu (např. ukládáním donucovacích pokut, jejichž výše pro tyto případy doznala oproti obecné úpravě významných změn).

Vzhledem k primární povinnosti upravit si podmínky předání informací a dat smluvně by úhrada vynaložených nákladů, včetně finanční kompenzace práv duševního vlastnictví, měla být zahrnuta v těchto smluvních ujednáních. Nároky poddodavatele by měly být uplatňovány směrem k významnému dodavateli, resp. jeho smluvnímu partnerovi. Případné neshody v této problematice nesmí být důvodem nesplnění povinnosti uložené rozhodnutím, která je primárním zájmem státu na zajištění kybernetické bezpečnosti v klíčových oblastech. Nelze tedy odpírat poskytnutí informací a dat s odůvodněním, že ještě nedošlo k dohodě o kompenzaci nákladů na jejich předání. Stát touto úpravou jasně deklaruje přednost zájmu na předání informací a dat před soukromoprávní dohodou o kompenzacích.

K § X – Podmínky lokalizace informací a dat

Zpracování dat a informací mimo Českou republiku s sebou nese určitou míru rizika pro zajištění jejich dostupnosti, integrity a důvěrnosti. Může jít o rizika spojená se zpracováním dat a informací v zemi s odlišným právním řádem, který nemusí datům a informacím poskytovat dostatečnou ochranu, rizika spojená s možným přístupem cizozemských orgánů k datům a informacím, rizika spojená s nedostupností dat a informací pro české orgány činné v trestním řízení, rizika spojená s nedostupností dat a informací pro jejich faktickou vzdálenost v případech přírodních katastrof, války, pandemie či jiných nepředvídatelných událostí na území cizích států. Tato rizika nelze plně mitigovat jiným nástrojem než omezením okruhu států, na jejichž území mohou být data a informace poskytovatelů regulovaných služeb zpracovávána.

S ohledem na zachování proporcionality zajištění národní bezpečnosti a ochrany svobody podnikání, jakož i s ohledem na minimalizaci státního donucení a ekonomických dopadů navrhovaného řešení na veřejný i soukromý sektor, je okruh povinných osob, na které tato povinnost dopadne omezen na poskytovatele regulovaných služeb v režimu vyšších povinností, protože u nich vzhledem k vyšší pravděpodobnosti zpracování citlivějších dat a informací převáží zájem na zajištění jejich důvěrnosti, dostupnosti a integrity.

Věcné vymezení rozsahu dat a informací, na které se toto omezení vtahuje je stanoveno obdobně jako povinnost zavádět bezpečnostní opatření, tedy v rámci stanoveného rozsahu řízení kybernetické bezpečnosti v souladu s ustanovením daným v zákoně o kybernetické bezpečnosti.

Prováděcí právní předpis následně stanoví, která data a informace v rámci stanoveného rozsahu mohou být zpracována na území kterých států (k tomu blíže viz odůvodnění relevantních ustanovení vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností).

Pro minimalizaci dopadů povinností vyplývajících z tohoto ustanovení do svobody podnikání a vlastnických práv a pro zajištění maximální kontinuity činností relevantních

regulovaných organizací je na splnění těchto povinností stanovena dostatečná lhůta 3 let od účinnosti tohoto zákona pro případné změny v dodavatelském řetězci.

K § X – Prověřování rizik spojených s dodavatelem

Navrhované ustanovení zavádí pravomoc Úřadu provádět prověřování rizik spojených s dodavatelem, vymezuje pojmy spojené s touto pravomocí a stanoví zmocnění pro úpravu prováděcích právních předpisů. Zavedení této pravomoci představuje stěžejní část mechanismu prověřování bezpečnosti dodavatelského řetězce.

K odst. 1

Navrhovaná pravomoc se realizuje 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 (viz odůvodnění k odst. 3), a které jsou spojeny s konkrétním orgánem či osobou.

Navrhovaná pravomoc neomezuje prověřování pouze na orgány či osoby, které jsou v okamžiku jednotlivých případů její realizace dodavateli do infrastruktury povinných osob mechanismu prověřování (viz odůvodnění k odst. 3), na kterou mohou dopadnout případná omezení (viz odůvodnění k odst. 3 a § X – Omezení rizik spojených s dodavatelem). Cílem mechanismu prověřování bezpečnosti dodavatelského řetězce je umožnit státu identifikovat a vyhodnocovat hrozby spojené také se subjekty, u nichž se lze domnívat, že by svá plnění do této infrastruktury dodávat mohly. V ideálním případě tak bude možné odhalit hrozbu ještě dříve, než bude ve vymezené infrastruktuře moci způsobit narušení bezpečnosti informací.

Úřad pro potřeby výkonu této pravomoci vychází jak z informací zjištěných v rámci vlastní činnosti, tak z informací, kterými disponují jiné orgány či osoby, a které jsou pro prověřování nezbytné. Mezi orgány státu, jež může v souvislosti s uvedenou pravomocí Úřad oslovit, jsou vyjmenovány ministerstva a jiné orgány s působností zejména v oblasti bezpečnosti, jež mohou disponovat informacemi relevantními pro vyhodnocení kritérií rizikovosti dodavatele stanovených prováděcím právním předpisem.

Podle předběžného projednání koncepce mechanismu prověřování bezpečnosti dodavatelského řetězce s uvedenými orgány státu a s ohledem na formulaci navrhovaného ustanovení se však až na výjimečné případy počítá toliko s poskytnutím informací, kterými uvedené orgány již disponují, spíše než s vlastním aktivním zjišťováním takových informací uvedenými orgány, jakkoliv tato možnost není obecně vyloučena. O poskytnutí informací či součinnosti může Úřad z téhož účelu požádat také jiné orgány či osoby, pakliže se lze důvodně domnívat, že mohou disponovat informacemi nezbytnými k vyhodnocení naplnění kritérií rizikovosti dodavatele a příslušné hrozby.

Vzhledem k rozsahu úvahy, kterou je pro vyhodnocení kritérií rizikovosti dodavatele a vymezeného rozsahu hrozeb nezbytné provést, lze očekávat potřebu brát v jednotlivých případech prověřování v úvahu také utajované a jiné neveřejné a citlivé informace, jež jsou chráněny zvláštními právními předpisy. Poskytnutí informací pro účely prověřování rizik spojených s dodavatelem se proto podle navrhovaného ustanovení nepovažuje za porušení zákonem stanovené či uznané povinnosti mlčenlivosti (například podle § 15 správního řádu, dle § 52 daňového řádu nebo § 16 zákona o provádění mezinárodních sankcích) a poskytnuté informace podléhají spolu s dalšími informacemi zvláštní ochraně (viz § X – Ochrana informací o omezení rizik spojených s dodavateli).

K odst. 2

S ohledem na velké množství subjektů, které mohou být předmětem prověřování podle odstavce 1, se stanoví postup prioritizace stávajících a potenciálních dodavatelů k prověření. Úřad při tom bude vycházet z postupu založeného na rizicích, tedy z vyhodnocení aktuální bezpečnostní situace, zejména na základě analýzy aktuálních kybernetických hrozeb a rizik, jakož i z informací získaných od ostatních orgánů a osob působících v oblasti kybernetické bezpečnosti.

Předně by tak měli být prověřeni dodavatelé, u kterých lze předpokládat nejvýznamnější vliv na vymezenou infrastrukturu povinných osob mechanismu prověřování, ať již z důvodu vysokého množství povinných osob, kterým poskytují svá plnění, nebo z důvodu vysokého procentuálního zastoupení u několika povinných osob. Prioritizaci subjektů k prověření Úřadem může dále ovlivnit například potřeba prověření konkrétních zájemců o poskytování významné veřejné zakázky nebo podezření na přítomnost bezpečnostní hrozby spojené s konkrétním subjektem, zjištěné jiným orgánem státu. Navržený prioritizační přístup bude aplikován i pro případné opakované prověření dodavatele, např. v případě, že budou zjištěny poznatky ohledně významných změn, které by mohly mít vliv na vyhodnocenou hrozbu.

Přestože cílem mechanismu prověřování bezpečnosti dodavatelského řetězce je prověřit zejména všechny dodavatele vymezených povinných osob mechanismu prověřování (viz odůvodnění k odst. 3). Významným faktorem pro výběr konkrétních subjektů k prověření budou také dostupné personální a technické kapacity Úřadu a ostatních orgánů a osob zapojených do prověřování.

K odst. 3

Navrhované ustanovení vymezuje pojmy, které navrhovaná právní úprava dále užívá v souvislosti s mechanismem prověřování bezpečnosti dodavatelského řetězce.

K písm. a)

Pojem *„kritická část stanoveného rozsahu“* vymezuje aktiva poskytovatele regulované služby v režimu vyšších povinností, kterému plynou povinnosti z prověřování bezpečnosti dodavatelského řetězce (tzn. povinné osoby mechanismu prověřování), na která se mohou vztahovat omezení využití plnění rizikových dodavatelů. Dochází tak k vymezení aktiv, která jsou z hlediska stanoveného rozsahu nejvýznamnější a na jejichž bezpečnost je třeba brát zvláštní zřetel, včetně výběru důvěryhodných dodavatelů plnění směřujících do těchto aktiv.

Kritická část stanoveného rozsahu sestává z podmnožiny aktiv, u kterých si povinná osoba postupem podle prováděcího právního předpisu – vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností sama ohodnotila dopad narušení bezpečnosti informací úrovní vysoká či kritická, a podmnožiny aktiv, která zajišťují funkce stanoveného rozsahu, vymezené prováděcím právním předpisem – vyhláškou o nepominutelných funkcích stanoveného rozsahu (ta vymezuje nepominutelné, neboli základní či „kritické“ funkce celého rozsahu aktiv, na které se vztahuje řízení kybernetické bezpečnosti podle zákona).

Povinná osoba tedy při identifikaci rozsahu aktiv, na která se vztahují povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, nejprve aktiva ohodnotí (a to již v rámci plnění povinností podle § X – Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby) a následně výčet aktiv ohodnocených úrovní vysoká či kritická pro potřeby plnění povinností z mechanismu prověřování doplní o aktiva, jež v jejím konkrétním případě zajišťují nepominutelné funkce stanovené příslušnou vyhláškou.

K písm. b)

Pojem *„bezpečnostně významná dodávka“* vymezuje plnění, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů.

Jedná se o plnění, spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu technických prostředků nebo vybavení, disponujících výpočetní kapacitou (tedy např. základní deska či celý server, nikoli však prostý napájecí kabel), programových prostředků nebo vybavení (typicky software, který technické prostředky a vybavení ovládá), případně informační či komunikační služby (typicky služby cloud computingu, řízené služby a další). Plnění přitom může naplňovat jak jeden z těchto atributů (např. pouze vývoj technického prostředku nebo pouze jeho výroba), tak jejich kombinaci (např. sestavení a servis technického prostředku a poskytnutí programového prostředku).

Účelem vymezení těchto plnění je vztáhnout případná omezení pouze na ty produkty a služby, které mohou mít relevantní dopad na bezpečnost vymezených aktiv. Vymezením pojmu jako některých druhů plnění směřujících pouze do některých druhů aktiv – těch, která jsou součástí kritické části stanoveného rozsahu (viz odůvodnění k písm. a) – dochází ke vztažení případných omezení na nezbytnou množinu situací, u kterých dává takové omezení smysl z technického hlediska, a které mají vazbu na nejvýznamnější aktiva, resp. prvky celé regulace.

K písm. c)

Pojem *„dodavatel bezpečnostně významné dodávky“* vymezuje okruh subjektů, na jejichž plnění se mohou vztahovat omezení využití v důsledku prověření rizik s nimi spojených.

Dodavatelem bezpečnostně významné dodávky je každý subjekt, který poskytuje bezpečnostně významnou dodávku, a to buď přímo (typicky osoba, s níž uzavírá povinná osoba mechanismu prověřování smlouvu o dodávce), nebo prostřednictvím jiného subjektu (typicky svého obchodního partnera – v dodavatelsko-odběratelském řetězci je tedy v pozici poddodavatele).

Omezení využití mohou být vztažena na všechna typově vymezená plnění (tzn. bezpečnostně významné dodávky), v jejichž dodavatelském řetězci se nachází (pod)dodavatel, u něhož bylo vyhodnoceno možné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku (viz § X – Omezení rizik spojených s dodavatelem). S ohledem na problematické vymezení hloubky dodavatelského řetězce, na kterou je přiměřené taková omezení vztahovat (jednotlivé dodavatelské řetězce bezpečnostně významných dodávek se diametrálně odlišují co do hloubky i šíře), se omezení aplikují pouze na ty dodavatele v řetězci, s nimiž se lze při vynaložení přiměřeného úsilí seznámit (viz § X – Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce).

K odst. 4 a 5

K vymezení konkrétních kritérií pro určení poskytovatele regulované služby v režimu vyšších povinností, kterému plynou povinnosti z prověřování bezpečnosti dodavatelského řetězce, nepominutelných funkcí stanoveného rozsahu pro určení kritické části stanoveného rozsahu a kritérií a podrobností jejich vyhodnocení, zmocňuje navrhované ustanovení prováděcí právní předpis.

K § X – Omezení rizik spojených s dodavatelem

Navrhované ustanovení zavádí pravomoc Úřadu omezit nebo zakázat využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, zjistí-li Úřad postupem podle § X – Prověřování rizik spojených s dodavatelem, že může být významně ohrožena bezpečnost České republiky nebo vnitřní či veřejný pořádek.

Účelem zavedení této pravomoci je umožnit státu adekvátně reagovat na nejzávažnější zjištění týkající se hrozeb spojených s užitím plnění konkrétního dodavatele ve vymezené části regulované infrastruktury. Podrobná kritéria a postup pro vyhodnocení hrozby stanoví prováděcí právní předpis – vyhláška o kritériích rizikovosti dodavatele.

Podle povahy a kontextu konkrétní vyhodnocené hrozby ukládá návrh Úřadu vydat konkrétní omezení formou opatření obecné povahy, kterým se tak budou muset řídit všechny stanovené povinné osoby mechanismu prověřování. Jelikož však bude opatření mířit vždy vůči typově vymezeným plněním konkrétního dodavatele – bezpečnostně relevantní dodávce – prakticky se omezení, které stanoví, projeví pouze u těch povinných osob, které takové plnění v kritické části stanoveného rozsahu využívají nebo jeho využití plánují. Možnost Úřadu reagovat na zjištěnou hrozbu, která nenaplní náležitosti pro vydání opatření obecné povahy, jinými zákonem stanovenými prostředky, například prostřednictvím varování podle § X – Varování, není ustanovením dotčena.

Stanovit omezení jiným způsobem, například rozhodnutím Úřadu, by vyžadovalo, aby Úřad disponovat významně větším rozsahem informací o bezpečnostně významných dodávkách než vyžaduje předkládaná podoba návrhu. Dispozice s takovým rozsahem informací by ale pro tento účel nebyla přiměřená, jelikož lze požadovaného cíle dosáhnout i omezenějšími prostředky, které představuje navrhovaná podoba návrhu. Proces vydávání opatření obecné povahy navíc umožňuje jak povinným osobám mechanismu prověřování, tak dotčeným dodavatelům a dalším subjektům, uplatnit k návrhu opatření připomínky, které by měly zajistit přiměřenost a proveditelnost opatření, včetně lhůt k zavedení stanovených omezení.

Navrhovaná úprava procesu vydávání opatření obecné povahy využívá téměř v plném rozsahu obecnou právní úpravu správního řádu, kterou pro potřeby mechanismu prověřování bezpečnosti dodavatelského řetězce upravuje pouze v částech, které jsou typicky svázány s nemovitostmi a územním rozvojem a jsou tedy pro potřeby mechanismu nepřiléhavé. Návrh naopak doplňuje povinnost Úřadu pravidelně přezkoumávat trvání skutečností, na jejichž základě byla vydána omezení, aby byla v případě jejich pominutí bezodkladně zrušena.

K § X – Výjimky z omezení rizik spojených s dodavatelem

Pro případ, že by opatření obecné povahy vydané podle § X – Omezení rizik spojených s dodavatelem mohlo za konkrétních okolností podstatným způsobem ohrozit poskytování regulovaných služeb podle zákona, zavádí návrh možnost povolení výjimek z opatření obecné povahy. Výjimka může být povolena jak konkrétnímu subjektu, tak, jsou-li Úřadu známy obecně platné důvody pro udělení výjimky, všem poskytovatelům dotčené regulované služby či jinému okruhu subjektů.

Řízení o povolení výjimky se zahajuje pouze z moci úřední, kdokoliv však může dát podnět k zahájení řízení o povolení výjimky. Rozsah subjektů, na které by se měla výjimka použít, stanoví podle skutkových okolností Úřad. Úřadu návrh ukládá chránit při povolování výjimky v maximální možné míře účel opatření obecné povahy a povolit výjimku pouze v nezbytném rozsahu, kdy převáží potřeba nenarušení poskytování regulované služby nad potřebou omezení hrozby vyhodnocené v důsledku prověřování rizik spojených s dodavatelem. Dozví-li se Úřad o skutečnostech, pro které by měla být výjimka udělena všem povinným osobám mechanismu prověřování, vůči kterým směřuje opatření obecné povahy, může být na místě spíše než vydání výjimky změna či zrušení opatření obecné povahy.

K § X – Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce

Navrhované ustanovení ukládá povinným osobám mechanismu prověřování zjišťovat základní informace o dodavatelích bezpečnostně významných dodávek do své vymezené infrastruktury – kritické části stanoveného rozsahu, tyto informace dokumentovat a hlásit

je Úřadu. Ustanovení dále zahrnuje informace zjištěné Úřadem v rámci mechanismu prověřování bezpečnosti dodavatelského řetězce do evidence vedené a chráněné Úřadem podle § X – Evidence vedené úřadem.

Účelem této povinnosti je potřeba seznámení samotných povinných osob s dodavatelským řetězcem, aby na něj mohly řádně aplikovat opatření obecné povahy vydané podle § X – Omezení rizik spojených s dodavatelem a další povinnosti podle zákona, dále pak potřeba Úřadu získat informace o dodavatelích dodávajících svá plnění do vymezené infrastruktury, aby mohl řádně zaměřovat a prioritizovat jednotlivá prověřování podle § X – Prověřování rizik spojených s dodavatelem.

S ohledem na problematické vymezení přiměřené hloubky dodavatelského řetězce, na kterou by se měla vztahovat omezení rizik spojených s dodavatelem [viz odůvodnění k § X – Prověřování rizik spojených s dodavatelem odst. 3 písm. c)], stanoví návrh povinné osobě mechanismu prověřování vyvinout přiměřené úsilí k zjištění informací o dodavatelském řetězci, například skrze dotazování přímého dodavatele, s nímž povinná osoba vstoupila do smluvního vztahu, případně skrze dohledání informací o poddodavatelích dodavatele v otevřených zdrojích.

Jelikož bude hodnocení, zda povinná osoba v daném případě přiměřené úsilí vyvinula či nikoli, záležet vždy na konkrétních skutkových okolnostech, lze předpokládat potřebu zahrnout úpravu informování o dodavatelském řetězci do smluv povinných osob s dodavateli. Jako vhodné se rovněž jeví zavést u povinných osob compliance procesy, které budou vyvinutí přiměřeného úsilí v daném případě dokumentovat pro potřeby kontroly plnění povinností podle § X – Kontrola vykonávaná Úřadem. K posílení právní jistoty přiměřenosti vyvinutého úsilí může přispět rovněž výkladová praxe, například v podobě metodických a výkladových materiálů vydaných Úřadem.

K § X – Omezení rizik spojených s dodavatelem ve veřejných zakázkách

Návrh ustanovení v návaznosti na § 233 zákona o zadávání veřejných zakázek umožňuje poskytovatelům regulované služby zrušit závazek ze smlouvy na veřejnou zakázku nebo od takové smlouvy odstoupit, jestliže by plněním z takového závazku či smlouvy došlo k porušení opatření obecné povahy podle § X – Omezení rizik spojených s dodavatelem.

Ustanovení míří především na situace, kdy povinná osoba mechanismu v postavení zadavatele podle zákona o zadávání veřejných zakázek uzavře s dodavatelem smlouvu na veřejnou zakázku s takovou dobou či podmínkami plnění, které jí neumožňují ve lhůtě stanovené opatřením obecné povahy podle § X – Omezení rizik spojených s dodavatelem splnit jím stanovené podmínky či zákazy.

S ohledem na ochranu zásady *pacta sunt servanda* nicméně návrh podmiňuje využití tohoto práva zadavatele pouze, pokud jedná bez zbytečného odkladu poté, co zjistí, že byly předpoklady výkonu tohoto práva naplněny. V případě nedůvodného odkladu takového jednání povinná osoba právo na zrušení závazku či odstoupení od smlouvy pozbývá, jelikož převáží právo dodavatele na ochranu jeho smluvních závazků.

Smlouva na veřejnou zakázku, která by byla uzavřena až po vydání opatření obecné povahy podle § X – Omezení rizik spojených s dodavatelem a jejíž plnění by bylo s tímto opatřením v rozporu, by pak byla neplatná pro rozpor se zákonem, stejně jako se rozpor se zákonem dovozuje v případě porušení zákazu stanoveného vykonatelným konstitutivním rozhodnutím, které bylo vydáno na základě zákonného zmocnění.

Otázku vyloučení účastníka zadávacího řízení před uzavřením smlouvy na veřejnou zakázku by mělo řešit stanovení takových zadávacích podmínek, které zadavateli umožní

vyloučit účastníka z důvodu omezení stanoveného opatřením obecné povahy podle § X – Omezení rizik spojených s dodavatelem.

K § X – Povinnosti subjektů poskytujících služby registrace jmen domén

Subjekty poskytující služby registrace jmen domén (registrátoři domén) mají povinnost hlásit Úřadu své identifikační a kontaktní údaje a v případě změn je neprodleně aktualizovat. Úřad následně nahlášené údaje postoupí agentuře ENISA za účelem vytvoření registru těchto subjektů.

Povinnost registrátorů domén a subjektů spravujících a provozujících registr internetových domén nejvyšší úrovně (registr TLD) udržovat přesnou a úplnou databázi registračních údajů jmen domén (údajů v registru WHOIS) a poskytování zákonného přístupu k těmto údajům má zásadní význam pro zajištění bezpečnosti, stability a odolnosti systému jmen domén, což přispívá k vyšší společné úrovni kybernetické bezpečnosti v celé Unii. Právním titulem pro zpracování osobních údajů ze strany výše uvedených subjektů by v těchto případech mělo být plnění právní povinnosti ve smyslu čl. 6 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů (GDPR). Touto povinností není dotčena možnost shromažďovat údaje o registraci jmen domén i z jiných důvodů, například na základě smluvních ujednání nebo právních požadavků stanovených v jiných unijních nebo národních právních předpisech. Cílem této povinnosti je dosáhnout úplnosti a přesnosti souboru registračních údajů, neměla by nicméně vést k vícenásobnému shromažďování stejných údajů. V aktuální praxi je registr WHOIS na národní úrovni veden zájmovým sdružením CZ.NIC provozujícím registr TLD pro národní doménu .cz, kterému tyto údaje nahlašují jednotliví registrátoři domén.

Podle navrhované úpravy by registry TLD a registrátoři domén zejména měli stanovit politiky a postupy pro shromažďování a uchovávání přesných a úplných registračních údajů jména domény a rovněž zamezit uvádění nesprávných registračních údajů a opravovat je v souladu s právem Unie v oblasti ochrany osobních údajů. Za účelem ověřování údajů souvisejících s registrací jmen domén by měly být ze strany registrů TLD a registrátorů domén přijaty a zavedeny přiměřené postupy odrážející osvědčené postupy používané v daném odvětví a pokud možno pokrok dosažený v oblasti elektronické identifikace. Mezi příklady ověřovacích postupů mohou patřit kontroly *ex ante* prováděné v době registrace a kontroly *ex post* prováděné po registraci. Při zavádění postupů pro ověření totožnosti držitele jména domény mohou registry TLD a registrátoři domén využívat prostředky pro elektronickou identifikaci vydané v rámci kvalifikovaného systému elektronické identifikace. Ověření totožnosti držitele jména domény může být ze strany registrátory domén realizováno prostřednictvím registru TLD na základě uzavřené smlouvy.

Registry TLD a registrátoři domén mají povinnost zveřejňovat také údaje o registraci jmen domén, které jsou vyloučeny z oblasti působnosti práva Unie v oblasti ochrany osobních údajů, jako jsou údaje týkající se právnických osob. V případě právnických osob by měly být zveřejněny alespoň název žadatele o registraci a jeho kontaktní telefonní číslo. Kontaktní e-mailová adresa by měla být rovněž zveřejněna za předpokladu, že neobsahuje žádné osobní údaje, čehož může být dosaženo např. použitím e--mailové přezdívky. Registry TLD a registrátoři domén by také měli v souladu s právem Unie v oblasti ochrany osobních údajů umožnit oprávněným žadatelům přístup ke konkrétním údajům o registraci domén týkajících se fyzických osob. Postup poskytování přístupu může zahrnovat užívání rozhraní, portálu nebo jiných technických nástrojů k zajištění účinného systému žádostí o registrační údaje a přístupu k těmto údajům. Přístup k osobním i neosobním údajům o registraci jmen domén by měl být bezplatný.

Dostupnost a včasný přístup k údajům o registraci jmen domén pro oprávněné žadatele o přístup má zásadní význam pro prevenci zneužívání systému jmen domén a boj proti němu

a pro prevenci a odhalování incidentů a reakci na ně. Oprávněnými žadateli o přístup se rozumí jakákoli fyzická nebo právnická osoba, která podává žádost na základě práva Unie nebo národního práva. Mohou sem patřit orgány příslušné podle směrnice a orgány, které jsou podle unijního nebo národního práva příslušné pro prevenci, vyšetřování, odhalování či stíhání trestných činů, a skupiny CERT nebo týmy CSIRT. Registry TLD a registrátoři domén mají povinnost umožnit oprávněným žadatelům o přístup zákonný přístup ke konkrétním údajům o registraci jmen domén, které jsou nezbytné pro účely žádosti o přístup, v souladu s právem Unie a národním právem. K žádosti oprávněných žadatelů o přístup by mělo být přiloženo odůvodnění umožňující posoudit nezbytnost přístupu k údajům.

Plnění povinnosti shromažďovat a uchovat přesné a úplné údaje o registraci jmen domén ve vyhrazené databázi by nemělo vést ke zdvojování shromažďovaných dat. Povinnost bude splněna i pokud bude databáze vedena pouze jedním subjektem, kterému budou ostatní hlásit požadované informace. Za tímto účelem registrátoři domén a registry TLD vzájemně spolupracují.

K § X – Výjimka z práva na informace

Navržená úprava vychází z dosavadní právní úpravy obsažené v § 10a dosavadního zákona o kybernetické bezpečnosti. Výjimka z práva na informace obsažená v § 10a navazovala na omezující poskytování informací podle § 11 odst. 4 písm. f) zákona o svobodném přístupu k informacím.

Jak uvádí důvodová zpráva k novelizaci zákona o kybernetické bezpečnosti z roku 2017 jejímž obsahem byla právě nová úprava obsažená v budoucím § 10a zákona: „*Tato (dosavadní) úprava byla dle předkladatele tohoto návrhu zákona velmi omezená již v době přijímání (prvního znění) zákona o kybernetické bezpečnosti. V současné době, kdy již bylo určeno 155 významných informačních systémů, spravovaných 58 subjekty, a 48 systémů kritické informační infrastruktury, jejichž správci jsou orgány veřejné správy, tedy potenciálních povinných subjektů podle zákona o svobodném přístupu k informacím, a kdy roste počet útoků v kybernetickém prostoru, je zapotřebí přistoupit k opatření i v obecnější rovině zajišťování kybernetické bezpečnosti. Je zapotřebí zdůraznit, že v současnosti účinná výjimka uvedená v § 11 odst. 4 písm. f) zákona o svobodném přístupu k informacím nenaplňuje požadavky na ochranu citlivých informací, zejména těch, které se vztahují k přijatým bezpečnostním opatřením podle zákona o kybernetické bezpečnosti. Potenciální útočník by tak v současné době mohl požádat podle tohoto zákona správce informačních nebo komunikačních systémů kritické informační infrastruktury nebo správce významných informačních systémů o poskytnutí informací o přijatých bezpečnostních opatřeních, přičemž tento povinný subjekt by byl povinen je poskytnout.* [...] *Informace, které není v zájmu zajišťování kybernetické bezpečnosti možné poskytovat, mohou být například následující: schémata, plány budov, technické specifikace (např. topologie sítě), konfigurační parametry, havarijní plány.“* Dosavadní úprava obsažená v § 10a zákona také dále rozšiřovala výjimku na informace, jejichž zpřístupnění by mohlo ohrozit účinnost opatření podle § 11 dosavadního zákona.

Úřad k tomuto tématu vydal také stanovisko ve formě podpůrného materiálu kde uvádí především následující: *„Při posuzování, zda by poskytnutí určité informace mohlo ohrozit zajišťování kybernetické bezpečnosti, je nezbytné zvážit, které informace jsou z hlediska zachování kybernetické bezpečnosti natolik důvěrné, že by jejich vyzrazením mohlo dojít k jejímu narušení. Taková informace by měla z pohledu důvěrnosti odpovídat úrovni „vysoká“ nebo „kritická“ podle přílohy č. 1 vyhlášky o kybernetické bezpečnosti. Pokud by zpřístupněním takové informace mohlo dojít k narušení kybernetické bezpečnosti, je podle názoru Úřadu nezbytné aplikovat § 10a zákona kybernetické bezpečnosti a takovou informaci neposkytnout. Tímto způsobem je vhodné ohodnotit například technickou či bezpečnostní*

dokumentaci (jejichž ochrana je akcentována i skutečností, že v komplexní podobě mohou být chráněny i podle zákona o ochraně utajovaných informací). Stejně tak je potřeba postupovat v případě informace, jejíž zpřístupnění by mohlo ohrozit účinnost opatření vydaného podle zákona o kybernetické bezpečnosti. Jak z ustanovení samotného plyne, bude se v tomto případě jednat o informaci, jejíž zveřejnění by mohlo mít negativní dopad na opatření vydané podle zákona o kybernetické bezpečnosti."

Na potřebě zachovat výjimku ve formě obecného *„ohrožení zajišťování kybernetické bezpečnosti"* nic nemění také skutečnost, že zákon o svobodném přístupu k informacím obsahuje s účinností od 24. dubna 2019 nové ustanovení § 11 odst. 1 písm. d) a v rámci něj možnost omezit poskytnutí informace, pokud *„její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku"*. Toto ustanovení je tak potřeba vnímat jako doplňující především tam, kde půjde o informace o bezpečnostních opatřeních podle zákona o kybernetické bezpečnosti, ale zároveň tyto informace nedosahují svou důvěrností úrovně „*vysoká*" nebo „*kritická*".

Na tuto dosavadní právní úpravu navazuje i navrhovaná úprava, která zachovává tři směry výjimky z práva na informace:

- zpřístupnění informace by mohlo ohrozit zajišťování kybernetické bezpečnosti,
- zpřístupnění informace by mohlo ohrozit účinnost protiopatření vydaného podle tohoto zákona, nebo
- byla by zpřístupněna informace, která je vedena v evidencích vedených Úřadem.

Navrhovaná úprava je oproti dosavadní právní úpravě rozdílná jen v případě rozšíření výjimky z evidence incidentů na všechny evidence, které jsou Úřadem vedeny. Přestože je navrhovanou úpravu možno vnímat jako rozšíření výjimky z práva na informace, jedná se v případě obsahu evidencí fakticky o informace, které je možno považovat z povahy věci za informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, a také k tomu tak (především v případě evidence povinných orgánů a osob) bylo dosud přistupováno. Návrh zákona důsledně rozlišuje pojem evidence a pojem seznam, přičemž na seznamy se tato výjimka neuplatní a uplatnit nemá (jedná se o veřejné informace). Výčet evidencí je taxativní a je uveden v samostatném ustanovení v návrhu zákona.

Předkladatel tohoto návrhu zákona se domnívá, že toto omezení práva na informace je plně v souladu s dosavadním zákonem o kybernetické bezpečnosti a především čl. 17 odst. 4 Listiny základních práv a svobod, když je stále toho názoru, že v oblasti kybernetické bezpečnosti, která hraje v oblasti bezpečnosti státu stále důležitější roli, převážil požadavek na zajištění bezpečnosti státu a veřejné bezpečnosti. Zároveň je nutné konstatovat, že povinný subjekt bude při rozhodování o žádosti o poskytnutí informací vždy povinen posoudit, zda by opravdu poskytnutí požadované informace mohlo ohrozit zajišťování kybernetické bezpečnosti a pečlivě v daném případě zvažovat potřebu omezení práva na informace.

Vzhledem k tomu, že také dosavadní právní úprava této výjimky byla vzhledem ke specifičnosti oblasti kybernetické bezpečnosti začleněna do obsahu zákona o kybernetické bezpečnosti, a ne do zákona o svobodném přístupu k informacím, přistupuje k této problematice návrh tohoto zákona stejně.

K § X – Ochrana informací

Při postupu Úřadu podle § X *[Varování]*,§X *[Omezení rizik spojených s dodavatelem]* a § X *[Výjimky z omezení rizik spojených s dodavatelem]* se, zejména v souvislosti s prověřováním a omezováním rizik spojených s dodavatelem, předpokládá dispozice

se značným množstvím utajovaných a jiných citlivých neveřejných informací (vč. například informací podléhající zákonem stanovené či uznané povinnosti mlčenlivosti), vyžadujících v souladu s jinými právními předpisy významně zvýšenou míru ochrany. Za tímto účelem se informace, s nimiž jiná právní úprava takovou zvýšenou míru ochrany pojí, uchovávají mimo spis a nelze vůči nim vykonávat právo nahlížení do spisu podle správního řádu.

V případě soudního přezkumu se pravidla o omezení nahlížení do spisu uplatní, v souladu se soudním řádem správním, také. Soud však bude rozhodovat se znalostí všech podkladů, včetně těch, které jsou uchovávány mimo spis.

K § X – Stav kybernetického nebezpečí

Toto ustanovení upravuje problematiku stavu kybernetického nebezpečí od přípravy na jeho řešení, vyhlášení až po samotné řešení vzniklých kybernetických bezpečnostních incidentů a událostí. Vzhledem k tomu, že zákon je postaven na principu minimalizace zásahu do autonomie vůle subjektů působících v kybernetickém prostoru, jsou zákonné povinnosti vyplývající ze zákona o kybernetické bezpečnosti za normální situace ukládány pouze těm orgánům a osobám, které poskytují zákonem a vyhláškou specifikované regulované služby, a jejichž systémy jsou tudíž vysoce bezpečnostně exponovány, tj. regulovaným subjektům. Zahraniční zkušenosti však ukazují, že může dojít k tak masivnímu ohrožení nebo narušení kybernetické bezpečnosti, že v jeho důsledku mohou být ohroženy nebo dokonce poškozeny fundamentální národní zájmy. Nelze-li takový incident zvládnout za užití standardních mechanismů zákona, může ředitel Úřadu rozhodnout o vyhlášení stavu kybernetického nebezpečí, v němž dojde k rozšíření osobní působnosti zákona i mimo okruh subjektů, na něž zákon o kybernetické bezpečnosti dopadá, tak aby mohly být dostatečně zabezpečeny chráněné zájmy České republiky vymezené v odst. 1 řešeného ustanovení.

Proces vyhlašování stavu kybernetického nebezpečí je upraven analogicky s krizovým zákonem. O vyhlášení stavu kybernetického nebezpečí rozhoduje ředitel Úřadu, který rovněž rozhoduje o prodloužení stavu kybernetického nebezpečí, přičemž ten může být prodloužen pouze se souhlasem vlády.

Rozhodnutí o vyhlášení stavu kybernetického nebezpečí zveřejní Úřad na své úřední desce a dalšími vhodnými způsoby, které zajistí, že budou adresáti, zejména osoby a orgány povinné k provádění či strpění opatření, dostatečně informováni o vyhlášení stavu kybernetického nebezpečí a jeho povaze. K tomu může Úřad využít například veřejná média jako televizní či rozhlasové vysílání, zveřejnění na internetových stránkách Úřadu a dalších organizací, zveřejnění na sociálních sítích a podobně. S ohledem na závažnost a urgentní povahu stavu kybernetického nebezpečí bylo přistoupeno k udělení povinnosti provozovatelům celoplošného televizního nebo rozhlasového vysílání, kteří jsou povinni bez náhrady nákladů na základě žádosti Úřadu neprodleně a bez úpravy obsahu a smyslu uveřejnit informace o vyhlášení stavu kybernetického nebezpečí.

Pro vyhlášení i prodloužení stavu kybernetického nebezpečí platí vedle obecných právních principů též konkrétní materiální omezení uvedená v tomto ustanovení. Stav kybernetického nebezpečí lze vyhlásit, respektive prodloužit pouze ze zákonného důvodu, na dobu nezbytně nutnou k vyřešení ohrožení, které bylo důvodem jeho vyhlášení, a pouze tehdy, nelze-li důvod jeho vyhlášení řešit běžnou činností Úřadu podle tohoto zákona.

Stav kybernetického nebezpečí, jako stav mimořádný, je koncipován jako stav mimo režim krizového zákona, byť z něj vychází a v mnoha ohledech na něj navazuje, i mimo režim ústavního zákona o bezpečnosti České republiky. Stav kybernetického nebezpečí však bylo nutno provázat s mimořádnými (krizovými) stavy podle těchto právních předpisů. Byla tak zachována konstrukce, že v případě, kdy je zřejmé, že na odvrácení škodlivého následku, který

vedl k vyhlášení stavu kybernetického nebezpečí, nedostačují postupy a prostředky přijaté podle návrhu zákona o kybernetické bezpečnosti, navrhne ředitel Úřadu vládě, aby byl vyhlášen nouzový stav. Toto propojení bylo zakotveno již v § 21 odst. 6 dosavadního zákona o kybernetické bezpečnosti, tento zákon jej tak v zásadě přejímá v nezměněné podobě.

Za situace, kdy nebude možno zajistit bezpečnost informací v informačních systémech nebo bezpečnost služeb nebo sítí elektronických komunikací v rámci vyhlášeného stavu kybernetického nebezpečí, je ředitel Úřadu povinen požádat předsedu vlády o vyhlášení nouzového stavu podle ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.

S ohledem na podobnost obou institutů a zákonných úprav, je možné při řešení otázek, které zákonná úprava stavu kybernetického nebezpečí v tomto zákoně neupravuje, vyjít podpůrně z ustanovení krizového zákona. V úvahu připadají například ustanovení hlavy V a VI krizového zákona.

K § X – Opatření k řešení stavu kybernetického nebezpečí

Toto ustanovení stanovuje strukturu oprávnění Úřadu a povinností orgánů a osob ve vztahu k řešení kybernetických bezpečnostních incidentů, omezení jejich dopadů a jejich předcházení během stavu kybernetického nebezpečí. Z dosavadních zkušeností při řešení mimořádných událostí a krizových situací v České republice i v zahraničí vyplývá potřeba specifické úpravy práv a povinností relevantních orgánů a osob.

Opatření pro řešení stavu kybernetického nebezpečí je oprávněn vydávat a nařizovat ředitel Úřadu, a to v reakci na aktuální hrozbu v oblasti kybernetické bezpečnosti nebo v reakci na konkrétní kybernetické bezpečnostní incidenty. Úřad je oprávněn aplikovat následující opatření pro řešení stavu kybernetického nebezpečí vůči subjektům v České republice:

- Úřad může v případě potřeby poskytnout věcné prostředky, které má v užívání a které jsou nezbytné k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem. Tímto se rozumí zejména hardware a software. Osoba, které byly věcné prostředky poskytnuty pro řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem, tyto Úřadu navrátí po pominutí důvodů, které vedly k jejich zapůjčení. Případně je tato osoba povinna Úřadu věcný prostředek nahradit jiným způsobem.
- Úřad si může v případě potřeby vyžádat u předem zasmluvněných osob a orgánů informace o personálních kapacitách a věcných prostředcích, kterými disponují, a požádat o přednostní poskytnutí, resp. sdílení, těchto personálních kapacit nebo věcných prostředků. Informace nejprve Úřadu poskytnou přehled o možnostech subjektu zapojit se do řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem. Tato forma spolupráce se předpokládá zejména s dalšími státními orgány, případně s provozovatelem Národního CERT.
- V případě potřeby může Úřad nařídit dotčeným osobám práci v pohotovostním režimu. Práce v pohotovostním režimu může být vyžádána zejména z důvodu potřeby řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem. Za práci v pohotovostním režimu přísluší dotčeným osobám adekvátní náhrada.
- V případě potřeby si Úřad může vyžádat 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. Toto opatření se použije zejména při řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem ve specifickém odvětví, o kterém nemá Úřad dostatečné znalosti a kde mu chybí věcné prostředky. Specifickým odvětvím se tímto rozumí odvětví na jehož zabezpečení a provoz se využívají prostředky informačních technologií a sítí elektronických komunikací, které se běžně nepoužívají nebo vyžadují vysokou specializaci osob zajišťujících jejich provoz.

- Úřad má možnost 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, Úřad toto opatření použije zejména v případech, kdy by další používání dotčených technických aktiv mohlo způsobit rozsáhlejší škody.
- Úřad může 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, pokud pro řešení situace nepostačuje vydání reaktivního protiopatření. Tato povinnost poskytne Úřadu přehled o stavu a způsobu provedených opatřeních. Jedná se o rozšíření povinnosti vyplývající z obecné úpravy v zákoně o kybernetické bezpečnosti i na další orgány a osoby, na které se obecná úprava mimo stav kybernetického nebezpečí nevztahuje, a nepostačovalo by tak užití institutu reaktivního protiopatření.
- V rámci řešení kybernetického bezpečnostního incidentu může Úřad nařídit provedení skenu zranitelností. Za účelem zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem pak může nařídit provedení skenu zranitelností nebo penetračního testu.
- Úřad může nařídit orgánům a osobám zpřístupnění neveřejných komunikačních sítí v jejich správě pro potřeby Úřadu. Toto opatření se použije pokud je zpřístupnění neveřejných komunikačních sítí nezbytné pro řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem.

V odst. 2 je zrcadlově k opatřením v odst. 1 konstituována povinnost osob a orgánů tato opatření strpět nebo zavést a spolupracovat s Úřadem během řešení stavu kybernetického nebezpečí.

K § X – Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost byl zřízen novelizací zákona o kybernetické bezpečnosti zákonem č. 205/2017 Sb., s účinností od 1. srpna 2017.

Dosavadní zákon o kybernetické bezpečnosti upravoval postavení Úřadu hned v několika ustanoveních. Jednalo se především o § 21a, pojednávající o jeho zřízení a postavení ředitele Úřadu, dále o § 22 stanovující jeho pravomoci, a stejně tak o § 20, který upravoval postavení Vládního CERT *„jako součásti Úřadu“*.

Tímto ustanovením návrhu zákona dochází k logickému sloučení těchto výše uvedených ustanovení do jednoho paragrafu.

V rámci odst. 1 tohoto ustanovení se jedná o převedení původního znění § 21a odst. 1, tedy ustanovení o existenci Úřadu, vytyčení jeho činnosti, důvodu existence a poslání, stejně tak jako jeho základní zakotvení – jak v rámci území České republiky, tak v rámci otázky financování jeho fungování.

Obsah odst. 2 upravuje postavení ředitele Úřadu a jedná se o doslovné znění původního § 21a odst. 2 a 3.

Pravomoci Úřadu jsou dány v rámci tohoto návrhu v odst. 3 a 4, přičemž základní rozdělení mezi těmito odstavci je stanovena tím způsobem, že v odst. 3 jsou uvedeny činnosti výslovně spjaté s procesy uvedenými v tomto návrhu zákona, především s činnostmi spojenými s poskytovateli regulovaných služeb. Jedná se tak např. o jejich identifikaci, registraci, zápis a vedení evidence, stejně tak jako o jejich další plnění povinností, ale také vedle poskytovatelů regulovaných služeb o činnosti spojené s vyhlašováním stavu kybernetického nebezpečí nebo pozastavení evropského certifikátu kybernetické bezpečnosti a další. Úřad však jako gestor pro oblast kybernetické bezpečnosti a pro vybrané oblasti ochrany utajovaných informací podle zákona o ochraně utajovaných informací vykonává řadu dalších činností. Tyto činnosti jsou uvedeny v odst. 4, přičemž se jedná o činnosti výzkumné a vývojové, koordinační, kooperační, preventivní nebo činnosti vedoucí k realizaci mezinárodní spolupráce. Tento odstavec také reflektuje evropské právní předpisy a úlohu, kterou na základě nich plní Úřad v rámci České republiky.

Oproti dosavadnímu znění zákona o kybernetické bezpečnosti je původní § 20 – Vládní CERT – přesunut přímo pod ustanovení o činnosti Úřadu a to do posledního odst. 5. Tato textová změna je analogická k ustanovení o Národním CERT a provozovateli Národního CERT, která jsou v dosavadním znění zákona rozdělena do dvou (§ 17 a § 18), přičemž tento návrh zákona je také spojuje. Existence Vládního CERT historicky přesahuje existenci Úřadu a datuje se k usnesení vlády č. 781 ze dne 19. října 2011, které uložilo řediteli Národního bezpečnostního úřadu vybudovat do konce roku 2015 plně funkční Národní centrum kybernetické bezpečnosti, jakož i vládní koordinační místo pro okamžitou reakci na počítačové incidenty – tedy Vládní CERT. Vládní CERT je koncipován jako centrální veřejnoprávní pracoviště a veřejnoprávní „single point of contact“ pro oblast kybernetické bezpečnosti. Jeho činnost zahrnuje příjem kontaktních údajů od vybraných orgánů a osob, příjem informací o kybernetické bezpečnostní situaci, a to zejména příjem povinných a iniciativních hlášení kybernetických bezpečnostních incidentů a dalších údajů o kybernetické bezpečnostní situaci od tuzemských a zahraničních orgánů veřejné moci a spolupracujících subjektů a jejich vyhodnocování. Vládní CERT dále poskytuje součinnost vybraným typům orgánů a osob při výskytu kybernetického bezpečnostního incidentu, zajišťuje součinnost s ostatními orgány a subjekty zajišťujícími kybernetickou bezpečnost v České republice a ve spolupracujících nebo spojeneckých státech a rovněž provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti, jehož předmětem je zkoumání známých zranitelností a koordinace jejich řešení. Vládní CERT je také koordinátorem pro zveřejňování zranitelností v souladu s čl. 12 odst. 1 směrnice.

K § X – Provozovatel Národního CERT

Toto ustanovení zakotvuje obecné podmínky pro výběr provozovatele Národního CERT a způsob jejich prokázání. V souvisejícím ustanovení o náležitostech veřejnoprávní smlouvy s provozovatelem Národního CERT podle tohoto zákona je současně upraven způsob založení závazku k provozování Národního CERT formou veřejnoprávní smlouvy uzavřené s Úřadem. Užití institutu veřejnoprávní smlouvy odpovídá předpokladu, že provozovatelem Národního CERT bude osoba soukromého práva. Závazky provozovatele Národního CERT vykonávat činnosti uvedené v tomto zákoně mají sice převážně charakter soukromoprávní, ve vztahu k poskytovatelům regulovaných služeb v režimu nižších povinností však bude provozovatel Národního CERT vystupovat jako subjekt, vůči němuž tyto orgány a osoby plní svou zákonnou povinnost hlášení kybernetických bezpečnostních incidentů.

Vzhledem k tomu, že Národní CERT je pracovištěm velkého významu pro systém kybernetické bezpečnosti České republiky, vyžaduje se, aby provozovatel nevyvíjel činnost proti zájmům České republiky ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Bezúhonnost a neexistence splatných finančních závazků vůči státu jsou v případě spolupráce státu a osoby soukromého práva standardně požadovanými formálními podmínkami. Zákon rovněž formuluje materiální předpoklady výkonu funkce provozovatele Národního CERT, přičemž se požaduje, aby provozovatel Národního CERT prokázal faktické schopnosti a zkušenosti s provozem a správou relevantních technických aktiv, a to po dobu nejméně 5 let, dále technické předpoklady k výkonu činnosti uložené mu tímto zákonem, jakož i schopnost pracovat v součinnosti se zahraničními subjekty působícími na úseku kybernetické bezpečnosti.

Model standardně soukromoprávního výkonu funkcí Národního CERT usnadňuje komunikaci mezi Národním CERT a orgány a osobami využívajícími jej povinně jako kontaktní místo. Národní CERT se bude také moci zapojit do mezinárodních sítí obdobných soukromoprávních pracovišť typu CERT a těžit z poznatků, které se v rámci těchto sítí neformálně předávají. Předpokládaný soukromoprávní charakter Národního CERT je vzhledem ke smyslu a účelu zákona vhodný i z toho důvodu, že provozovatel Národního CERT není ve své činnosti zcela omezen zásadou enumerativnosti veřejnoprávních pretenzí a může z pozice osoby soukromého práva iniciativně provádět také další činnosti k dosažení účelu zákona, samozřejmě v jeho mezích a v mezích smlouvy uzavřené s Úřadem. Provozovatel Národního CERT tak bude moci například poskytovat metodickou a informační pomoc i subjektům stojícím mimo osobní působnost zákona, tj. osobám mimo definice jednotlivých kategorií orgánů a osob, které o to projeví zájem. Národní CERT bude moci dále vyvíjet vlastní vzdělávací, publikační, výzkumnou nebo vývojovou činnost apod. Podmínkou omezující iniciativně vykonávané činnosti Národního CERT k dosažení účelu tohoto zákona je samozřejmě také jejich bezrozpomost s plněním povinností vyčtených v zákoně taxativně.

Ustanovení dále vymezuje činnost Národního CERT, který bude sloužit zejména jako společné kontaktní a koordinační místo pro poskytovatele regulovaných služeb v režimu nižších povinností a osoby, na které nebude dopadat zákon o kybernetické bezpečnosti. Národní CERT bude Úřadu předávat informace o nahlášených kybernetických hrozbách, kybernetických bezpečnostních událostech, kybernetických bezpečnostních incidentech a zranitelnostech v oblasti kybernetické bezpečnosti. V případě kybernetických bezpečnostních incidentů s významným dopadem na kontinuitu poskytování regulované služby bude Národní CERT plnit informační povinnost jak vůči Úřadu, tak vůči jiným členským státům, na jejichž území by mohlo dojít k narušení kontinuity zasažené služby. V neposlední řadě bude Národní CERT plnit roli CSIRT týmu podle směrnice.

Zákon dále požaduje, aby provozovatel Národního CERT plnil povinnosti svěřené mu tímto zákonem nestranně a koordinoval svou činnost s Úřadem. Činnosti nezbytné pro zajištění kybernetické bezpečnosti České republiky a plnění požadavků příslušné unijní legislativy vykonává provozovatel Národního CERT vůči Úřadu bezúplatně, což úzce souvisí s požadavkem dle odst. 1 písm. h) řešeného ustanovení, dle kterého musí být provozovatel Národního CERT osobou, která nebyla založena nebo zřízena výlučně za účelem dosažení zisku, čímž není dotčena možnost provozovatele Národního CERT vlastním jménem a na vlastní odpovědnost vykonávat i další hospodářskou činnost v oblasti kybernetické bezpečnosti neupravenou tímto zákonem, pokud tato činnost nenaruší plnění povinností dle odst. 3. Činnost Národního CERT by měla být vykonávána výhradně ve veřejném zájmu s důrazem na zachování důvěrnosti informací obdržených od subjektů tak, aby byla zachována důvěra těchto subjektů v Národní CERT.

K § X – Inspektoři

V prvé řadě je třeba uvést, proč nová právní úprava zavádí institut autorizovaného inspektora. Nově zaváděná kritéria pro určení poskytovatele regulované služby markantně navýší počty povinných osob, v řádech tisíců oproti současnému stavu. Jedná se zejména o okruh poskytovatelů regulovaných služeb v režimu nižších povinností.

Z těchto důvodů je zapojení autorizovaných inspektorů primárním způsobem prověření plnění povinností ze strany poskytovatelů regulovaných služeb v režimu nižších povinností. Díky udělené autorizaci inspektora dochází k přenesení části výkonu veřejné správy na tyto fyzické osoby, které budou následně kontrolu poskytovatelů regulovaných služeb v režimu nižších povinností pro Úřad zajišťovat. Nad výkonem činnosti inspektorů přitom bude dohled vykonávat Úřad.

Vzhledem k tomu, že takto přenáší Úřad na inspektory část své dohledové činnosti, musí tyto osoby projít procesem autorizace. Při něm si Úřad ověří splnění požadavků, které na inspektory klade v odst. 1. Základní podmínkou je řádně podaná žádost fyzické osoby o udělení autorizace, ke které žadatel připojí doklady prokazující, že je bezúhonný, že nebyl v posledních 3 letech před podáním žádosti potrestán pokutou ve výši nejméně 100 000 Kč za přestupek podle tohoto zákona a že splňuje požadavky na odbornou způsobilost, tj. vzdělání a praxi a zároveň úspěšně složil zkoušku inspektora. Podrobnosti k těmto požadavkům stanovuje prováděcí právní předpis.

Jelikož Úřad rozhoduje o stanovení požadavků pro udělení autorizace inspektora a vede řízení o žádosti fyzické osoby o udělení autorizace, je to právě Úřad, kdo podle odst. 2 zajišťuje a organizuje zkoušku inspektora. Vzhledem k tomu, že se bude jednat o poměrně náročnou odbornou činnost, ponese sebou zajištění a organizace zkoušky náklady na provoz. Tyto náklady budou částečně pokryty poplatky za vykonání zkoušky, jež jsou příjmem Úřadu. Pravidla, forma a průběh zkoušky jsou podrobněji stanoveny v prováděcím právním předpise.

Podle odst. 3 musí žadatel zkoušku složit nejpozději do 6 měsíců ode dne zahájení řízení o žádosti. Žadatel může zkoušku opakovat pouze jednou. Pokud žadatel nestihne zkoušku splnit ve stanovené lhůtě nebo u zkoušky dvakrát neuspěje, bude jeho žádost o udělení autorizace zamítnuta. Je tak na odpovědnosti žadatele, aby se ve stanovené lhůtě na vypsaný termín přihlásil a zkoušku složil.

Novou žádost o udělení autorizace může podle odst. 4 podat žadatel nejdříve 6 měsíců od pravomocného skončení předchozího řízení, resp. zamítnutí žádosti. Vzhledem k tomu, že zamítnutí žádosti podle odst. 3 je navázáno na nesložení zkoušky inspektora, jeví se jako vhodné posunout možnost opakovat celé řízení včetně skládání zkoušky tak, aby měl žadatel přiměřený čas se znovu a lépe připravit. Toto posunutí má za cíl zabránit tomu, aby se žadatelé snažili zkouškou projít formou pokusu a omylu. V takovém případě by totiž nemuselo dojít k dostatečnému ověření odborné způsobilosti žadatele.

Autorizaci uděluje Úřad rozhodnutím na 3 roky. Jednou z podmínek pro udělení autorizace je mj. složení zkoušky inspektora. Zkušební otázky budou neustále aktualizovány, díky čemuž si Úřad vždy ověří potřebnou aktuální úroveň znalostí daného žadatele. Vzhledem k tomu, že je oblast kybernetické bezpečnosti dynamické prostředí a s tím související technologie se neustále vyvíjí, byla délka platnosti autorizace stanovena na 3 roky, přestože je v jiných oborech běžné autorizaci udělovat třeba i na 5 let. Z výše uvedených důvodu si Úřad rovněž ponechal možnost v rozhodnutí o udělení autorizace stanovit další podmínky pro výkon činnosti inspektora a ty tak v případě potřeby rozšířit.

Důležitým institutem této úpravy je seznam inspektorů vedený Úřadem. Úřad na základě rozhodnutí o autorizaci inspektora zapíše žadatele na tento seznam. Platí zde přitom

vyvratitelná právní domněnka, že fyzická osoba zapsaná v tomto seznamu je autorizovaným inspektorem. Seznam inspektorů slouží primárně pro potřebu poskytovatelů regulovaných služeb v režimu nižších povinností. V seznamu budou uvedeny zejména kontaktní údaje a informace o platnosti autorizace, tedy údaje potřebné pro výběr inspektora.

Platnost autorizace lze prodloužit o další 3 roky rozhodnutím Úřadu na základě písemné žádosti žadatele. Postupuje se přitom obdobně jako při žádosti o udělení autorizace, tedy podle odst. 1 až 5. O prodloužení může žadatel požádat nejdříve 6 měsíců před koncem platnosti již udělené autorizace. Zároveň musí žadatel stihnout o prodloužení autorizace požádat před uplynutím její platnosti. V takovém případě platnost původní autorizaci neskončí dříve než bude o žádosti o prodloužení autorizace pravomocně rozhodnuto. Žadatel, který vykonává činnost inspektora a následně podá ve stanoveném časovém období žádost o prodloužení autorizace, tím dává jasně najevo svůj zájem v činnosti inspektora pokračovat. Prodloužením autorizace na dobu, než bude rozhodnuto o jeho žádosti o prodloužení, tak bude zabráněno tomu, aby byl inspektor ze seznamu inspektorů vymazán. Takový stav by mohl způsobit komplikace především u již probíhajících kontrol. Tímto způsobem je však kontinuita vykonávaných kontrol zajištěna.

Na žádost inspektora lze jeho autorizaci podle odst. 8 pozastavit z konkrétně vymezených důvodů, nejdéle však na 1 rok. V případě, že je autorizace pozastavena, nesmí inspektor vykonávat žádnou kontrolu. Během pozastavení autorizace tak nelze inspektora ustanovit rozhodnutím Úřadu k výkonu kontroly.

Úřad autorizaci inspektora odebere i před uplynutím délky její platnosti, pokud o to sám inspektor požádá nebo pokud přestane inspektor splňovat požadavky, na základě kterých mu byla autorizace původně udělena. Z toho plyne, že inspektor musí požadavky pro udělení autorizace splňovat po celou dobu platnosti autorizace, resp. výkonu činnosti inspektora a nikoliv pouze v době posouzení žádosti o udělení autorizace a jejího udělení. Na základě pravomocného rozhodnutí o odebrání autorizace Úřad inspektora vymaže ze seznamu inspektorů.

K § X – Stálá komise pro kontrolu činnosti Úřadu

Návrh tohoto ustanovení beze změn navazuje na ustanovení § 24a, § 24b a § 24c dosavadního zákona o kybernetické bezpečnosti a je tak také možné zcela odkázat na důvodovou zprávu k zákonu č. 35/2018 Sb., o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny, která toto ustanovení do dosavadního zákona o kybernetické bezpečnosti přinesla.

Způsob vytvoření zvláštních kontrolních orgánů (a především stanovení minimálního počtu členů tak, aby v něm byly zastoupeny všechny poslanecké kluby) tohoto typu je vedle tohoto návrhu zákona upraven obdobně také v celé řadě dalších právních předpisů (např. zákona o zpravodajských službách České republiky, o Bezpečnostní informační službě, o Vojenském zpravodajství, o ochraně utajovaných informací a o bezpečnostní způsobilosti, apod.) a tvoří tak společně soustavu obdobných ustanovení upravujících tento institut.

K § X – Portál NÚKIB

Portál NÚKIB slouží k vykonávání digitálních úkonů ze strany poskytovatelů regulovaných služeb, resp. poskytování digitálních služeb a sdílení informací ze strany Úřadu. Jde o komunikační platformu, která umožňuje oboustrannou komunikaci mezi Úřadem a regulovanými subjekty, zejména snadné provádění standardizovaných podání vůči Úřadu. S výjimkou možnosti registrace poskytovatele regulované služby není Portál NÚKIB veřejně přístupný a přistupovat do něj mohou pouze subjekty, jimž byly přiděleny přihlašovací údaje.

Většina podání (např. hlášení kontaktních údajů, incidentů nebo provedení protiopatření) bude činěna prostřednictvím standardizovaných formulářů, které umožní předvyplnění mnoha informací, které Úřad u konkrétní organizace již eviduje. Používání takových podání v rámci Portálu NÚKIB umožňuje automatizované zpracování na straně Úřadu, nadto dochází ke snížení administrativní zátěže na straně poskytovatelů regulovaných služeb.

Koncept Portálu NÚKIB a v něm prováděné postupy či podání jsou v souladu se zákonem o právu na digitální službu a zásadami obsaženými v Informační koncepci ČR a Zásadami pro tvorbu digitálně přívětivé legislativy. Vznik kontaktního místa ve formě platformy využívající on-line formuláře a automatizaci navíc explicitně zmiňuje recitál 106 směrnice NIS2.

Odstavec 2 odkazem na odpovídající ustanovení zákona stanovuje taxativní výčet úkonů, které lze provést výlučně prostřednictvím Portálu NÚKIB a odpovídajícího formuláře. Tento přístup přitom není v rozporu s § 14 zákona o právu na digitální služby, který sice stanovuje zákaz povinného využívání digitálních služeb a činění digitálních úkonů, ale pouze ve vztahu k nepodnikajícím fyzickým osobám. Poskytovatelé regulovaných služeb jsou v drtivé většině právnické osoby nebo organizační složky státu, teoreticky ve zcela výjimečných případech podnikající fyzické osoby, na něž se však citovaný zákaz nevztahuje. Nadto jsou v dílčích zákonných ustanoveních obsaženy náhradní způsoby provedení úkonů a podmínky jejich použití. Účelem je zajištění komunikace i v případě, kdy by došlo k objektivní nemožnosti využít Portál NÚKIB, ať už z důvodů na straně Úřadu (např. nedostupnost Portálu NÚKIB), nebo samotného poskytovatele regulované služby (např. nedostupnost internetového připojení).

Odstavec 3 vylučuje aplikaci ustanovení § 30 správního řádu, které upravuje provádění úkonů jménem právnické osoby, a to z toho důvodu, že úprava odpovídající správnímu řádu, resp. občanskému soudnímu řádu, na který je odkazováno, není technicky proveditelná, tak aby byla možná automatická autentizace a identifikace relevantních jednajících osob. V případě absence automatické autentizace a identifikace osob jednajících za poskytovatele regulovaných služeb by Úřadu hrozila nepřiměřená administrativní zátěž způsobující značné průtahy zejména při prvotní registraci těchto subjektů. Zvolené řešení nikterak nelimituje práva adresátů této právní úpravy a pouze navazuje na dostupná technologická řešení při využití referenčních údajů vedených v základních registrech. Veškeré náležitosti činění úkonů prostřednictvím Portálu NÚKIB, včetně vymezení oprávněných a pověřených osob, jsou přitom upraveny ve vyhlášce o Portálu NÚKIB.

Poslední odstavec, odstavec 4, obsahuje pouze zmocňovací ustanovení, na základě kterého bude vydávána vyhláška o Portálu NÚKIB, která stanovuje technické a organizační podmínky používání portálu a obsahové náležitosti veškerých formulářových podání v souladu s nálezem Ústavního soudu ze dne 12. listopadu 2019, sp. zn. Pl. ÚS 19/17.

K § X – Evidence vedené Úřadem

Úřad vede v rámci zajištění své činnosti evidence, přičemž zákon důsledně rozlišuje ve své terminologii mezi pojmy evidence a seznam. Vymezení evidencí vedených Úřadem v odstavci 1 je úzce provázáno s výjimkou z práva na informace upravenou v tomto zákoně. Právě z těchto evidencí nelze poskytovat informace na základě předpisů upravujících svobodný přístup k informacím, protože u těchto evidencí by zveřejňování citlivých informací v nich obsažených vedlo k ohrožení zajišťování kybernetické bezpečnosti. Naopak v případě seznamů, pokud zákon tento termín používá, se jedná o vedení informací, které jsou *a priori* veřejné.

Odstavec 2 pak stanovuje, že údaje obsažené ve vymezených evidencích lze poskytovat ostatním orgánům veřejné moci, nicméně pouze na základě jejich žádosti, a je-li to nezbytné pro výkon jejich působnosti. Zaslaná žádost zároveň určuje účel využití poskytnutých informací.

Odstavec 3 umožňuje sdílení údajů o incidentech událostech a hrozbách mezi Úřadem a relevantními partnery, což souvisí s funkčním nastavením koordinačních mechanismů a vzájemné spolupráci při řešení incidentů, ať už na základě směrnice nebo jiných předpisů či dohod. Úzká spolupráce se předpokládá zejména s Národním CERT nebo CERT týmy ostatních členských států EU.

Odstavec 4 nastavuje shodně s § 10 dosavadního zákona o kybernetické bezpečnosti ještě vyšší standard ochrany ve vztahu k informacím z evidence kybernetických bezpečnostních incidentů, událostí a kybernetických hrozeb, kdy se na relevantní zaměstnance Úřadu uplatní povinnost mlčenlivosti v případě jednotlivých zaměstnanců.

K § X – Autorizace subjektů posuzování shody podle aktu o kybernetické bezpečnosti

Návrh tohoto adaptačního ustanovení evropského nařízení beze změn navazuje na ustanovení § 22b dosavadního zákona o kybernetické bezpečnosti.

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 (tzv. „akt o kybernetické bezpečnosti“) ve svém čl. 54 odst. 1 písm. f) stanoví, že jednotlivé evropské systémy certifikace (tzn. prováděcí akty Evropské komise, přičemž se předpokládá využití institutu přímo použitelného aktu – prováděcího nařízení Evropské komise) v příslušných případech zahrnují rovněž konkrétní nebo dodatečné požadavky na subjekty posuzování shody, s cílem zajistit jejich technickou způsobilost k hodnocení požadavků na kybernetickou bezpečnost. Podle čl. 60 odst. 3 aktu o kybernetické bezpečnosti se splnění těchto požadavků posuzuje v řízení o autorizaci.

Obdobně jako v § 11 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů, bylo nutno explicitně jmenovat čtyři typy řízení týkající se autorizací, a to řízení o žádosti o autorizaci subjektu posuzování shody, řízení o pozastavení vykonatelnosti rozhodnutí o autorizaci, řízení o změně rozhodnutí o autorizaci a řízení o zrušení rozhodnutí o autorizaci, protože aktem o kybernetické bezpečnosti [konkrétně čl. 58 odst. 7 písm. e)] je toliko stanoveno, že vnitrostátní orgány certifikace „v příslušných případech autorizují subjekty posuzování shody podle čl. 60 odst. 3 a omezují, pozastavují nebo odebírají stávající autorizaci, pokud subjekty posuzování shody porušují požadavky tohoto nařízení“. S ohledem na uvedenou textaci čl. 58 odst. 7 písm. e) aktu o kybernetické bezpečnosti je současně nutno navázat řízení o pozastavení vykonatelnosti rozhodnutí o autorizaci, o změně rozhodnutí o autorizaci nebo o zrušení rozhodnutí o autorizaci nejen na porušení požadavků prováděcího nařízení Evropské komise (slovy návrhu zákona „přímo použitelného předpisu Evropské unie vydaného na základě aktu o kybernetické bezpečnosti“), ale také samotného aktu o kybernetické bezpečnosti („subjekty posuzování shody porušují požadavky tohoto nařízení“).

V odstavci 2 je stanovena povinnost subjektu posuzování shody přiložit k žádosti o autorizaci všechny doklady o plnění konkrétních nebo dodatečných požadavků. Jedná se opět o formulaci povinnosti koncipovanou obdobně jako v zákoně č. 22/1997 Sb. (konkrétně v § 11 odst. 1 větě druhé), tzn. v míře specifikace dokladů odpovídající tomu, že konkrétní nebo dodatečné požadavky budou stanoveny až (v budoucnu) prováděcími akty Evropské komise, a nelze tedy v tuto chvíli konkrétně stanovit, o jaké doklady prokazující tyto v budoucnu stanovené požadavky se jedná. Současně je ale nutno povinnost předložit doklady prokazující plnění požadavků subjektu posuzování shody uložit, jinak by relevantní skutečnosti nemohly být v řízení o žádosti o autorizaci řádně ověřeny.

V odstavci 3 je (obdobně jako v § 11 odst. 5 zákona č. 22/1997 Sb.) upraven postup správního orgánu v případě, že správní orgán vydá rozhodnutí o pozastavení vykonatelnosti rozhodnutí o autorizaci. V takovém případě má subjekt posuzování shody možnost ve stanovené lhůtě zjednat nápravu porušení stanovených požadavků. V situacích, kdy je zjednání nápravy možné, nedochází hned k rušení rozhodnutí o autorizaci.

Zvláštní ustanovení k § 71 správního řádu pak představuje tento návrh. Jedná se o ustanovení zcela obdobné § 20 zákona č. 22/1997 Sb., včetně totožného nastavení lhůt pro vydání rozhodnutí o autorizaci. Důvodem této úpravy je, že autorizace podle aktu o kybernetické bezpečnosti bude obdobně procesně, a tak i časově náročná jako autorizace podle zákona č. 22/1997 Sb.

K § X – Národní koordinační centrum výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti

Úřad plní roli Národního koordinačního centra výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti podle 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 (dále jen „nařízení 2021/887“). Evropská unie dlouhodobě usiluje o posílení kompetencí a kapacit v oblasti kybernetické bezpečnosti. Jednou z aktivit směřujících k tomuto cíli je i vytvoření Evropského průmyslového, technologického a výzkumného centra kompetencí (dále jen „Kompetenční centrum“) a na něj navazující sítě národních koordinačních center.

Základní činností Úřadu bude zejména koordinovat spolupráci v oblasti kyberbezpečnostního výzkumu a vývoje na národní úrovni, poskytovat podporu při podávání žádostí a následné administraci využívání finančních prostředků alokovaných z programů Evropské unie (zejména Digital Europe a Horizon Europe) a zajišťovat komunikaci s Kompetenčním centrem a Evropskou komisí ohledně priorit a potřeb České republiky v dané oblasti.

Další činností Úřadu bude v souladu s čl. 8 odst. 4 nařízení 2021/887 posuzovat způsobilost žadatelů o registraci v členství v Komunitě kompetencí pro kybernetickou bezpečnost (dále jen „Komunita“), vytvořenou za účelem přispívání k plnění poslání Kompetenčního centra. Registraci žadatele jako člena Komunity provádí Kompetenční centrum po posouzení způsobilosti žadatele o registraci v členství ze strany Úřadu.

Žadatelem o registraci členství v Komunitě může být pouze osoba, která prokáže základní a zvláštní způsobilost.

K § X – Základní způsobilost žadatele o registraci členství v Komunitě

Žadatel musí prokázat základní způsobilost pro registraci členství v Komunitě. Podmínky pro základní způsobilost vychází z čl. 8 odst. 3 a odst. 4 nařízení 2021/887. Základní způsobilost zahrnuje jak podmínku, aby měl žadatel sídlo v České republice, dále některé obecné podmínky ve vztahu k 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. Dále ustanovení v odstavci 3 a odstavci 5 formuluje vnitrostátní bezpečnostní důvody vycházející z mechanismu prověřování bezpečnosti dodavatelského řetězce podle tohoto návrhu zákona, zákona č. 37/2021 Sb., o evidenci skutečných majitelů, ve znění pozdějších předpisů, a zákona č. 1/2023 Sb., o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (sankční zákon).

K § X – Zvláštní způsobilost žadatele o registraci členství v Komunitě

Zvláštní způsobilost má žadatel, který prokáže, že je způsobilý k registraci v souladu s čl. 8 odst. 3 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. Žadatel tak musí prokázat, že může přispívat k plnění poslání a má odborné znalosti v oblasti kybernetické bezpečnosti alespoň v jedné z těchto oblastí:

- akademická oblast, výzkum nebo inovace;
- průmyslový vývoj nebo vývoj produktů;
- odborná příprava a vzdělávání;
- bezpečnost informací nebo reakce na incidenty;
- etika;
- formální a technická normalizace a specifikace.

Prokázat zvláštní způsobilosti může žadatel např. prostřednictvím reference, publikace, dlouhodobější zkušenosti/projekty v dané oblasti, zapojení do EU iniciativ atd.

K § X – Posouzení způsobilosti žadatele o registraci členství v Komunitě

V případě, že žadatel o registraci členství v Komunitě prokáže základní a zvláštní způsobilost, postoupí Úřad žádost žadatele Kompetenčnímu centru k registraci. V opačném případě Úřad zahájí řízení o nezpůsobilosti žadatele k registraci členství v Komunitě podle správního řádu.

K § X – Způsobilost žadatele k členství v Komunitě

Úřad v souladu s čl. 8 odstavec 4 průběžně posuzuje splňování podmínek základní a zvláštní způsobilosti žadatele i po jeho registraci jako člena Komunity. V případě pochybností zahájí Úřad řízení o způsobilosti žadatele k členství v Komunitě.

K § X – Veřejnoprávní smlouva s provozovatelem Národního CERT

Toto ustanovení upravuje způsob výběru provozovatele Národního CERT, účel a podstatné náležitosti veřejnoprávní smlouvy, kterou bude Úřad uzavírat s provozovatelem Národního CERT. Zákon předpokládá, že tato veřejnoprávní smlouva bude zveřejněna ve Věstníku Úřadu. Zveřejnění obsahu této smlouvy společně s institutem výběru provozovatele Národního CERT v řízení o výběru žádosti podle správního řádu a institutem zveřejnění výsledku výběru přitom představuje projev principu transparentnosti výkonu veřejné správy.

Vzhledem k tomu, že může dojít k situaci, kdy nebude uzavřena veřejnoprávní smlouva s provozovatelem Národního CERT nebo kdy uzavřená veřejnoprávní smlouva pozbude účinnosti (např. pokud provozovatel Národního CERT přestane splňovat zákonné podmínky), je potřeba pro tento výjimečný případ upravit provizorní fungování Národního CERT. V takovém případě bude činnost Národního CERT vykonávat Úřad.

K § X – Zpracování osobních údajů

Návrh tohoto ustanovení téměř beze změn navazuje na ustanovení § 22c dosavadního zákona o kybernetické bezpečnosti. Tento návrh ustanovení navazuje na úpravu nakládání s osobními údaji v případě Úřadu a provozovatele Národního CERT, přičemž se nově aplikuje také na inspektory podle tohoto návrhu zákona. Působnost Úřadu, provozovatele Národního CERT i inspektorů je stanovena tímto návrhem zákona.

V případě návrhu úpravy vůči Úřadu a provozovateli Národního CERT je možné se plně odkázat na důvodovou zprávu k původnímu návrhu tohoto ustanovení zavedeného zákonem

č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

V případě inspektorů zavedených tímto návrhem zákona je možno konstatovat, že jejich postavení bude obdobné postavení provozovatele Národního CERT. Inspektoři jsou povinni při výkonu své činnosti postupovat podle 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), přičemž ale při výkonu své působnosti zajišťují plnění základní povinnosti státu, jak je vymezena v čl. 1 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky. Z tohoto důvodu je potřeba v činnostech, na které by nedopadalo Obecné nařízení, postupovat podle hlavy IV zákona o zpracování osobních údajů nadepsané „Ochrana osobních údajů při zajišťování obrany a bezpečnosti České republiky“.

Jak v případě Úřadu a provozovatele Národního CERT, tak i v případě inspektorů platí, že protože má činnost vycházející ze směrnice NIS2 velmi zásadní význam z hlediska ochrany bezpečnosti České republiky, je nutno stanovit i pro tyto činnosti základní systém výjimek (v rámci možností stanovených v čl. 23 Obecného nařízení o ochraně osobních údajů) tak, aby výkonem práv a povinností podle Obecného nařízení o ochraně osobních údajů nemohlo dojít k omezení či dokonce ohrožení plnění povinností NÚKIB podle zákona o kybernetické bezpečnosti.

Stanovením těchto výjimek však není dotčena možnost využití mechanismu pro výjimku upraveného v § 11 a násl. zákona o zpracování osobních údajů ze strany Úřadu.

Za tímto účelem se do dosavadního zákona o kybernetické bezpečnosti vložil § 22c, na jehož obsah tento návrh navazuje, a který představuje obecnou úpravu zpracování osobních údajů ze strany Úřadu, provozovatele Národního CERT a inspektorů.

K § X – Vzájemná součinnost s členskými státy Evropské unie

Toto ustanovení zákona přímo transponuje články 26 odst. 5 a 37 směrnice NIS2, stanovující nezbytný rámec pro úzkou spolupráci mezi členskými státy zejména vůči subjektům, které poskytují své služby ve více členských státech nebo v nich mají své sítě a informační systémy. S ohledem na skutečnost, že subjekty vyjmenované v čl. 26 odst. 1 písm. b) směrnice spadají do výlučné jurisdikce jediného členského státu, je mechanismus pro spolupráci mezi dozorovými orgány zcela nezbytnou součástí nově vznikajícího zákona. Směrnice současně není přímo aplikovatelným předpisem, je proto třeba odpovídající postupy zakotvit v národním právu v souladu s principem *secundum et intra legem*.

Odst. 1 řešeného ustanovení zakotvuje základní způsoby spolupráce a pomoci zmíněné v čl. 37 odst. 1 a 2 směrnice NIS2, tedy sdílení informací, koordinaci a spolupráci při provádění opatření v oblasti dohledu a vymáhání.

Odst. 2 obsahuje taxativní vymezení důvodů pro odmítnutí žádosti o součinnost jiného členského státu v souladu s čl. 37 odst. 1 směrnice NIS2. Nad rámec tohoto ustanovení zmiňuje čl. 37 povinnost konzultovat žádost před jejím zamítnutím s ostatními dotčenými příslušnými orgány, potažmo s Komisí či agenturou ENISA, požádá-li o to některý z dotčených členských států. Tyto procesy budou řešeny *ad hoc* například v rámci Skupiny pro spolupráci (NIS Cooperation Group).

Odst. 3 stanovuje pravomoci Úřadu při vzájemné spolupráci v případě subjektů vyjmenovaných v čl. 26 odst. 1 písm. b) směrnice NIS2, sídlících v jiných členských státech a spadajících do výlučné jurisdikce členského státu, kde mají svou hlavní provozovnu. V souladu s čl. 26 odst. 5 směrnice NIS2 je zakotvena pravomoc Úřadu vykonat v mezích

žádosti jiného členského státu vůči těmto poskytovatelům opatření v oblasti dohledu a vymáhání, vykonává-li v rámci České republiky daný poskytovatel své služby nebo nachází-li se v České republice aktiva k poskytování těchto služeb. Kromě samotné žádosti je Úřad při poskytování součinnost podle tohoto ustanovení limitován také svými zákonnými pravomocemi. Úřad tak na základě žádosti nikdy nemůže vykonat úkon, ke kterému podle národních předpisů nemá pravomoc. Žádost jiného členského státu, do jehož působnosti daný subjekt spadá, pouze aktivuje pravomoci Úřadu vůči danému subjektu a zároveň ohraničuje rozsah užití těchto pravomocí.

Odst. 4 pouze doslovně přejímá definici hlavní provozovny dle čl. 26 odst. 2 směrnice NIS2, což je nezbytné pro zachování fungování výše popsaného mechanismu určování výlučné jurisdikce a případně poskytnutí součinnosti.

Odst. 5 v souladu s požadavkem směrnice NIS2 doplňuje výčet relevantních subjektů obsažený v odst. 3 o subjekty poskytující službu registrace doménových jmen v rámci České republiky, a to s ohledem na fakt, že tento druh služby není dle zákona regulovanou službou. Zákon nicméně pro registrátory doménových jmen stanovuje specifické povinnosti, registrátoři doménových jmen tak jsou povinnými osobami *sui generis*, na které se potenciálně může vztáhnout mechanismus poskytování vzájemné spolupráce.

K § X – Prováděcí právní předpisy a zmocňovací ustanovení

Povinnosti stanovené orgánům a osobám podle tohoto návrhu zákona musí mít bezpodmínečně základ v ustanoveních tohoto návrhu zákona (čl. 4 odst. 1 Listiny základních práv a svobod: *„Povinnosti mohou být ukládány toliko na základě zákona a v jeho mezích a jen při zachování základních práv a svobod.“*), avšak některá ustanovení je na základě tohoto zmocnění potřeba rozvést blíže v prováděcích právních předpisech. Dalším důvodem je také potřeba zajistit, aby byla konkretizace některých ustanovení dostatečně flexibilní ve vztahu k budoucímu vývoji.

Jedná se tak především o stanovení konkrétních kritérií pro poskytovatele regulovaných služeb, konkrétního obsahu bezpečnostních opatření pro oba režimy poskytovatelů regulovaných služeb, způsob stanovení významnosti kybernetických bezpečnostních incidentů nebo detaily spojené s mechanismem bezpečnosti dodavatelského řetězce či inspektorů kybernetické bezpečnosti. Samostatný prováděcí právní předpis stanoví také podmínky fungování Portálu NÚKIB.

K vydání všech těchto prováděcích právních předpisů se zmocňuje Úřad.

K § X – Kontrola vykonávaná Úřadem

Kontrolní pravomoci specifikované tímto ustanovením vykonává Úřad. Předmětem kontroly, při jejímž výkonu se postupuje podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), a kterou vykonávají pověření zaměstnanci Úřadu, je dodržování povinností stanovených tímto zákonem, rozhodnutími a opatřeními obecné povahy vydanými Úřadem podle tohoto zákona a dodržování prováděcích právních předpisů v oblasti kybernetické bezpečnosti.

Rozsah kontrolovaných povinností se liší v závislosti na typu orgánu a osoby, u které je kontrola vykonávána – především se bude jednat o kontrolu plnění povinností ze strany poskytovatelů regulovaných služeb, ale také může jít o subjekt poskytující služby registrace doménových jmen, významné dodavatele a další orgány a osoby, na které se vztahuje tento návrh zákona.

Úřad je jediným orgánem, který může kontrolovat plnění povinností podle tohoto návrhu zákona u všech orgánů a osob, kterým jsou zákonem ukládány povinnosti. Pouze v případě poskytovatelů regulované služby v režimu nižších povinností se okruh osob oprávněných k

výkonu kontroly plnění povinností stanovených tímto zákonem rozšiřuje i na inspektory. V tomto ohledu je důležité, že nad inspektory je prováděn dohled výkonu jejich činnosti (tzn. zda inspektoři dodržují požadavky kladené na ně tímto zákonem a prováděcími předpisy) – tuto kontrolu vykonává Úřad.

K § X – Kontrola vykonávaná inspektory

Ustanovení nově upravuje kontrolu vykonávanou inspektory (více k tomu v odůvodnění paragrafu Inspektoři) Tuto doposud výhradní pravomoc Úřadu mohou nově po splnění podmínek vykonávat Úřadem autorizovaní inspektoři. Úřad bude dohlížet na to, aby tento způsob kontroly byl pro povinné osoby stejně přínosný jako kontrola vykonávaná Úřadem.

V odst. 1 je obdobně jako v paragrafu Kontrola vykonávaná Úřadem upravena pravomoc inspektorů kontrolovat dodržování povinností stanovených tímto zákonem rozhodnutími a opatřeními obecné povahy vydanými Úřadem podle tohoto zákona včetně dodržování prováděcích právních předpisů v oblasti kybernetické bezpečnosti. Kontrolu prováděnou inspektory dále konkretizuje nový prováděcí právní předpis (vyhláška o inspektorech).

V odst. 2 je zakotvena povinnost nechat si na vlastní žádost vykonat kontrolu inspektorem, první kontrolu je nutné provést nejpozději do dvou let od písemného vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb, postup evidence poskytovatelů upravuje paragraf Zápis do evidence poskytovatelů regulované služby. Následně je nutné kontrolu plnění povinností provádět v pravidelných intervalech tří let.

Odst. 3 ponechává výhradní pravomoc Úřadu provést kontrolu u povinné osoby v režimu nižších povinností i nad rámec stanoveného požadavku k provedení kontroly podle odst. 2. K provedením kontroly je Úřad oprávněn pověřit místo sebe inspektora, který disponuje obdobnými pravomocemi jako samotný Úřad. Úřad tento postup může například využít v případech, kdy dojde k významnému narušení kybernetické bezpečnosti u povinné osoby, způsobené například rozsáhlým bezpečnostním incidentem, který měl dopad na poskytování regulované služby.

Odst. 4 upravuje požadavek na zajištění objektivnosti, spravedlivosti a nestrannosti inspektora při kontrolním postupu. I když jsou důvody, kdy lze pochybovat o nepodjatosti obecné, k naplnění toho znaku mohou stačit již pouhé pochybnosti, nebo jistá míra pravděpodobnosti. Specifické důvody podjatosti jsou v našem právním prostředí blíže rozvedeny judikaturou. O vyloučení inspektora z důvodů podjatosti rozhoduje Úřad usnesením (blíže k tomu například rozsudek ze dne 22. března 2013, č. j. 5 As 43/2011-185).

Odst. 5 stanovuje dva speciální režimy pro úhradu nákladů za kontrolu vykonanou autorizovaným inspektorem. V případě, že se povinná osoba obrátí formou žádosti podle odst. 2 na inspektora, je povinna uhradit náklady na provedenou kontrolu přímo zvolenému inspektorovi. Úřad proto z těchto důvodů v prováděcím předpise definuje kritéria a postupy, na základě kterých dojde k přesnému určení ceny za kontrolu provedenou inspektorem, zohledňující všechny relevantní faktory pro naplnění účelu kontroly, avšak dostatečně zohledňující také zájmy a finanční možnosti povinné osoby v režimu nižších povinností. V případě druhého režimu, kdy je kontrola vykonána Úřadem, byť prostřednictvím inspektora mimo režim uvedený v odst. 2 (tzv. kontrolu reaktivní), nese veškeré náklady na takto provedenou kontrolu samotný Úřad.

Odst. 6 sděluje, že kontrolní postup inspektora podle odst 3, stejně tak jako kontrolní postupy Úřadu se řídí přiměřeně kontrolním řádem, který v dostatečné míře rozvíjí a doplňuje práva a povinnosti kontrolované a kontrolující osoby, tak aby bylo garantováno řádné zjištění skutkového stavu a všem účastníkům kontrolního procesu poskytnuty záruky pro ochranu nejen procesních práv.

Odst. 7 řeší problematiku přizvaných osob, avšak s tou výhradou, že se tím inspektor nezříká odpovědnosti za řádný průběh kontroly a její objektivní výsledek.

Odst. 8. Stanovuje povinnost kontrolované osoby uchovávat protokoly z provedených kontrol. Požadavek uchovávat protokoly alespoň 6 let je nutné minimum k tomu, aby bylo zaručeno, že Úřad v případě potřeby bude mít k dispozici podklady z minimálně dvou posledních kontrol u povinné osoby. Důvody jsou praktické, zejména pro povinnou osobu, jelikož inspektor bude mít možnost následující kontroly lépe zacílit na problémové oblasti, tím pádem v protokolu sepisovat kromě zjištěných neshod i pro povinnou osobu praktické doporučení dalšího postupu. Samotná doba trvání kontroly v pravidelném intervalu tří let, se může postupně zkracovat, což se pozitivně promítne do celkové ceny kontroly provedené na vlastní žádost postupem podle odst. 2.

K § X – Pravidla pro výkon kontroly vykonávané inspektorem na vlastní žádost

Toto ustanovení specifikuje pravidla pro výkon kontroly na vlastní žádost, jedná se o nový postup povinných osob, který doposud právní úprava kybernetické bezpečnosti neznala. Zapojení autorizovaných inspektorů do kontrolních procesů prováděných doposud výhradně Úřadem, má zajistit zachování dohledové efektivity i při tak významném nárůstu nově regulovaných subjektů.

I když je inspektor osobou, které Úřad umožnil výkon kontrolní pravomoci nad povinnými osobami v režimu nižších povinností, je nutné nastavit rovnováhu mezi tím, že některé postupy, jako je žádost inspektora o provedení kontroly a požadavek úhrady kontroly mají soukromoprávní povahu, inspektor však v rovném postavení vůči povinné osobě není, ba naopak, jedná se o vztah vrchnostenský. Proto je z pohledu navrhovatele této úpravy velmi důležité proces inspekce nastavit komplexně a přehledně a zohledňovat četná specifika, která tento způsob provádění kontrol obnáší.

Odst. 1 stanovuje požadavek aby povinná osoba a inspektor, před zahájením samotné kontroly mezi sebou uzavřeli smlouvu, jejíž povinné minimální náležitosti jsou v tomto odstavci taxativně vyjmenovány.

Následující odst. 2 upřesňuje, že informace získané před uzavřením smlouvy mohou být také podstatné pro samotný výkon kontroly. Tento odstavec tak cíli na skutečnost, aby před samotným uzavřením smlouvy, ve které se má určit mimo jiné i cena za provedenou inspekci, je inspektor oprávněn požadovat informace, na základě kterých dojde k přesnému určení doby, po kterou bude inspekce u povinné osoby probíhat, a tím pádem ve smlouvě stanovit reálnou cenu za provedenou kontrolu. S ohledem na velké rozdíly mezi povinnými osobami v režimu nižších povinností se jedná o velmi podstatnou a důležitou činnost, při které je nutná součinnost smluvních stran. Postup určení doby trvání kontroly včetně způsoby stanovení ceny za provedenou kontrolu dále rozvádí prováděcí právní předpis (vyhláška o inspektorech).

Odst. 3 vylučuje použití kontrolního řádu obecně, avšak obsahuje četné výjimky z ustanovení kontrolního řádu, na které se toto vyloučení nevztahuje. Tam kde došlo k vyloučení kontrolního řádu, jsou procesy upraveny speciálně tímto zákonem nebo prováděcím právním předpisem. Pro Úřad je důležité aby kontrolní procesy i v případě kontroly provedené na žádost povinného subjektu, co nejvíce korespondovaly se současnými kontrolami prováděnými Úřadem. Pro lepší přehlednost přikládáme názvy ustanovení kontrolního řádu, podle kterých je inspektor povinen při kontrolní činnosti postupovat: § 2 – Kontrola, § 7 – Vstup na pozemky, do staveb a jiných prostor, § 8 – Další práva kontrolujícího, § 9 – Povinnosti kontrolujícího, § 10 – Práva a povinnosti kontrolované osoby a povinné osoby, § 13 – Námitky, § 15 přestupky, § 18 písm. a) a b) – Ukončení kontroly, § 20 – Povinnost mlčenlivosti, § 21 odst. 1 a 2 – Oprava nesprávností a došetření věci. Obdobně jako je tomu u povinné osoby

s povinností uchovávat protokol z provedené kontroly, je inspektor povinen uchovávat všechny podklady z provedených kontrol alespoň po dobu 6 let.

Odst. 4 reaguje na skutečnost, že došlo k vyloučení použití kontrolního řádu, vyjma ustanovení, která jsou uvedena v předchozím odstavci. Tím, že došlo k vyloučení § 12 kontrolního řádu, který nám definuje minimální požadavky na obsah protokolu, bylo nutné toto ustanovení upravit speciálně a zohlednit tak konkrétní požadavky a specifika na protokol sepsaný inspektorem. Jedním z velmi důležitých bodů, který je nutné mít přesně a objektivně zpracovaný je harmonogram kontroly, který je u kontroly vykonávané inspektorem velmi důležitým nástrojem, který pomáhá oběma stranám si uvědomit časovou náročnost kontroly, její rozsah a tím pádem určit i finální cenu za takto provedenou kontrolu.

Odst. 5 upravuje standardní lhůtu, v průběhu které je inspektor povinen sepsat protokol o kontrole, tato lhůta je shodná s lhůtou, která je dána na vypracování protokolu při postupu podle kontrolního řádu.

Odst. 6 upravuje způsob vyřizování námitek, jedná se opět o proces, který je speciálně upraven oproti § 14 kontrolního řádu. Hlavním rozdílem v procesu vyřizování námitek je skutečnost, že ty jdou rovněž v těchto případech na vrub inspektorovi, který u povinné osoby kontrolu vykonal.

Odst. 7 zmiňuje správní řízení navazující na výkon kontroly provedené na žádost inspektorem, ve kterém mohou být skutečnosti zjištěné při kontrole jediným podkladem pro rozhodnutí o přestupku podle jiného právního předpisu.

K § X – Povinnosti inspektora

V tomto ustanovení nalezneme výčet povinností, které musí inspektor při své činnosti dodržovat a jejichž nedodržení představuje přestupek podle tohoto zákona. Inspektor přitom může v důsledku udělených pokut přestat splňovat jednu z podmínek pro udělení autorizace inspektora a o autorizaci před uplynutím lhůty, pro kterou byla udělena, přijít. Povinnosti, na které toto ustanovení odkazuje, jsou dále rozvedeny jednak souvisejícími ustanoveními zákona, jednak příslušným prováděcím právním předpisem.

V odst. 1 jsou uvedeny konkrétní požadavky na výkon kontroly, které musí inspektor během své činnosti naplňovat. Jde o standardní požadavky kladené na činnost auditorů podle zákona č. 93/2009 Sb., o auditorech a o změně některých zákonů (zákon o auditorech), resp. příslušnými technickými normami (zejm. ČSN EN ISO 19011 nebo ISO řady 17000). Činnost inspektorů podle tohoto návrhu zákona a auditorů podle zákona o auditorech je svým charakterem srovnatelná, z toho důvodu jsou i na činnost inspektorů kladeny principiálně obdobné požadavky jako na činnost auditorů a navrhovaná úprava se regulací auditorů v mnohém inspiruje. Odst. 1 stanovuje principiální požadavky na výkon kontroly inspektorem, které jsou v podrobnostech dále rozvedeny v prováděcím právním předpise.

Inspektor podle odst. 2 odpovídá za přiměřené určení délky trvání kontroly vůči jejímu rozsahu. Jde sice o standardní požadavek kladený na audity podle zákona o auditorech nebo podle příslušných technických norem, nicméně v zákoně je tato skutečnost z praktických důvodů zdůrazněna. Kontroly vykonávané inspektory jsou podle návrhu zákona povinným požadavkem kladeným na poskytovatele regulovaných služeb v režimu nižších povinností. Ačkoli služby inspektorů budou nabízeny na trhu otevřeném každé osobě splňující požadavky na autorizaci inspektora, a případné excesy v nabídkách inspektorů by tedy měly být korigovány konkurenčním prostředím, nelze vyloučit, že ve výjimečných situacích se poskytovatel regulované služby poptávající služby inspektora dostane do slabší vyjednávací pozice (zejm. v situacích, kdy sám není schopen posoudit, zda sjednané podmínky poskytování kontroly inspektorem jsou skutečně přiměřené a odpovídající okolnostem). Cílem komentovaného

ustanovení je pak zajistit, aby inspektoři nezneužívali slabšího postavení svých klientů a nestanovovali délku kontroly nepřiměřeně okolnostem s cílem uměle navýšit svou odměnu za vykonán kontroly.

Odst. 3 stanovuje maximální délku kontroly vykonané inspektorem z pokynu Úřadu. Volba jednoho roku reflektuje mnohaleté zkušenosti Úřadu s prováděním kontrol regulovaných subjektů a měla by být zcela dostačující i pro kontrolu velkých organizací spravujících velké množství aktiv. Maximální délka kontroly pak slouží jednak k zastropování nákladů na kontrolu, které nese Úřad, jednak k zajištění využitelnosti provedeného auditu pro účely další činnosti Úřadu (zejm. uložení nápravných opatření nebo pokuty za přestupek v případě identifikace pochybení kontrolované osoby), která by neúměrným prodlužováním kontrol ze strany inspektorů mohla být ochromena. Pokud inspektor nedodrží požadavek na maximální délku kontroly, dopustí se přestupku.

Odst. 4 stanoví povinnost inspektora informovat Úřad o existenci důvodů pro jeho vyloučení z výkonu kontroly z důvodu podjatosti. Navrhovaná úprava vychází z obecné úpravy podjatosti obsažené v kontrolním řádu a správním řádu. O podjatosti se inspektor může dozvědět buďto sám ze své činnosti, nebo na základě námitky kontrolované osoby. Inspektor, o němž lze důvodně předpokládat, že má s ohledem na svůj poměr k předmětu kontroly nebo ke kontrolované osobě takový zájem na výsledku kontroly, pro nějž lze pochybovat o jeho nepodjatosti, je vyloučen z výkonu kontroly (na základě usnesení Úřadu). Porušení povinnosti bezodkladně informovat Úřad o důvodech pro vyloučení z výkonu kontroly je přestupkem podle tohoto zákona.

Jedna ze základních povinností inspektora po skončené kontrole je podle odst. 5 doručení protokolu o kontrole včetně jeho dodatků Úřadu. Inspektor tak činí jak v případě, kdy kontrolu vykonal na vlastní žádost kontrolovaného subjektu, tak v případě, kdy vykonal kontrolu, ke které byl ustanoven Úřadem. Doručení protokolu o kontrole a jeho dodatků Úřadu je dodatečnou povinností k obecně platné povinnosti doručit protokol o kontrole včetně všech jeho dodatků kontrolované osobě (vycházející z příslušných ustanovení kontrolního řádu, která jsou pro inspektory závazná nezávisle na způsobu iniciace kontroly). Je třeba mít na paměti, že inspektoři kontrolu poskytovatelů regulovaných služeb v režimu nižšího povinností v obou uvedených případech zajišťují pro Úřad. Úřad je pak orgánem odpovědným za vyhodnocení informací obsažených v protokolu o kontrole a jeho dodatcích a k provedení navazujících kroků (uložení nápravného opatření nebo pokuty za přestupek v případě identifikace pochybení kontrolované osoby, resp. sankcionování inspektora za nesplnění jeho povinností vztahujících se k výkonu kontroly). Tento požadavek je tak zcela v souladu s principem fungování přenesení části výkonu veřejné správy na inspektory a rovněž tím, že nad výkonem činnosti inspektorů bude Úřad vykonávat dohled.

K § X – Nápravná opatření

Toto ustanovení upravuje podmínky, za nichž lze uložit nápravná opatření orgánům a osobám povinným podle tohoto návrhu zákona. Účelem nápravných opatření je odstranění nedostatků zjištěných při kontrole, tj. především dodatečné řádné splnění některé z povinností stanovených tímto zákonem nebo na jeho základě (typicky v případě poskytovatelů regulovaných služeb doplnění nedostatečně prováděného bezpečnostního opatření, aktualizace údajů, apod.). Obsahem nápravných opatření však mohou být i jiné povinnosti, a to v závislosti na typu povinné osoby, charakteru zjištěných nedostatků a jejich možných následků. Na rozdíl od předchozího zákona č. 181/2014 Sb. tento návrh zákona neukládá Úřadu povinnost konat, pokud zjistí při kontrole nedostatky, ale ponechává mu určitou volnost pro případ, že by uložení nápravného opatření v konkrétní situaci nebylo přiměřené nebo žádoucí.

Odst. 1 dále reflektuje skutečnost, že kontrolu poskytovatelů regulované služby v režimu nižších povinností provádí inspektoři. Činnost inspektorů v oblasti kontroly plnění povinností stanovených tímto zákonem nebo na základě tohoto zákona bude principiálně shodná s činností prováděnou v tomto smyslu Úřadem, z toho důvodu bude možné uložit nápravné opatření také na základě výsledků kontroly provedené inspektorem. Nápravná opatření ukládá vždy Úřad, nikdy inspektor.

Oproti předchozí právní úpravě se explicitně stanoví oprávnění Úřadu uložit spolu s nápravným opatřením i povinnost oznámit jeho provedení a výsledek a stanovit pro oznámení lhůtu. Oznámení se provede prostřednictvím Portálu NÚKIB, obdobně jako všechna obdobná hlášení podle tohoto zákona.

Návrh zákona sice na rozdíl od předchozí právní úpravy explicitně neupravuje oprávnění Úřadu uložit orgánu nebo osobě dočasný zákaz používání systému (nebo jeho části) ohroženého kybernetickým bezpečnostním incidentem do doby, než budou zjištěné nedostatky odstraněny, nicméně toto oprávnění Úřadu je zachováno v rámci pravomoci k vydání reaktivního opatření k řešení kybernetického bezpečnostního incidentu nebo k zabezpečení aktiv před kybernetickým bezpečnostním incidentem.

Stejně jako v případě dosavadní právní úpravy, také podle tohoto návrhu zákona nese náklady spojené s provedením nápravných opatření uložených Úřadem orgán a osoba, kterým byla nápravná opatření uložena. Nesplnění některé z povinností uložených nápravným opatřením pak zakládá skutkovou podstatu přestupku podle tohoto zákona.

Odstavce 2 a 3 upravuje procesní otázky spojené s vydáváním nápravných opatření. Praxe ukázala, že variabilita povinností, které mohou být v různých situacích nápravným opatřením uloženy, vyžaduje také to, aby mohlo být nápravné opatření uloženo bez nutnosti provedení kontroly podle kontrolního řádu. Smyslem tohoto ustanovení je jeho aplikace na skutkově jasné případy, přičemž cílem je zrychlení celého procesu a šetření práv účastníků řízení. O to větší nároky na odůvodnění a obsah takového úkonu však budou na Úřad v těchto případech kladeny (obdobně jako např. v případě reaktivního protiopatření, které má s nápravným opatřením z tohoto pohledu celou řadu obdobných východisek). Praktické poznatky vedou také k tomu, 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 nepřiznává rozkladu podanému proti rozhodnutí o uložení nápravného opatření odkladný účinek (ustanovení je v tomto obdobné jako např. v případě opatření k nápravě uložených podle § 204 odst. 3 atomového zákona).

K § X – Přestupky

Ustanovení o přestupcích se v návrhu zákona člení do jednotlivých odstavců odpovídajících povinnému orgánu nebo osobě, vůči kterým návrh zákona přestupky adresuje.

Odstavec 1 vymezuje jednotlivé přestupky v návaznosti na zákonné povinnosti stanovené poskytovatelům regulovaných služeb v režimu vyšších povinností, tak aby všechny povinnosti byly odpovídajícím způsobem vymahatelné a nešlo pouze o imperfektní normy.

Totožným způsobem jsou v odstavci 2 vymezeny přestupky, kterých se mohou dopustit poskytovatele regulovaných služeb v režimu nižších povinností. Odstavec 3 se pak zaměřuje na poskytovatele regulovaných služeb v režimu vyšších povinností, kterým vyplývají specifické povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce podle tohoto návrhu zákona, a kteří se v něm označují souhrnně jako „povinná osoba mechanismu prověřování“.

Odstavec 4 pak míří na subjekty spravující a provozující registr internetových domén nejvyšší úrovně a subjekty poskytující služby registrace doménových jmen, kteří mají

specifickou množinu povinností zakotvenou v tomto návrhu zákona a nejedná se o stejný typ povinné osoby jakou je poskytovatel regulované služby.

Následující odstavec, odstavec 5 je specifický tím, že zde uvedených přestupků se lze dopustit pouze v souvislosti se stavem kybernetického nebezpečí, jehož obsah je rovněž upravený tímto návrhem zákona. Tento druh přestupků lze obecně vnímat jako závažnější s ohledem na významné zájmy České republiky, jejichž ohrožení mj. vede k vyhlášení stavu kybernetického nebezpečí.

Skupina přestupků podle odstavců 6 až 8 souvisí s efektivním uplatňováním systému certifikací kybernetické bezpečnosti v České republice zejména na základě aktu o kybernetické bezpečnosti, ale částečně také v návaznosti na směrnici NIS2. Odstavec 6 vymezuje specifický přestupek, jehož se může dopustit držitel evropského certifikátu kybernetické bezpečnosti. S tím úzce souvisí přestupky podle odstavce 7, kterých se mohou dopustit výrobci či poskytovatelé produktů, služeb nebo procesů, kteří vydali EU prohlášení o shodě dle aktu o kybernetické bezpečnosti, a přestupky podle odstavce 8, kterých se může dopustit jakákoliv právnická či fyzická podnikající osoba. Přestupek podle odstavce 8 písm. g) pak specificky souvisí s efektivním uplatňováním sankčního mechanismu pozastavení platnosti certifikace zakotveným v zákoně na základě směrnice NIS2.

Odstavec 9 vymezuje přestupek porušení mlčenlivosti, jehož se mohou dopustit pouze zaměstnanci Úřadu ve vztahu k obsahu vedených evidencí.

Jakákoliv osoba či orgán se pak mohou dopustit přestupků vymezených v odstavci 10, typicky jde o neposkytnutí součinnosti Úřadu, což je povinnost dopadající v konkrétních případech nejen na poskytovatele regulovaných služeb, ale i další orgány a osoby. Odstavec 11 zakotvuje specifický přestupek neposkytnutí součinnosti v rámci zvládání kybernetického bezpečnostního incidentu ze strany subjektu, který není poskytovatelem regulované služby. Poskytovatelé regulovaných mají zakotven vlastní přestupek s obdobnou skutkovou podstatou, se kterým se však spojena vyšší sankce.

Odstavce 12 a 13 zakotvují přestupky související se systémem kontrol prostřednictvím inspektorů. Možnými pachateli přestupků dle odst. 12 jsou pouze inspektoři a tyto přestupky odpovídají povinnostem inspektora při výkonů jeho funkce, tedy zejména výkonu kontrol. Přestupků dle odst. 13 se naopak z povahy věci mohou dopustit pouze osoby, které inspektory nejsou, případně už jimi nejsou z důvodu ukončení platnosti jejich autorizace.

Poslední přestupek dle odst. 14 souvisí s řádným fungováním Národního koordinačního centra výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti a přijímáním a vyřizováním žádostí o registraci do tohoto centra, resp. související komunity, v souladu s nařízením (EU) 2021/887, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

Výše pokut zakotvená v odst. 15 buďto přímo vychází ze směrnice NIS2, nebo je této stanovené výši pokut řádově odpovídající. Obdobná výše pokut je stanovena také v předpisech z oblasti ochrany osobních údajů, přičemž zde není důvod se od této praxe významně odchylovat. Ústředním principem, zdůrazněným i v obsahu směrnice NIS2, přitom zůstává, že by uložené sankce měly být vždy účinné, přiměřené a odrazující, přičemž budou zohledněny okolnosti každého jednotlivého případu a majetkové a osobní poměry delikventa tak, aby pro něj případná pokuta nebyla likvidační. Vysoká výše maximální hranice pokuty tak Úřadu nebrání ukládat pokuty řádově nižší, nicméně musí existovat efektivní sankční nástroje v případech, kdy se budou potenciálně velmi movité regulované organizace soustavně vyhýbat plnění svých zákonných povinností. Maximální výše pokut v dosavadním zákonu o kybernetické bezpečnosti často nemusela dosahovat ani výše nákladů na zabezpečení dané

organizace, což mohlo být v určitých případech nedostatečně odrazující, a tedy neefektivní. Propastný rozdíl je patrný zejména při srovnání sankcí v obecném nařízení o ochraně osobních údajů (GDPR) a dosavadním zákoně o kybernetické bezpečnosti.

Horní hranice pokut odpovídají závažnosti jednotlivých přestupků, respektive možným krajním důsledkům protiprávního jednání či opomenutí. Vzhledem k závažnosti a okolnostem, za kterých může být vyhlášen stav kybernetického nebezpečí, jsou například pokuty ukládané za nesoučinnost během tohoto stavu nebo neprovedení uložených povinností srovnatelné se sankcemi, které hrozí za nezavedení bezpečnostních opatření. S některými na první pohled méně závažnými přestupky jsou spojeny vysoké sankce z důvodu možných důsledků při neplnění odpovídajících povinností. Například za nenahlášení kontaktních údajů nebo dalších údajů nebo jejich změny Úřadu hrozí pokuta až do výše 100 milionů korun, a to z důvodu, že nenahlášení těchto údajů znamená v určitých případech *a priori* nemožnost jakékoliv součinnosti při řešení akutního kybernetického bezpečnostního incidentu s potenciálně extrémními dopady. Takový stav pak v zásadě znemožňuje činnost Úřadu a v krajních případech může ohrožovat fungování regulovaných služeb významných třeba z hlediska národní bezpečnosti. Tento přístup ke stanovování výše pokut navazuje na dosavadně platný přístup zákona o kybernetické bezpečnosti, kdy např. za nenahlášení provedení reaktivního opatření byla stanovena maximální výše pokuty totožná s maximální výši pokuty za jeho samotné neprovedení.

Jak již bylo řečeno, maximální výše pokut, které je možné uložit za porušení pravidel obsažených v zákoně, jsou stanoveny v souladu s požadavky NIS2, v případě některých přestupků jednak pevnou, jednak pohyblivou částkou, přičemž pro konkrétní případ bude relevantní ta z částek, která je vyšší. Pevný strop pro uložení pokuty se tedy uplatní jednak v případech, kdy roční celosvětový obrat právnické osoby nebo konsolidačního celku nebude dosahovat hodnoty pevného maxima, jednak v případech, kdy nepůjde o osobu, u které by byl obrat relevantním kritériem (typicky u orgánů veřejné správy).

Při počítání celosvětového obratu lze aplikovat postupy používané při ukládání pokut za porušení pravidel obsažených v 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), neboť úprava obsažená v tomto nařízení a ve směrnici NIS2 je v zásadě shodná. Vycházet je možné i z příručky pro počítání pokut podle obecného nařízení o ochraně osobních údajů Evropského sboru pro ochranu osobních údajů.

Pojem konsolidační celek zmíněný v odst. 15 písm. a) a b) představuje transpozici požadavku směrnice NIS2 na stanovení pohyblivého stropu podle „*celosvětového ročního obratu u podniku, ke kterému patří (...) subjekt*“, v angličtině „*the undertaking to which the (...) entity belongs*“. Pojem podnik ve smyslu směrnice NIS2 i obecného nařízení o ochraně osobních údajů je třeba vykládat ve smyslu čl. 101 a 102 Smlouvy o fungování Evropské Unie a bohaté judikatury Soudního dvora Evropské unie spíše jako ekonomickou, nikoli pouze právní jednotku, přičemž i podle současné podoby návrhu příručky pro počítání pokut podle obecného nařízení o ochraně osobních údajů Evropského sboru pro ochranu osobních údajů je potřeba při stanovení celosvětového obratu podniku zohledňovat ekonomickou situaci skupiny. Tím spíše tímto směrem míří i směrnice NIS2, která hovoří o obratu podniku,jehož je regulovaný subjekt součástí. Pojem konsolidační celek vychází z úpravy konsolidovaných účetních závěrek dle ustanovení § 22 a následujících zákona č. 563/1991 Sb., o účetnictví a navazující části páté vyhlášky č. 500/2002 Sb. Je-li osoba s ohledem na citované předpisy součástí konsolidačního celku, tzn. jsou-li výsledky jejího hospodaření zachyceny v konsolidované účetní závěrce, může být v případě výpočtu sankcí dle odst. 11 písm. a) a b) vycházeno z čistého celosvětového obratu celého konsolidačního celku, nikoli pouze jedné konkrétní osoby.

K § X – Společná ustanovení k přestupkům

Řízení o přestupcích proti tomuto zákonu se obecně řídí pravidly zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, s některými modifikacemi vyvěrajícími ze specifické povahy pravidel kybernetické bezpečnosti, resp. regulovaných subjektů.

Stejně jako podle předchozí právní úpravy je za projednávání přestupků a ukládání pokut za přestupky a jejich výběr odpovědný Úřad. Pokuty jsou příjmem státního rozpočtu. Orgánem oprávněným k vymáhání pokut v případě jejich neuhrazení v zákonem stanovené lhůtě je příslušný celní úřad.

Materiálně-formální pojetí přestupků se pro oblast regulace kybernetické bezpečnosti nejeví jako zcela vhodné. Společenská škodlivost je u těchto přestupků dána již samotným naplněním skutkové podstaty přestupku. V případě, že by konkrétní společenská škodlivost protiprávního jednání nedosahovala ani minimální hranice typové škodlivosti, nebyl by dán veřejný zájem na jeho stíhání. Proto se upravuje vyvratitelná právní domněnka spočívající v tom, že se má za to, že čin, který vykazuje formální znaky přestupku podle tohoto zákona, je společensky škodlivý.

S ohledem na specifickou povahu přestupků, které projednává Úřad, jsou vyloučena nebo omezena některá ustanovení zákona o odpovědnosti za přestupky a řízení o nich. Tyto přestupky jsou specifické okruhem a charakterem osob, na které dopadají, důvěrností informací, které jsou v rámci řízení projednávány, a veřejným zájmem na rychlém a efektivním provedení přestupkového řízení, neboť jeho cílem není pouze zpětné potrestání pachatele za spáchání přestupku, ale mnohdy též motivace pachatele ke splnění povinnosti, za jejíž nesplnění byl sankcionován a kde je stále dán zájem na jejím splnění (typicky splnění reaktivního opatření nebo zavedení bezpečnostního opatření).

Vylučuje se ustanovení o přípustném riziku, neboť ohrožení kybernetické bezpečnosti nemůže být odůvodněno výkonem společensky prospěšné činnosti.

Vylučuje se ustanovení o podmíněném upuštění od uložení správního trestu, neboť návrhem stanovené přestupky proti kybernetické bezpečnosti jsou natolik závažného charakteru, že pouhé projednání věci před Úřadem nemůže postačovat k nápravě nezákonného stavu nebo pachatele přestupku. Aplikace odstavce 2 uvedeného ustanovení by navíc byla problematická, neboť potenciální škoda vzniká především státu (v důsledku ohrožení veřejného pořádku a kybernetické bezpečnosti jako celku) a odběratelům služeb pachatele přestupku (v důsledku snížení bezpečnosti poskytovaných služeb) a její vyčíslení by bylo mnohdy nemožné. Z obdobných důvodů se vylučuje i ustanovení o upuštění od uložení správního trestu, přičemž však zůstává zachována možnost uložení napomenutí.

Vylučuje se část ustanovení o účastnících řízení, neboť předmětem přestupkového řízení před Úřadem nikdy nebude rozhodování o náhradě škody poškozeného, stejně jako nebude za přestupek uložen jiný trest než pokuta, potažmo napomenutí. Z obdobných důvodů se vylučují i ustanovení o poškozeném, ustanovení o nařízení ústního jednání na požádání poškozeného, ustanovení o řízení o náhradě škody a o vydání bezdůvodného obohacení, ustanovení o náhradě nákladů řízení vůči poškozenému a ustanovení o oprávnění poškozeného podat odvolání.

Vylučuje se ustanovení o osobě přímo postižené spácháním přestupku, neboť okruh přímo postižených osob bude často natolik široký, že by bylo přestupkové řízení přiznáním práv podle § 71 zákona o odpovědnosti za přestupky a řízení o nich neúměrně zatěžováno.

Vylučuje se část ustanovení o příkazu, neboť není žádoucí, aby v řízeních před Úřadem navazujících na podání odporu proti příkazu nebylo možné např. rozšířit předmět řízení o nové skutky a uložit vyšší pokutu, než která byla stanovena v příkazu. Nadto mohou v řízení vyjít

najevo nové skutečnosti, které Úřadu nebyly známy v době vydání příkazu (ačkoli tehdy známé skutečnosti jeho vydání odůvodňovaly) a které mohou odůvodnit stanovení vyšší pokuty (např. vyjde najevo, že se nejedná o první pochybení regulované osoby, nebo že jde o závažnější pochybení, než bylo presumováno příkazem). S ohledem na charakter přestupků proti pravidlům kybernetické bezpečnosti přitom není žádoucí, aby závažnost pochybení nebo jiné přitěžující okolnosti nebyly v řízení reflektovány, neboť by tím byl ohrožen jeden ze základních smyslů vedení řízení o přestupku v této oblasti, tedy donutit pachatele splnit povinnost, za jejíž nesplnění je sankcionován. Z obdobných důvodů se vylučuje i ustanovení o nemožnosti změny výroku rozhodnutí napadeného odvoláním v neprospěch obviněného.

Vylučuje se ustanovení o povinnosti správního orgánu projednat ve společném řízení spolu související přestupky více obviněných. Stále zůstává obecná fakultativní možnost vedení takového řízení ve společném režimu, avšak povinnost vést společně řízení s různými pachateli není vhodná s ohledem na informace, které by tak byly vzájemně mezi pachatele rozšířeny o jednotlivých osobách.

Pro odstranění výkladových problémů a zajištění vyšší míry právní jistoty adresátů zákona a s ohledem na závažnost přestupků spočívajících v porušení povinnosti uložené nápravným opatřením, rozhodnutím nebo opatřením obecné povahy, přestupků spočívajících v porušení povinností z mechanismu prověřování dodavatelského řetězce a přestupků spočívajících v neoznámení informací a udržování stavu neinformování Úřadu, se stanoví nevyvratitelná právní domněnka, že v těchto případech jde o trvající přestupky podle zákona o odpovědnosti za přestupky a řízení o nich. I samotné formulace skutkových podstat správních deliktů podle tohoto zákona pracují s udržováním protiprávního stavu a s trváním protiprávní skutečnosti, čímž dostávají doktríně i relevantní judikatuře správních soudů, podle kterých je podstatným znakem trvajících deliktů to, že se postihuje právě ono udržování protiprávního stavu, a na udržování protiprávního stavu má směřovat i skutková podstata deliktu.

Oznamovací povinnosti podle tohoto zákona plní zcela jinou funkci a vyjadřují jiný cíl než typické oznamovací povinnosti podle jiných předpisů, u nichž dává smysl postihovat pouze vyvolání protiprávního stavu, ale již ne jeho udržování (např. povinnost neprodleně ohlásit útvaru policie ztrátu nebo odcizení zbraně podle zákona č. 119/2002 Sb., o střelných zbraních a střelivu, nebo povinnost oznámit stavební činnost na území s archeologickými nálezy podle zákona č. 20/1987 Sb., o státní památkové péči). Informace, které Úřad po adresátech normy vyžaduje, jsou nezbytné pro výkon dalších činností Úřadu podle zákona a Úřad si je nemůže, nebo může jen stěží, opatřit jinak. Např. informace o splnění protiopatření Úřadu jsou nezbytné pro vyhodnocení účinnosti protiopatření a pro posouzení úrovně kybernetické bezpečnosti v odvětvích, pro která bylo protiopatření vydáno. Dokud Úřad informaci o provedení protiopatření nezíská, nemá informaci o tom, zda a které povinné osoby protiopatření splnily a v jakém stavu jsou informační systémy poskytovatelů regulované služby, a nemůže dále v plném rozsahu vykonávat své preventivní a analytické činnosti a reagovat na navazující krizové situace. Stejně tak nesplněním povinnosti informovat Úřad o dodavatelích bezpečnostně významných dodávek pachatel významným způsobem ztěžuje činnost Úřadu v oblasti prověřování bezpečnosti dodavatelského řetězce, neboť informace o dodavatelích jsou základním vstupem pro prověřování jejich bezpečnosti ze strany Úřadu.

Pachatel přestupku tak od okamžiku vzniku oznamovací povinnosti až do okamžiku předání informace Úřadu udržuje protiprávní stav nepředání informace nezbytné pro další činnost Úřadu a zamezuje či významně ztěžuje výkon zákonných pravomocí Úřadu v dotčených oblastech.

K § X – Pozastavení platnosti certifikace

Pozastavení platnosti certifikace je jedním ze dvou zcela nových správních trestů, jehož zakotvení v právním řádu vyžaduje směrnice NIS2, konkrétně její čl. 32 odst. 5. Podle tohoto ustanovení musí členské státy zajistit, aby měly dozorové orgány (zde Úřad) v případě nesplnění uloženého nápravného opatření pravomoc dočasně pozastavit nebo v souladu s vnitrostátním právem požádat certifikační nebo autorizační orgán nebo soud o dočasné pozastavení certifikace nebo povolení (osvědčení) týkajícího se části nebo všech příslušných služeb nebo činností poskytovaných základním subjektem. Uvedené ustanovení má za cíl dále posílit účinnost a odrazující účinek opatření v oblasti vymáhání, jež jsou uplatňována v případě porušení směrnice (srov. bod 133 preambule směrnice NIS2). Podpůrně má toto ustanovení za cíl také zajistit, aby se organizace, u nichž byly identifikovány nedostatky v řízení kybernetické bezpečnosti v organizaci, nemohly za tohoto stavu svým zákazníkům prokazovat certifikáty deklarujícími kybernetickou bezpečnost organizace, čemuž bude předcházet skutečnost, že organizaci bylo uloženo tyto nedostatky odstranit a organizace se splnění své povinnosti vyhýbá. Tento správní trest tak nemá sloužit jako pouhé potrestání poskytovatele regulované služby za nesplnění jeho zákonných povinností, ale především jako donucovací prostředek k provedení povinnosti, pro jejíž nesplnění byl uložen.

Podle odst. 1 lze pozastavit platnost evropského certifikátu kybernetické bezpečnosti nebo jiného certifikátu nebo osvědčení souvisejícího se zajištěním kybernetické bezpečnosti regulované služby (např. ISO/IEC 27 001). Směrnice NIS2 nestanoví, které konkrétní certifikáty nebo osvědčení mají být uvedeným ustanovením dotčeny, stejně jako nestanoví vazbu mezi tímto ustanovením a certifikacemi podle 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“). Znění směrnice NIS2 dokonce nevylučuje, aby byly dočasným pozastavením platnosti dotčeny licence pro poskytování relevantních služeb nebo živnostenská oprávnění. V zájmu zajištění kontinuity poskytování regulovaných služeb (která by pozastavením licence pro poskytování služby nebo živnostenského oprávnění byla významným způsobem ohrožena) však návrh míří pouze na osvědčení a certifikace, které jsou relevantní z hlediska zajištění a deklarace kybernetické bezpečnosti regulované služby a jejichž pozastavení neohrozí vlastní poskytování regulované služby.

Trest pozastavení platnosti certifikace nebo osvědčení lze uložit pouze poskytovateli regulované služby v režimu vyšších povinností. Rozšíření možnosti ukládání i na poskytovatele regulovaných služeb v režimu nižších povinností se s ohledem na charakter těchto subjektů a omezený rozsah povinností, které jim z navrhované regulace plynou, nejeví jako přiměřené. Zároveň je tím vyhověno požadavku směrnice NIS2, která vyžaduje ukládání tohoto druhu trestu jen základním subjektům. Oproti znění směrnice NIS2 však z působnosti navrhovaného ustanovení nejsou vyloučeny subjekty veřejné správy.

Vzhledem k závažnosti daného trestu a dopadu na činnost subjektů a v konečném důsledku na uživatele by toto dočasné pozastavení mělo být uplatňováno pouze v krajních případech, úměrně závažnosti porušení a s ohledem na okolnosti každého jednotlivého případu. Aplikovatelnost trestu není omezena jinými předpoklady (např. vyčerpáním zbylých sankčních mechanismů zákona), nicméně z povahy věci by mělo být ukládáno pouze tam, kde skutečně povede k cíli, tedy ke splnění uloženého nápravného opatření, a nebude představovat nepřiměřený zásah do práv regulované osoby.

Stejně tak by toto dočasné pozastavení mělo být uplatňováno pouze na nezbytně nutnou dobu, tedy jakmile je povinnost uložená nápravným opatřením splněna, mělo by dojít k obnově

platnosti certifikace. V zájmu posílení preventivní i represivní funkce navrhovaného trestu je však stanovena minimální doba, na kterou bude pozastavení platnosti certifikace nebo osvědčení uloženo. Stanovení minimální doby pozastavení má za cíl také ulehčit nápadu práce Úřadu, neboť ten bude moci efektivněji plánovat kontroly splnění uložených nápravných opatření a na ně navazujících pozastavení platností certifikace nebo osvědčení. Stanovená doba 6 měsíců se v kontextu dosavadních zkušeností Úřadu s ukládáním nápravných opatření a lhůt k jejich splnění jeví jako přiměřená, neboť lhůty, které Úřad poskytuje pro splnění uložených nápravných opatření, v mnoha případech tuto dobu přesahují (zvláště pokud se jedná o nápravná opatření spočívající v provedení komplexních bezpečnostních opatření podle zákona).

V závislosti na vydavateli pozastavovaného certifikátu nebo osvědčení bude trest proveden buďto pozastavením platnosti evropského certifikátu kybernetické bezpečnosti vydaného Úřadem, nebo uložením povinnosti pozastavit platnost certifikátu nebo osvědčení subjektu posuzování shody, který certifikát nebo osvědčení vydal. V druhém případě bude účastníkem řízení kromě poskytovatele regulované služby, o pozastavení jehož certifikace nebo osvědčení se řízení vede, také orgán posuzování shody, který předmětnou certifikaci nebo osvědčení vydal a který bude osobou povinnou k vykonání uložené povinnosti pozastavit platnost certifikace nebo osvědčení.

Svým charakterem se tento trest blíží reaktivnímu opatření, pro jeho vydání jsou tedy stanoveny obdobné procesní požadavky. O uložení pozastavení platnosti certifikace nebo osvědčení bude vedeno správní řízení a vlastní trest bude uložen rozhodnutím Úřadu. Považuje-li Úřad skutková zjištění za dostatečná, může být vydání rozhodnutí o pozastavení platnosti certifikace nebo osvědčení prvním úkonem v řízení. Zahájení řízení bude v mnoha případech navazovat na provedenou kontrolu nebo jiné zjištění skutečností o neplnění uloženého nápravného opatření. Obdobně jako v případě reaktivního opatření je cílem navrhovaného trestu bezodkladná a účinná reakce na identifikovaný nezákonný stav a ohrožení kybernetické bezpečnosti regulovaných aktiv, rozklad proti rozhodnutí o pozastavení platnosti certifikace nebo osvědčení tedy nebude mít odkladný účinek.

V České republice v současné době neexistuje žádná centrální databáze certifikací a osvědčení, z toho důvodu je potřeba informaci o pozastavení certifikace nebo osvědčení distribuovat mezi veřejnost a odběratele služeb dotčeného poskytovatele regulované služby jiným vhodným způsobem. Jako nejefektivnější způsob se jeví uveřejnění informace o pozastavení platnosti certifikace nebo osvědčení na internetových stránkách Úřadu jakožto centrálním zdroji informací o zajišťování kybernetické bezpečnosti v České republice. Na internetových stránkách Úřadu budou uveřejňovány minimálně informace o vydání rozhodnutí o pozastavení platnosti certifikace nebo osvědčení a o vydání osvědčení o splnění uloženého nápravného opatření a o pominutí důvodů pro pozastavení platnosti certifikace nebo osvědčení. U certifikátů vydávaných Úřadem bude moci být uvedena i informace o vlastním pozastavení a obnově platnosti certifikace.

Splnění uloženého nápravného opatření nemůže být ze strany regulované osoby pouze deklarováno, ale musí být též prokázáno. Za tím účelem Úřad u regulované osoby provede kontrolu splnění uloženého nápravného opatření. Kontrola se provede nejdříve po uplynutí minimální lhůty stanovené zákonem. Na základě výsledků provedené kontroly vydá Úřad osvědčení o splnění uloženého nápravného opatření, které bude sloužit jako podklad pro obnovu platnosti certifikátu nebo osvědčení. Pokud se bude pozastavení platnosti certifikace nebo osvědčení týkat certifikace nebo osvědčení vydaného jinou osobou než Úřadem, Úřad o vydání osvědčení informuje všechny účastníky původního řízení o uložení pozastavení platnosti certifikace nebo osvědčení; vlastní provedení obnovy platnosti již Úřad nedozoruje a poskytovatel regulované služby by si jej měl ohlídat sám. Informace o vydání osvědčení o

splnění nápravného opatření a o pominutí důvodů pro pozastavení platnosti certifikace nebo osvědčení se uvede na internetových stránkách Úřadu.

Vůči zahraničnímu subjektu posuzování shody, který vydal certifikaci nebo osvědčení, jež je předmětem řízení o pozastavení platnosti, nebo poskytovateli regulované služby usazenému v jiném členském státě budou přiměřeně aplikována ustanovení o vzájemné spolupráci členských států obsažená v tomto zákoně a směrnici NIS2.

K § X – Pozastavení výkonu řídicí funkce

Pozastavení výkonu řídicí funkce je jedním ze dvou zcela nových správních trestů, jehož zakotvení v právním řádu vyžaduje směrnice NIS2, konkrétně její čl. 32 odst. 5. Podle tohoto ustanovení musí členské státy zajistit, aby měly dozorové orgány (zde Úřad) v případě nesplnění uloženého nápravného opatření pravomoc požadovat po k tomu příslušných orgánech nebo soudech uložení dočasného zákazu výkonu řídicí funkce v základním subjektu jakékoliv fyzické osobě, která má odpovědnost za výkon řídicích funkcí na úrovni výkonného ředitele nebo zákonného zástupce v tomto subjektu. Uvedené ustanovení má za cíl dále posílit účinnost a odrazující účinek opatření v oblasti vymáhání, jež jsou uplatňována v případě porušení směrnice (srov. bod 133 preambule směrnice NIS2). Citované ustanovení je také součástí komplexu opatření pro posílení odpovědnosti vedení organizace za zajišťování kybernetické bezpečnosti, na kterou klade směrnice NIS2 zvláštní důraz. Doplňuje tak např. ustanovení o povinném vzdělávání managementu nebo o odpovědnosti osob oprávněných jednat jménem regulovaného subjektu za plnění povinností spočívajících v zajištění dodržování směrnice (srov. zejm. čl. 20 a čl. 32 odst. 6 směrnice NIS2).

Podpůrně má toto ustanovení za cíl také zajistit, že v řídicí funkci organizace nebude po dobu nápravy nedostatku, pro který bylo uloženo provedení nápravného opaření, osoba, která nápravě nedostatku svým jednáním brání. Tento správní trest tak nemá sloužit jako pouhé potrestání poskytovatele regulované služby za nesplnění jeho zákonných povinností, ale především jako donucovací prostředek k provedení povinnosti, pro jejíž nesplnění byl uložen.

Směrnice NIS2 stanoví, že členské státy nemají konstituovat dozorovému orgánu novou pravomoc (byť i tato možnost byla v průběhu vyjednávání textu směrnice NIS2 zvažována), ale mají využít existujících vnitrostátních mechanismů. Na vnitrostátní úrovni upravuje proces vyloučení člena statutárního orgánu z výkonu funkce zákon č. 90/2012 Sb., o obchodních korporacích, když umožňuje soudu i bez návrhu rozhodnout, že člen statutárního orgánu obchodní korporace, který v posledních 3 letech před zahájením řízení opakovaně nebo závažně porušil své povinnosti při výkonu funkce, nesmí až po dobu 3 let od právní moci rozhodnutí o vyloučení vykonávat funkci člena statutárního orgánu jakékoli obchodní korporace. Návrh zákona z tohoto procesu vychází, některé prvky však v zájmu dosažení sledovaného cíle modifikuje. Ustanovení zákona o obchodních korporacích upravující vyloučení člena statutárního orgánu z výkonu funkce se pak v částech právních účinků pravomocného rozhodnutí o vyloučení člena statutárního orgánu, informování rejstříkového soudu a odpovědnosti za porušení dočasného zákazu výkonu funkce použijí obdobně. To platí i pro procesní otázky spojené s vedením řízení, které se budou řídit zákonem č. 99/1963 Sb., občanským soudním řádem. Úřad je jakožto ústřední orgán státní správy České republiky osvobozen od soudních poplatků.

Odst. 1 stanoví, že soud může rozhodovat pouze na návrh Úřadu. Návrh Úřadu může směřovat vůči osobám v řídicích pozicích regulovaných osob, s ohledem na rozmanitost regulovaných osob pak není omezen pouze na statutární orgány obchodních korporací. V souladu s požadavkem směrnice NIS2 a vzhledem k možným komplikacím spojeným s aplikací uvedeného ustanovení u subjektů veřejné správy (v nichž jsou řídicí pozice často

obsazovány specifickým postupem) nejsou v množině osob, proti kterým lze návrh směřovat, zahrnuty funkce ve veřejné správě.

Důvodem pro pozastavení výkonu řídicí funkce musí být jednání, které má přímou souvislost s plněním povinnosti uložené nápravným opatřením Úřadu a které představuje závažné nebo opakované (tedy i méně závažné, ale vícečetné) porušení povinností osoby při výkonu řídicí funkce, které vede ke zmaření řádného splnění rozhodnutí Úřadu. Toto jednání musí být osobě v řídicí funkci přičitatelné. Typicky půjde o situace, kdy osoba v řídicí funkci odmítne provést bez relevantního důvodu povinnost uloženou nápravným opatřením Úřadu, nebo její splnění bezdůvodně maří či oddaluje.

Obdobně jako v případě trestu pozastavení platnosti certifikace nebo osvědčení lze i trest pozastavení výkonu řídicí funkce uložit pouze poskytovateli regulované služby v režimu vyšších povinností. Rozšíření možnosti ukládání i na poskytovatele regulovaných služeb v režimu nižších povinností se s ohledem na charakter těchto subjektů a omezený rozsah povinností, které jim z navrhované regulace plynou, nejeví jako přiměřené. Zároveň je tím vyhověno požadavku směrnice NIS2, která vyžaduje ukládání tohoto druhu trestu jen základním subjektům.

Vzhledem k závažnosti daného trestu a dopadu na činnost subjektů a v konečném důsledku na uživatele by dočasné pozastavení výkonu řídicí funkce mělo být uplatňováno pouze v krajních případech, úměrně závažnosti porušení a s ohledem na okolnosti každého jednotlivého případu. Aplikovatelnost trestu není omezena jinými předpoklady (např. vyčerpáním zbylých sankčních mechanismů zákona), nicméně z povahy věci by mělo být ukládáno pouze tam, kde skutečně povede k cíli, tedy ke splnění uloženého nápravného opatření, a nebude představovat nepřiměřený zásah do práv regulované osoby.

Stejně tak by dočasné pozastavení výkonu řídicí funkce mělo být uplatňováno pouze na nezbytně nutnou dobu, tedy jakmile je povinnost uložená nápravným opatřením splněna, má dojít k obnově možnosti výkonu řídicí funkce. V zájmu posílení preventivní i represivní funkce navrhovaného trestu je však stanovena minimální doba, na kterou bude pozastavení výkonu řídicí funkce uloženo. Stanovení minimální doby pozastavení má za cíl také ulehčit nápadu práce Úřadu, neboť ten bude moci efektivněji plánovat kontroly splnění uložených nápravných opatření a na ně navazujících pozastavení výkonu řídicí funkce. Stanovená doba 6 měsíců se v kontextu dosavadních zkušeností Úřadu s ukládáním nápravných opatření a lhůt k jejich splnění jeví jako přiměřená, neboť lhůty, které Úřad poskytuje pro splnění uložených nápravných opatření, v mnoha případech tuto dobu přesahují (zvláště pokud se jedná o nápravná opatření spočívající v provedení komplexních bezpečnostních opatření podle zákona).

Na základě pravomocného rozhodnutí soudu o pozastavení výkonu řídicí funkce se tato informace zapíše do obchodního rejstříku podle zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob. Zároveň se tato informace uveřejní na internetových stránkách Úřadu jakožto centrálním zdroji informací o zajišťování kybernetické bezpečnosti v České republice.

Splnění uloženého nápravného opatření nemůže být ze strany regulované osoby pouze deklarováno, ale musí být též prokázáno. Za tím účelem Úřad u regulované osoby provede kontrolu splnění uloženého nápravného opatření. Kontrola se provede nejdříve po uplynutí minimální lhůty stanovené zákonem. Na základě výsledků provedené kontroly vydá Úřad osvědčení o splnění uloženého nápravného opatření, po kterém bude možné obnovit výkon řídicí funkce a které bude sloužit jako podklad pro výmaz informace o pozastavení výkonu funkce z obchodního rejstříku (nemělo by být potřeba vydávat nové soudní rozhodnutí). Informace o vydání osvědčení o splnění nápravného opatření a o pominutí důvodů pro pozastavení výkonu řídicí funkce se uvede na internetových stránkách Úřadu.

Vůči poskytovateli regulované služby usazenému v jiném členském státě budou přiměřeně aplikována ustanovení o vzájemné spolupráci členských států obsažená v tomto zákoně a směrnici NIS2.

K § X – Vztah ke správnímu řádu a zákonu o kontrole

Směrnice NIS2 po členských státech požaduje, aby kontrola dodržování povinností plynoucích ze směrnice byla účinná a aby byly dozorové orgány schopny řádně vykonávat své svěřené pravomoci. Úřad se jakožto správní orgán při výkonu svých pravomocí řídí ustanoveními správního řádu, při výkonu kontroly pak ustanoveními zákona o kontrole. Oba předpisy poskytují správním, resp. kontrolním orgánům určité nástroje pro efektivní výkon svých pravomocí, včetně prostředků donucení. Pro zajištění řádného průběhu kontrol a správních řízení vedených Úřadem a výkonu rozhodnutí Úřadu lze využít především pořádkové pokuty podle správního řádu (zejm. pro případ, že účastník řízení nebo jiná osoba významně ztěžuje postup Úřadu tím, že neuposlechne pokynu úřední osoby), pokuty za přestupek proti kontrole podle kontrolního řádu (za neposkytnutí potřebné součinnosti podle kontrolního řádu) a donucovací pokuty, jimiž se vymáhá splnění povinnosti uložené rozhodnutím.

Výše pokut, které je možné podle obou dotčených předpisů ukládat, jsou stanoveny ve výši odpovídající době svého přijímání (v případě správního řádu se částky neměnily od roku 2006, v případě zákona o kontrole jsou neměnné od roku 2014). Za tu dobu došlo mj. vlivem inflace i růstu ekonomiky ke změně vnímání hodnoty peněz a ke změně vnímání účinnosti a efektivity pořádkových pokut a donucovacích pokut, které jsou v současnosti neúměrně nízké. Oba předpisy jsou nadto univerzálně aplikovatelné na postupy správních orgánů napříč odvětvími a žádným způsobem nezohledňují závažnost a charakter pochybení, v jejichž souvislosti jsou aplikovány. Do navrhované regulace kybernetické bezpečnosti budou primárně spadat velké a střední podniky, tzn. subjekty, jejichž obrat se pohybuje v řádech stovek milionů až miliard korun. Maximální výše pokut, které bude možné uložit za nejzávažnější pochybení proti navrhované regulaci, jsou stanoveny na úrovni 250 milionů Kč. Uložení pořádkové nebo donucovací pokuty v současné výši (50, resp. 100 tisíc Kč) tak nemůže být pro regulované subjekty motivační. Stejně tak maximální pokuta za přestupek proti kontrole, jehož spácháním se regulovaný subjekt může vyhnout uložení maximální výše pokuty za neplnění povinností v oblasti kybernetické bezpečnosti, nemůže být stanovena na částce 500 000 Kč, neboť vůbec neodpovídá povaze a závažnosti pochybení. Z uvedených důvodů je potřeba zvýšit maximální sazby pokut, jejichž cílem je donutit regulovanou osobu poskytovat součinnost Úřadu při výkonu jeho dozorových pravomocí.

Speciální úprava ukládání pořádkové pokuty je inspirována zákonem č. 395/2009 Sb., o významné tržní síle a nekalých obchodních praktikách při prodeji zemědělských a potravinářských produktů. Také do působnosti tohoto zákona spadají hospodářsky silné subjekty, vůči nimž bylo potřeba posílit motivační funkci donucovacích prostředků správního řádu a zákona o kontrole (byť jeho aplikace je nahrazena speciální procesní úpravou). Pořádkové pokuty, kterými má být zajištěno poskytnutí nezbytné součinnosti pro provedení šetření, je možné ukládat opakovaně, maximální výše pořádkových pokut je stanovena na shodné úrovni jako vlastní pokuta za porušení pravidel stanovených zákonem. Šetřený subjekt je tedy motivován k poskytnutí nezbytné součinnosti, neboť až na nejzávažnější případy tím snižuje finanční dopady porušení svých zákonných povinností. Tím je dosaženo zkrácení šetření věci a umožněna rychlá náprava nevyhovujícího stavu. Obdobný přístup je třeba aplikovat i ve vztahu k regulaci kybernetické bezpečnosti, neboť i v této oblasti je dán zvýšený veřejný zájem na rychlém vyšetření možného porušení pravidel kybernetické bezpečnosti a na bezodkladné nápravě nevyhovujícího stavu.

Odst. 1 stanoví maximální výši jedné pořádkové pokuty na 100 000 Kč, celkově pak nesmí výše opakovaně ukládaných pokut přesáhnout 10 000 000 Kč nebo 1 % z čistého obratu dosaženého právnickou nebo podnikající fyzickou osobou za poslední ukončené účetní období, podle toho, která z daných částek je vyšší. Pořádkovou pokutu je lze možné uložit i opakovaně, což jen zdůrazňuje její procesní charakter sloužící k přinucení povinné osoby k plnění příslušné povinnosti. Maximální částky jsou stanoveny jako dvojnásobek jednorázové pokuty podle správního řádu, resp. jako zlomek pevné a polovina pohyblivé maximální pokuty za nejzávažnější přestupky proti zákonu. Nadto stále platí povinnost Úřadu ukládat pokuty přiměřeně okolnostem, zohledňovat konkrétní skutkové okolnosti případu a neukládat pokuty, které by byly likvidační (což by šlo navíc proti smyslu pořádkových pokut). Méně ekonomicky silným subjektům tak budou zpravidla ukládány pokuty nižší.

Obdobným způsobem a z obdobných důvodů dochází i ke zvýšení maximální výše celkově uložených donucovacích pokut, kterými se vymáhá plnění rozhodnutí Úřadu.

U obou institutů bylo přistoupeno k vázání pohyblivé hranice pokuty pouze na obrat dotčené právnické nebo podnikající fyzické osoby (na rozdíl od pohyblivé hranice pokuty za přestupek proti zákonu, která je vázána na celosvětový obrat konsolidačního celku, pokud je dotčená osoba jeho součástí). Oba druhy pokut budou ukládány za účelem donucení dotčené osoby plnit své povinnosti, často v okamžiku, kdy celosvětový obrat konsolidačního celku není znám (neboť jsou teprve shromažďovány podklady pro učinění závěru, zda bude uložena pokuta za přestupek) a jeho zjišťování by komplikovalo průběh probíhajícího řízení a mařilo účel ukládání pořádkové nebo donucovací pokuty, kterým je rychlé a efektivní donucení osoby splnit uloženou povinnost.

Odst. 3 zvyšuje maximální pokutu za přestupek proti kontrole podle zákona o kontrole na 10 000 000 Kč. Jde o zlomek maximální pokuty za nejzávažnější přestupky proti zákonu, kterým se subjekt neposkytnutím součinnosti podle zákona o kontrole může vyhnout. Zároveň však jde o částku, která by i pro ekonomicky silné subjekty měla být motivační. Uložení pokuty za přestupek proti kontrole přitom nevylučuje ukládání pořádkových pokut v případě, že stále nebude splněna sankcionovaná povinnost. V takovém případě nepůjde o dvojí trestání, neboť každý z institutů míří na porušení odlišné povinnosti. Cílem sankčních ustanovení kontrolního řádu je přinutit kontrolovaný subjekt ke spolupráci při kontrole, odmítá-li ji dobrovolně. Sankce je zde ukládána za porušení hmotněprávní povinnosti, tedy povinnosti vytvořit podmínky pro výkon kontroly a poskytovat při ní potřebnou součinnost. Naopak cílem pořádkových pokut je sankcionování porušení procesní povinnosti a jejím primárním cílem není potrestání pachatele, ale donucení ke splnění povinnosti, která není plněna (jakmile je povinnost splněna, nelze pořádkové pokuty na rozdíl od pokuty za přestupek proti kontrole dále ukládat).

K § X – Součinnost a informační povinnost

Navrhované ustanovení upravuje spolupráci Úřadu s dozorovými orgány podle jiných právních předpisů a dalšími orgány a osobami, u nichž je to vyžadováno směrnicí NIS2 nebo národními potřebami. Předmětem spolupráce je především výměna informací nezbytných pro řádný výkon zákonných pravomocí Úřadu a jiných dozorových orgánů a poskytování relevantních informací institucím Evropské unie.

Odstavec 1 se týká spolupráce Úřadu s jinými orgány veřejné moci. Výměna informací má sloužit k efektivnímu výkonu zákonem svěřených pravomocí Úřadu i jiných orgánů veřejné moci, zvláště v oblastech, ve kterých se pravomoci Úřadu a jiných orgánů veřejné moci překrývají nebo doplňují (typicky v oblastech regulace kritické infrastruktury nebo dozoru nad odvětvími, kde je kybernetická bezpečnost regulována také sektorovou legislativou). Výměnou informací však nesmí být dotčena zákonná mlčenlivost zaměstnanců Úřadu, stejně jako Úřad

musí dbát ochrany zajišťování kybernetické bezpečnosti nebo účinnost protiopatření vydaného podle tohoto zákona.

Podle odstavce 2 je každý povinen vyhovovat žádostem Úřadu o součinnost při plnění jeho úkolů. Toto ustanovení míří zejm. na součinnost regulovaných orgánů a osob, ale i jiných orgánů a osob nespadajících do působnosti zákona, jejichž informace nebo další součinnost jsou nezbytné pro řádný výkon činnosti Úřadu. Příkladem může být poskytnutí informací nezbytných pro posouzení naplnění kritérií pro identifikaci nebo určení regulované služby, nebo poskytnutí informací o kybernetickém bezpečnostním incidentu. Náhrada nákladů souvisejících s poskytnutím požadované informace náleží dožádanému subjektu pouze, stanoví-li tak zvláštní předpis.

Odstavec 3 stanovuje výjimku z povinnosti mlčenlivosti Generálního finančního ředitelství podle zákona č. 280/2009 Sb., daňového řádu, které vede centrální evidence a registry nezbytné pro výkon působnosti všech orgánů finanční správy a které je nadřízeno Odvolacímu finančnímu ředitelství a všem finančním úřadům. Výjimka se vztahuje na informace získané při správě daní, které jsou nezbytné pro posouzení, zda orgán nebo osoba naplňuje kritéria pro identifikaci regulované služby stanovená tímto zákonem. Průlom do daňové mlčenlivosti je tedy limitován na nezbytný rozsah údajů za účelem identifikace. Jedním z kritérií pro identifikaci regulované služby je i velikost podniku. Pro určení velikosti podniku jsou stěžejní údaje o počtu zaměstnanců a údaje o obratu nebo aktivech společnosti a vazbách mezi majetkově spřízněnými společnostmi. Úřad těmito informacemi z vlastní činnosti nedisponuje a je při jejich zjišťování odkázán na veřejně dostupné informace, tvrzení posuzovaného subjektu a informace od jiných orgánů veřejné správy. Informace o hospodaření podnikatelů nejsou vždy veřejně dostupné, stejně jako není vždy možné z veřejných zdrojů dohledat kompletní informace o vazbách majetkově spřízněných subjektů. Finanční správa získává informace o majetkových poměrech a finančním hospodaření subjektu při správě daní, orgány finanční správy jsou tak schopny poskytnout Úřadu relevantní informace nezbytné pro posouzení zákonných kritérií. Stejně tak je finanční správa schopna poskytnout Úřadu spolehlivé informace o předmětu činnosti posuzovaného subjektu, případně další informace nezbytné pro posouzení naplnění kritérií pro identifikaci regulované služby. V odůvodněných případech tak zásada mlčenlivosti při správě daní ustupuje jinému veřejnému zájmu, zde veřejnému zájmu na zajišťování kybernetické bezpečnosti u vybraných subjektů. Za účelem zajištění hladké komunikace mezi orgány finanční správy a Úřadem z hlediska odbornosti a jednotného postupu finanční správy není prolomení daňové mlčenlivosti stanoveno daňovým řádem pro finanční správu obecně. Současně navrhované ustanovení zachovává možnost Generálního finančního ředitelství žádosti nevyhovět, pokud by poskytnutím informací mohlo dojít k narušení řádného výkonu správy daní. Návrh tak umožňuje v konkrétních případech zohlednit také zájem státu na účinné správě daní.

Z obdobných důvodů jako odst. 3 stanovuje odst. 4 oprávnění Úřadu získat způsobem umožňujícím dálkový přístup z evidence skutečných majitelů úplný výpis platných údajů a údajů, které byly vymazány bez náhrady nebo s nahrazením novými údaji podle zákona upravujícího evidenci skutečných majitelů. Automatizace získávání informací má za cíl zrychlit a zjednodušit proces identifikace nově regulovaných subjektů. Umožnění dálkového přístupu do evidence skutečných majitelů bylo předem konzultováno s Ministerstvem spravedlnosti, které samo navrhlo obecnější formulaci zmocňovacího ustanovení.

Odst. 5 upravuje poskytování informací vyžadovaných směrnicí NIS2. V části se jedná o informace o identifikaci povinných subjektů nebo přijímání a zavádění národních strategií kybernetické bezpečnosti, které jsou poskytovány i za účinnosti zákona č. 181/2014 Sb., v části jde o nové informační povinnosti mající za cíl efektivnější řízení kybernetických

bezpečnostních rizik na úrovni Evropské unie a posílení spolupráce mezi členskými státy a unijními institucemi.

K § X – Výmaz z evidence poskytovatelů regulovaných služeb

Ustanovení upravující výmaz z evidence poskytovatelů regulovaných služeb zrcadlí ustanovení o zápisu do evidence. Platí tedy, že obdobným procesem, jakým jsou poskytovatel regulované služby nebo jím poskytované regulované služby zapsáni do evidence, jsou z ní také vymazáni.

Odst. 1 upravuje situaci, kdy zapsaná služba, kterou poskytovatel regulované služby poskytuje, přestane splňovat kritéria pro identifikaci regulované služby, nebo přestala být poskytována úplně. V takovém případě Úřad, jakmile se dozví o skutečnosti, že zapsaná služba již nesplňuje definiční znaky regulované služby, zapsanou službu vymaže z evidence poskytovatelů regulovaných služeb a o tomto úkonu daného poskytovatele regulované služby písemně vyrozumí.

Odst. 2 upravuje situaci, kdy zapsaná služba, kterou poskytovatel regulované služby poskytuje, přestane splňovat kritéria pro určení regulované služby, nebo přestala být poskytována úplně. Úřad postupuje obdobně jako v případě, že se dozví o novém poskytovateli regulované služby nebo nové regulované službě, která naplňuje kritéria pro určení regulované služby, tedy v rámci správního řízení rozhodne o tom, že služba, kterou poskytovatel regulované služby poskytuje, nesplňuje kritéria pro určení regulované služby. Na základě pravomocného rozhodnutí pak Úřad provede výmaz z evidence.

Zatímco první dva odstavce upravují situaci, kdy zapsaná služba přestala splňovat kritéria regulované služby, avšak poskytovatel regulované služby poskytuje další regulované služby, pro které zůstává veden v evidenci poskytovatelů regulovaných služeb, odst. 3 upravuje situaci, kdy poskytovatel regulované služby přestane splňovat kritéria regulované služby pro všechny služby, které poskytuje a které má v evidenci zapsány. V takovém případě není dále nutné vést poskytovatele regulované služby v evidenci poskytovatelů regulovaných služeb a Úřad jej z evidence vymaže. Praktickým důsledkem bude nutnost nové registrace poskytovatele regulované služby v případě, že tento orgán nebo osoba začne znovu poskytovat službu naplňující kritéria regulované služby.

Obdobně jako v případě zápisu do evidence poskytovatelů regulovaných služeb musí být poskytovatel regulované služby, jehož služba je z evidence mazána, o výmazu písemně vždy vyrozuměn. Písemné vyrozumění o výmazu z evidence musí být poskytovateli regulované služby prokazatelně doručeno, neboť až od tohoto okamžiku přestává být poskytovatel regulované služby ve vztahu k vymazané službě povinen plnit zákonné požadavky.

K § X – Společná a zvláštní ustanovení o řízení před Úřadem

Odst. 1 upravuje součinnost orgánů a osob nezbytnou pro řádné posouzení naplnění kritérií pro identifikaci nebo určení regulované služby. Za účinnosti zákona č. 181/2014 Sb. byla povinnost součinnosti dovozována z obecných ustanovení správního řádu o opatřování podkladů rozhodnutí, v případě určování prvků kritické infrastruktury pak z ustanovení o poskytování součinnosti podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). Povinnost poskytnout Úřadu nezbytnou součinnost má podle navrhovaného ustanovení každý orgán nebo osoba, o kterých lze důvodně předpokládat, že naplňují kritéria pro identifikaci nebo určení regulované služby. Povinnost se tak vztahuje jak na subjekty, u nichž je potřeba posoudit naplnění kritérií pro identifikaci regulované služby (tzn. typicky subjekty, které měly povinnost provést tzv. samoidentifikaci, ale neučinily tak, nebo Úřad považuje za nezbytné výsledek samoidentifikace přezkoumat), tak na subjekty, s nimiž má být vedeno řízení o určení regulované služby.

Odst. 2 stanoví povinnost orgánů odpovědných za určování prvků kritické infrastruktury podle krizového zákona informovat Úřad o určení prvku kritické infrastruktury a důvodech jeho určení. Tato povinnost je stanovena v návaznosti na úzké propojení regulace fyzické a kybernetické bezpečnosti subjektů označených za kritické podle 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 (směrnice CER). Subjekty určené jako kritické podle pravidel směrnice CER (transponovaných do vnitrostátního práva právě prostřednictvím krizové legislativy) se stávají povinnými subjekty i podle tohoto zákona. Proces zahrnutí těchto subjektů do regulace kybernetické bezpečnosti však není automatický, Úřad v souladu s pravidly prováděcího předpisu vydá o určení kritického subjektu poskytovatelem regulované služby rozhodnutí. Za tím účelem Úřad potřebuje disponovat informacemi o tom, které orgány a osoby byly určeny subjekty spadajícími do působnosti regulace odolnosti kritických subjektů (v důsledku určení prvku kritické infrastruktury).

Odst. 3 a násl. upravují specifické požadavky na proces některých jednání Úřadu podle tohoto zákona. Úřad je při své činnosti standardně vázán ustanoveními správního řádu, některá specifická jednání však vyžadují úpravu obecných pravidel. Jde zejména o proces registrace poskytovatele regulované služby, změn registrace, zápisu do evidence poskytovatelů regulovaných služeb a výmazu z evidence, určování regulované služby a řízení o změně režimu poskytovatele regulované služby, u nichž je dán zájem na rychlém a efektivním vyřízení bez zbytečného prodlení. Důvody jsou přitom obdobné jako v případě procesu určování provozovatelů základní služby podle zákona č. 181/2014 Sb. Vzhledem k zájmům, jejichž ochrana byla určováním provozovatelů základních služeb sledována (zejména národní bezpečnosti a ochrana obyvatelstva), bylo nutné, aby proces určování podle zákona č. 181/2014 Sb. probíhal pokud možno bez výraznějšího zpoždění. Oproti předchozí právní úpravě bude většina regulovaných subjektů zařazena do působnosti tohoto zákona na základě samoidentifikace a následné odpovědně provedené registrace. Zjednodušení procesu registrace a zápisu je tedy 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 poskytovatelů regulovaných služeb tyto subjekty nejsou odpovědné za zabezpečování svých systémů a hlášení incidentů. Jakékoli prodlužování procesu zařazení subjektů do regulace oddaluje okamžik, od kterého jsou tyto subjekty odpovědné za zajišťování kybernetické bezpečnosti své organizace a ochranu regulovaných služeb.

Identifikace regulovaných služeb probíhá na základě relativně jednoduchých a v zásadě jednoznačných kritérií pro identifikaci regulované služby, samoidentifikace by tedy pro povinné subjekty neměla představovat významnější komplikace. Proces registrace poskytovatele regulované služby a zápisu do evidence poskytovatelů regulovaných služeb tak není potřeba zatěžovat nadbytečnými procesními požadavky, které by proces zařazení subjektu do regulace neúměrně komplikovaly. Registrace poskytovatele regulované služby Úřadem v případě, že ten svou povinnost zaregistrovat se sám nesplní, je pouze náhradou jednání poskytovatele regulované služby a faktickou nápravou nezákonného stavu. Zápis do evidence poskytovatelů regulovaných služeb je pak automatickým důsledkem registrace poskytovatele regulované služby.

V případě, že poskytovatel regulované služby zapsaný v evidenci poskytovatelů regulovaných služeb přestane splňovat kritéria pro identifikaci regulované služby, nebo nebude

souhlasit s důvody pro svou registraci a zápis (pokud ji provedl jeho jménem Úřad), má možnost vyzvat Úřad k přezkoumání splnění kritérií regulované služby a relevance svého vedení v evidenci poskytovatelů regulovaných služeb iniciací řízení o výmazu z evidence (ať již formou žádosti o zahájení řízení o výmazu, nebo podnětu k zahájení řízení z moci úřední).

Řízení o určení regulované služby a řízení o změně režimu poskytovatele regulované služby z režimu nižších povinností na režim vyšších povinností jsou řízeními vedenými ve veřejném zájmu (na určení regulované služby nebo změnu režimu poskytovatele regulované služby v důsledku naplnění kritérií reflektujících základní bezpečnostní zájmy státu v oblasti kybernetické bezpečnosti není právní nárok). Z toho důvodu je stanoveno, že tato řízení lze zahájit pouze z moci úřední.

Z výše popsaných důvodů založených na potřebě rychlého a efektivního rozhodování o zařazení poskytovatele regulované služby nebo některé z jím poskytovaných služeb do regulace tohoto zákona, resp. zachování regulace služeb, u nichž je naplnění kritérií pro identifikaci nebo určení regulované služby rozporováno, je u vybraných řízení vyloučeno podání rozkladu proti rozhodnutí Úřadu. Podání rozkladu proti rozhodnutí Úřadu je dále vyloučeno u rozhodnutí o udělení, prodloužení a odebrání autorizace inspektora. Rozhodnutí o udělení a prodloužení autorizace inspektora jsou vydávána ve prospěch tohoto inspektora, marné plynutí lhůty pro podání rozkladu by tedy jen prodlužovalo okamžik zahájení činnosti inspektora. U rozhodnutí o odebrání autorizace inspektora je pak dán veřejný zájem na co nejrychlejším ukončení činnosti inspektora, který nesplňuje podmínky pro udělení autorizace a pro výkon kontrol podle tohoto zákona. V uvedených případech není dotčena možnost podat proti rozhodnutí Úřadu žalobu ke správnímu soudu. Naopak možnosti obrany proti rozhodnutí Úřadu o neudělení autorizace inspektora nejsou omezeny.

Odst. 6 pak stanoví zjednodušený režim pro vedení řízení o výmazu z evidence poskytovatelů regulovaných služeb zahájené z moci Úřední. V případech, kdy Úřad považuje skutková zjištění za dostatečná bude výmaz z evidence poskytovatelů regulovaných služeb proveden zjednodušeným způsobem bez vyhotovení písemného rozhodnutí. Zkracuje se tak proces vedoucí k vyřazení poskytovatele regulované služby nebo některé z jím poskytovaných služeb z působnosti zákona, pokud pro jejich zařazení již nejsou dány zákonné důvody. Poskytovateli regulované služby není takovým rozhodnutím nikterak zasahováno do práv, naopak jsou mu pouze odnímány či redukovány jeho zákonné povinnosti.

K § X – Zvláštní ustanovení k exekuci správního rozhodnutí

Ustanovení správního řádu o exekuci správního rozhodnutí umožňují provést exekuci nepeněžitého plnění náhradním výkonem v případě zastupitelných plnění, přímým vynucením v případě nezastupitelných plnění, zejména vyklizením, odebráním movité věci a předvedením, nebo ukládáním donucovacích pokut. Ve vztahu k exekuci rozhodnutí Úřadu, kterým se významnému dodavateli ukládá povinnost předat poskytovateli regulované služby informace a data související s provozem aktiv sloužících k poskytování regulované služby, vyvstávají výkladové spory o to, zda lze informace a data podřadit pod pojem movitá věc, a tedy zda lze při výkonu rozhodnutí postupovat podle ustanovení správního řádu o exekuci odebráním movité věci. Občanský zákoník sice definuje pojem věc široce, když stanoví, že věcí v právním smyslu je vše, co je rozdílné od osoby a slouží potřebě lidí, odborná veřejnost se však přiklání k výkladu, že informace věcí v právním smyslu nejsou. Exekuce rozhodnutí Úřadu by tak v části týkající se informací musela probíhat v jiném režimu než exekuce dat. Z toho důvodu navrhované ustanovení stanoví, že exekuce celého rozhodnutí Úřadu, tedy i v části předání informací, se řídí ustanoveními správního řádu upravujícími exekuci movité věci.

K § X – Zástupce poskytovatele regulované služby

Navrhované ustanovení je obdobou § 3a zákona č. 181/2014 Sb. a upravuje ustanovení zástupce poskytovatelů vybraných regulovaných služeb a subjektů poskytujících služby registrace jmen domén usazených mimo Evropskou unii. V případě poskytovatelů vybraných digitálních služeb může, vzhledem k povaze těchto služeb, snadno dojít k tomu, že dotčený podnikatel nemusí být usazen (mít sídlo) v rámci Evropské unie. Směrnice takovou situaci řeší stanovením povinnosti poskytovatele v případě, že nabízí v Unii své služby, ustavit si v rámci Unie svého zástupce. Členský stát Unie, ve kterém je takový zástupce určen, se pak považuje za stát, v němž je poskytovatel digitálních služeb usazen a dopadá na něj tedy regulace příslušného orgánu tohoto členského státu.

Směrnice NIS2 pojem usazení váže na umístění hlavní provozovny a ve svém recitálu 114 jej vymezuje takto: *„Kritérium provozovny pro účely této směrnice předpokládá účinný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem. To, zda je toto kritérium splněno, by nemělo záviset na tom, zda se sítě a informační systémy fyzicky nacházejí na daném místě; sama přítomnost a samotné používání takových sítí a systémů nejsou podstatou hlavní provozovny, a tudíž ani nejsou rozhodujícími kritérii pro její určení. Mělo by se mít za to, že hlavní provozovna se nachází v členském státě, kde jsou v Unii převážně přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. To bude obvykle odpovídat místu, kde se nachází ústřední správa subjektu v Unii. Nelze-li takový členský stát určit nebo nejsou-li tato rozhodnutí přijímána v Unii, mělo by se mít se za to, že hlavní provozovna je v členském státě, v němž jsou prováděny operace v oblasti kybernetické bezpečnosti. Nelze-li takový členský stát určit, mělo by se mít za to, že hlavní provozovna se nachází v členském státě, v němž má subjekt provozovnu s nejvyšším počtem zaměstnanců v Unii. Pokud jsou služby prováděny skupinou podniků, měla by se za hlavní provozovnu skupiny podniků považovat hlavní provozovna řídícího podniku.“*

Směrnice se pak dále ve svém recitálu 116 věnuje vymezení poskytování služeb v rámci Unie, když stanoví následující: *„Aby bylo možno určit, zda takový subjekt nabízí služby v rámci Unie, mělo by být ověřeno, zda má tento subjekt v úmyslu nabízet služby osobám v jednom nebo více členských státech. Pouhá dostupnost internetových stránek subjektu nebo jeho zprostředkovatele v Unii nebo dostupnost e-mailové adresy nebo dalších kontaktních údajů nebo používání jazyka obecně používaného ve třetí zemi, v níž je subjekt usazen, by k ověření tohoto úmyslu postačovat neměla. Avšak faktory jako používání jazyka nebo měny obecně používaných v jednom nebo více členských státech, spolu s možností objednat služby v tomto jazyce, nebo zmínka o zákaznících či uživatelích nacházejících se v Unii by mohly být zjevným dokladem o tom, že subjekt má v úmyslu nabízet služby v rámci Unie.“*

Otázkou zaměření služeb na konkrétní členský stát se zaobíral i Soudní dvůr Evropské unie, konkrétně ve svých rozhodnutích ve věcech C-585/08 a C-144/09. Za účelem určení, zda podnikatel, jehož činnost je prezentována na jeho internetové stránce nebo na internetové stránce jeho zprostředkovatelské společnosti, může být považován za podnikatele „zaměřujícího“ činnost na členský stát, na jehož území má spotřebitel své bydliště ve smyslu čl. 15 odst. 1 písm. c) nařízení č. 44/2001, je třeba ověřit, zda před případným uzavřením smlouvy se spotřebitelem z uvedených internetových stránek a celkové činnosti podnikatele vyplývalo, že podnikatel zamýšlel obchodovat se spotřebiteli s bydlištěm v jednom či více členských státech, včetně členského státu, ve kterém má spotřebitel bydliště, v tom smyslu, že byl připraven uzavřít s nimi smlouvu.

Následující skutečnosti, jejichž výčet není taxativní, mohou představovat indicie umožňující se domnívat, že činnost podnikatele je zaměřena na členský stát bydliště spotřebitele:

1. mezinárodní povaha činnosti,
2. popis cesty do sídla podnikatele s počátkem v jiných členských státech,
3. použití jiného jazyka nebo jiné měny, než jsou jazyk nebo měna, které jsou obvykle používány v členském státě, ve kterém má podnikatel sídlo s možností provést rezervaci a potvrdit ji v tomto jiném jazyce,
4. uvedení telefonického spojení s mezinárodním předčíslím,
5. vynaložení nákladů na službu sponzorovaných odkazů na internetu s cílem usnadnit spotřebitelům s bydlištěm v jiných členských státech přístup na stránku podnikatele nebo jeho zprostředkovatele,
6. použití jiného jména domény prvního řádu, než je doména členského státu, ve kterém má podnikatel sídlo, a
7. uvedení mezinárodní klientely složené ze zákazníků s bydlištěm v jiných členských státech.

Naproti tomu pouhá dostupnost internetové stránky podnikatele nebo jeho zprostředkovatelské společnosti v členském státě, na jehož území má spotřebitel bydliště, nepostačuje. Stejně je tomu v případě uvedení elektronické adresy, jakož i dalších kontaktních údajů nebo v případě využití jazyka nebo měny, které jsou obvykle používány v členském státě, ve kterém má podnikatel sídlo.

V rozhodnutí ve věci C-230/14 Soudní dvůr Evropské unie uvedl, že soud může za účelem určení zaměření služeb na členský stát zohlednit zejména skutečnost, že činnost správce, v rámci níž k uvedenému zpracování dochází, spočívá v provozování webových stránek s inzeráty na nemovitosti nacházející se na území tohoto členského státu, které jsou v jazyce tohoto státu, a že je tato činnost tedy zaměřena především, nebo dokonce zcela na uvedený členský stát, a dále skutečnost, že tento správce má v uvedeném členském státě zástupce, jehož úkolem je vymáhat pohledávky vyplývající z této činnosti, jakož i zastupovat správce ve správních a soudních řízeních souvisejících se zpracováním předmětných údajů.

Směrnice řeší i stav, kdy je poskytovatel vybraných digitálních služeb usazen v jednom členském státu Evropské unie (v našem případě tedy v České republice), ale jeho sítě a informační systémy jsou umístěny v jiném členském státu. V takovém případě se zavádí povinnost Úřadu spolupracovat s příslušným úřadem tohoto dotčeného členského státu pro zjištění reálného stavu zajištění bezpečnosti sítí a informačních systémů a řešení případných nedostatků. Poskytování vzájemné pomoci upravuje návrh zákona v § X věnovanému vzájemné spolupráci členských států.

Ustaveným zástupcem musí být vždy osoba (fyzická, či právnická), která je usazená v Evropské unii, neboť v případě, že by tomu tak nebylo, ztrácel by institut ustavení zástupce jakýkoliv reálný smysl. Vzhledem k působnosti Úřadu je právní úprava adresována v tomto ustanovení zástupcům usazeným v České republice. Pro větší právní jistotu se stanoví, že zástupce musí být výslovně (doložitelně) pověřen k jednání jménem poskytovatele regulovaných služeb. Tím, že poskytovatel regulované služby určí svého zástupce, nejsou dotčeny právní kroky, které by mohly být podniknuty proti poskytovateli regulované služby samotnému.

Návrh pak v souladu s požadavky směrnice NIS2 stanoví pravomoc Úřadu dozorovat poskytovatele vybraných digitálních služeb a jednat s nimi jako s usazenými v České republice v případě, že mají hlavní provozovnu mimo Evropskou unii a neustavili si svého zástupce v žádném členském státě Evropské unie. Uvedené má za cíl motivovat poskytovatele

regulovaných služeb k ustanovení zástupců v Evropské unii nebo ke zřízení provozoven na území Evropské unie, neboť do té doby jsou za své jednání (a porušování pravidel kybernetické bezpečnosti) odpovědní ve všech členských státech Evropské unie, ve kterých poskytují své služby.

K § X – Finanční zabezpečení stavu kybernetického nebezpečí

S ohledem na povahu stavu kybernetického nebezpečí a jeho podobnost s jinými krizovými stavy lze důvodně očekávat vznik nákladů spojených s přípravou na stav kybernetického nebezpečí a odstraňování jeho následků prostřednictvím jednotlivých opatření. V souladu se zákonem o rozpočtových pravidlech Úřad za tímto účelem vyčleňuje objem finančních prostředků k tomu potřebných, které se považují za závazný ukazatel státního rozpočtu na příští rok. V zásadě totožná právní úprava je obsažena v § 25 krizového zákona ve vztahu k finančnímu zabezpečení krizových opatření, návrh zákona ji tedy přejímá v mírně obměněné podobě.

K § X – Přechodná ustanovení

Přechodná ustanovení mají zajistit plynulý přechod z předcházející právní úpravy na úpravu novou. Je tak například stanovena kontinuita plnění povinností v oblasti kybernetické bezpečnosti u dosud regulovaných osob, platnost vydaných opatření Úřadu a nápravných opatření, nebo v jakém režimu budou probíhat řízení Úřadu týkající se splnění povinností uložených zákonem č. 181/2014 Sb.

Za účelem zachování dosažené úrovně kybernetické bezpečnosti u informačních systémů regulovaných zákonem č. 181/2014 Sb., které budou spadat i do působnosti tohoto zákona, a nezmaření investic vynaložených na zavedení bezpečnostních opatření podle vyhlášky č. 82/2018 Sb. návrh upravuje povinnosti vybraných poskytovatelů regulovaných služeb v období mezi zrušením zákona č. 181/2014 Sb. a uplynutím lhůt pro splnění veškerých požadavků a zavedení požadovaných opatření dle tohoto zákona.

I pro povinné osoby podle § 3 zákona č. 181/2014 Sb., které budou spadat do působnosti tohoto zákona na základě naplnění kritérií pro identifikaci regulované služby, bude platit stejná povinnost registrace poskytovatele regulované služby jako pro subjekty, které dosud regulaci kybernetické bezpečnosti nepodléhaly, a stejně jako nově regulovaným subjektům jim od okamžiku doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb začnou běžet lhůty pro zahájení plnění povinností podle tohoto zákona. Zatímco některé povinnosti podle tohoto zákona bude třeba začít plnit ihned od vyrozumění o zápisu do evidence, u některých povinností, typicky zavádění bezpečnostních opatření a hlášení kybernetických bezpečnostních incidentů, se uplatní přechodná lhůta pro přizpůsobení prostředí organizace plnění nových povinností. Pokud by přechodná ustanovení toto mezidobí explicitně neupravovala, došlo by k narušení kontinuity zajišťování kybernetické bezpečnosti služeb u těch organizací, které byly povinny plnit povinnosti v oblasti kybernetické bezpečnosti za účinnosti předchozí právní úpravy a u nichž je dán veřejný zájem na pokračování plnění těchto povinností. Z toho důvodu navrhované ustanovení stanoví, že v mezidobí skončení účinnosti staré právní úpravy a uplynutí lhůt pro zahájení plnění nové právní úpravy jsou dosavadní správci informačních systémů podle § 3 písm. c) až f) zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona, povinni plnit povinnosti spojené se zaváděním a prováděním bezpečnostních opatření, hlášením kybernetických bezpečnostních incidentů a plněním opatření Úřadu podle zákona č. 181/2014 Sb., a to alespoň v rozsahu, ve kterém budou povinnými osobami podle tohoto zákona.

Přechodné ustanovení podle odst. 1 se použije pouze na správce informačních systémů regulovaných předchozí právní úpravou. Ačkoli zákon č. 181/2014 Sb. reguloval jako povinné

osoby i tzv. provozovatele systémů, tj. osoby zajišťující funkčnost technických a programových prostředků tvořících regulovaný informační systém, tyto osoby spadaly do působnosti zákona převážně pro činnost spočívající v provozu „cizích“ informačních systémů, jen výjimečně svých vlastních. Naopak do působnosti nové regulace budou někteří dosavadní provozovatelé systémů spadat pro svou vlastní činnost vykonávanou prostřednictvím vlastních informačních systémů a i povinnosti v oblasti řízení bezpečnosti informací, které jim budou novou úpravou uloženy, se budou vztahovat na jejich vlastní organizaci, nikoli na organizaci odběratelů jejich služeb. Předmět a rozsah činnosti provozovatele informačního systému podle zákona č. 181/2014 Sb. a podle nové právní úpravy se tedy bude významným způsobem lišit, a z toho důvodu postrádá kontinuita regulace činnosti těchto osob ve smyslu staré právní úpravy význam.

Pro poskytovatele regulované služby v režimu vyšších povinností bude platit, že v přechodném období budou dodržovat všechna pravidla zákona č. 181/2014 Sb. a vyhlášky č. 82/2018 Sb., neboť i za účinnosti nové právní úpravy budou povinni dodržovat všechna ustanovení zákona a prováděcího předpisu upravujícího bezpečnostní opatření pro vyšší režim. Rozsah nové právní úpravy přitom nebude užší než rozsah povinností stanovených předchozí právní úpravou. Pro poskytovatele regulovaných služeb v režimu nižších povinností pak bude platit, že v přechodném období budou dodržovat alespoň ta pravidla zákona č. 181/2014 Sb. a vyhlášky č. 82/2018 Sb., která mají svůj odraz v pravidlech závazných pro poskytovatele regulovaných služeb v režimu nižších povinností. Opatření, která jdou nad rámec požadavků stanovených pro režim nižších povinností, tedy poskytovatel regulované služby v režimu nižších povinností nemusí nadále plnit. Dobrovolné plnění přísnějších požadavků není vyloučeno.

Přechodné lhůty stanovené novou právní úpravou pro zahájení plnění povinností spojených se zaváděním a prováděním bezpečnostních opatření, hlášením kybernetických bezpečnostních incidentů a plněním opatření Úřadu pak poskytovatelé regulovaných služeb využijí k přizpůsobení své organizace novým požadavkům a zavedení nových postupů, pokud je nová úprava vyžaduje.

Způsob plnění povinností podle předchozí právní úpravy bude odpovídat minimálně požadavkům stanoveným touto úpravou. Pro hlášení kybernetických bezpečnostních incidentů však platí, že se provádí podle pravidel nové regulace. Je tím zajištěno, že všechny regulované subjekty bez rozdílu budou využívat nový informační systém Úřadu (Portál NÚKIB) a Úřad nebude muset udržovat v platnosti staré a překonané procesy. U plnění zbylých povinností je taktéž preferováno používání nových procesních postupů a nových prostředků pro komunikaci s Úřadem.

Pokud by se ve výjimečných případech mělo stát, že dosavadní regulované osoby, u nichž je dán veřejný zájem na pokračování zařazení do regulace kybernetické bezpečnosti, nenaplní kritéria pro identifikaci regulované služby a z regulace nabytím účinnosti nového zákona automaticky vypadnou, přechodné opatření zajišťující kontinuitu řízení kybernetické bezpečnosti se neuplatní. Pro tyto subjekty bude platit pouze nová lhůta pro plnění povinností ze zákona navazující na určení regulované služby a poskytovatele regulované služby rozhodnutím Úřadu pro naplnění kritérií pro určení regulované služby.

Za účelem zachování právní jistoty adresátů normy je v odst. 2 stanoveno, že v řízeních ve věcech týkajících se plnění povinností podle zákona č. 181/2014 Sb. se postupuje podle pravidel tohoto zákona (v posledním účinném znění). Procesní pravidla některých institutů společných staré i nové úpravě doznala v návrhu nové regulace více či méně podstatných změn, které mohou mít vliv na postavení účastníků řízení nebo výběr ukládaných sankcí. Stejně tak hmotněprávní ustanovení doznala zásadních změn. Je proto postaveno najisto, že plnění

povinností plynoucích ze staré právní úpravy bude vymáháno v rozsahu a způsoby upravenými v této staré právní úpravě.

K § X – Změna zákona o elektronických komunikacích

V rámci svého článku 43 ruší směrnice NIS2 k datu nabytí své účinnosti články 40 a 41 směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace (dále jen „Kodex“). Je tomu tak zjednodušeně z toho důvodu, že dosavadní požadavky Kodexu, tedy *„zajistit, aby poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací přijali vhodná a přiměřená technická a organizační opatření k odpovídajícímu zvládnutí rizik pro bezpečnost sítí a služeb. [...]“* odpovídají požadavkům směrnice NIS2, která technická a organizační opatření všem poskytovatelům veřejných sítí elektronických komunikací a veřejně dostupných služeb elektronických komunikací také ukládá.

Transpozičním ustanovením článků 40 a 41 Kodexu je v českém právním prostředí ustanovení § 98 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění novelizace provedené zákonem č. 374/2021 Sb. a účinné od 1. ledna 2022.

Ustanovení § 98 zákona o elektronických komunikací doznalo touto novelizací změn a vztahuje se na *„osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací [...]“*, tedy na širší množinu, než na kterou dopadá tento návrh zákona. Z výše uvedených důvodů a z důvodu minimalizace zásahu do jiných právních předpisů doplňuje návrh zákona aktuální znění zákona o elektronických komunikacích o nový odstavec upravující vztah povinných osob podle zákona o elektronických komunikacích a zákona o kybernetické bezpečnosti. Zákon o kybernetické bezpečnosti je v této úzké problematice zvláštním předpisem vůči zákonu o elektronických komunikacích, a pokud se tedy bude jednat o orgán nebo osobu naplňující jak kritéria daná zákonem o elektronických komunikacích, tak zákonem o kybernetické bezpečnosti, budou tento orgán nebo osoba plnit povinnosti v oblasti kybernetické bezpečnosti podle zákona o kybernetické bezpečnosti. Zbylá ustanovení zákona o elektronických komunikacích a povinnosti plynoucí těmto orgánům nebo osobám z těchto ustanovení nejsou dotčena.

K § X – Změna zákona o informačních systémech veřejné správy

Vzhledem k novelizaci právní úpravy regulace využívání služeb cloud computingu v rámci zákona o kybernetické bezpečnosti, kdy dochází k vypuštění povinností pro orgány veřejné moci zajistit dodržování bezpečnostních pravidel pro orgány veřejné moci využívající služby cloud computingu a zařadit poptávaný cloud computing do bezpečnostní úrovně před uzavřením smlouvy s poskytovatelem cloud computingu a rovněž vzhledem ke zrušení prováděcího právního předpisu stanovujícího tato bezpečnostní pravidla je nutné promítnout do zákona č. 365/2000 Sb., o informačních systémech veřejné správy důsledky z těchto změn plynoucí.

V § 2 se doplňuje definice bezpečnostní úrovně informačního systému veřejné správy a upřesňuje odpovídajícím způsobem současná definice bezpečnostní úrovně cloud computingu, tak aby v § 6n vyjádřená povinnost „Orgán veřejné správy může využívat a poskytovatel cloud computingu může orgánu veřejné správy nebo poskytovateli státního cloud computingu poskytovat pouze cloud computing, jehož bezpečnostní úroveň je stejná nebo vyšší než bezpečnostní úroveň informačního systému veřejné správy nebo jeho části, k zajištění jehož provozu je využíván“ měla jasnější oporu v definičním ustanovení.

V §5b zákona se vzhledem ke zrušení bezpečnostních pravidel pro orgány veřejné moci využívající služby cloud computingu ruší ustanovení odst. 2 stanovující povinnost pro orgány

veřejné správy se těmito pravidly řídit. Pro orgány veřejné správy, které jsou zároveň povinnými osobami podle zákona o kybernetické bezpečnosti, ale stále platí zavádět a provádět bezpečnostní opatření a další povinnosti vyplývající ze zákona o kybernetické bezpečnosti.

Další změna zákona o informačních systémech veřejné správy reaguje na změny v povinných osobách zákona o kybernetické bezpečnosti, kdy nadále zákon o kybernetické bezpečnosti stanovuje jen jedinou povinnou osobu, a to poskytovatele regulovaných služeb. V § 6i odst. 3, který stanoví kontrolní oprávnění pro Úřad ke kontrole dodržování některých povinností vyplývajících ze zákona o informačních systémech veřejné správy, tak je odkaz na regulované systémy podle dosavadního zákona o kybernetické bezpečnosti nahrazen odkazem na regulované služby, resp. poskytování regulovaných služeb.

Vzhledem ke zrušení v zákoně o kybernetické bezpečnosti stanovené povinnosti zařadit „poptávaný cloud computing“ do bezpečnostní úrovně a rovněž zrušení zmocnění k vydání prováděcího právního předpisu pro stanovení bezpečnostních úrovní pro využívání cloud computingu orgány veřejné moci je k zachování funkčnosti systému regulace využívání cloud computingu orgány veřejné správy nutné tuto povinnost a s ní i prováděcí právní předpis přenést do zákona o informačních systémech veřejné správy, který právě těžiště regulace využívání cloud computingu orgány veřejné správy obsahuje. Do zákona o informačních systémech veřejné správy se tedy ze zákona o kybernetické bezpečnosti přenáší povinnost pro orgány veřejné moci zařadit informačních systém, jehož provoz má být zajištěn cloud computingem, do bezpečnostní úrovně podle prováděcího právního předpisu. Zmocnění k vydání tohoto prováděcího právního předpisu zůstává Úřadu, rovněž se ale přesouvá do zákona o informačních systémech veřejné správy. A konečně kontrolní pravomoc k přezkoumání správnosti zařazení informačního systému veřejné správy, k zajištění jehož provozu má být cloud computing využívání rovněž zůstává Úřadu, ale přesouvá se do zákona o informačních systémech veřejné správy.

V neposlední řadě je třeba vyškrtnout odkaz na bezpečnostní pravidla z § 6n písm. c), které stanovovalo povinnost orgánu veřejné správy využívat a poskytovateli cloud computingu poskytovat pouze cloud computing, který umožňuje orgánu veřejné správy postupovat podle bezpečnostních pravidel pro orgány veřejné moci využívající služby cloud computingu podle právního předpisu upravujícího kybernetickou bezpečnost, což vzhledem ke zrušení těchto bezpečnostních pravidel již není možné.

Poslední předkládanou změnou zákona o informačních systémech veřejné správy je napravení rozporu legislativního textu s faktickým stavem, kdy v novelizačním textu vyjmenovaná ustanovení předpokládala stanovení některých náležitostí žádostí o zápis do katalogu cloud computingu právním předpisem upravujícím kybernetickou bezpečnost, avšak tyto náležitosti jsou stanoveny prováděcím právním předpisem vydaným podle zákona o informačních systémech veřejné správy.

K § X - Změna zákona o střetu zájmů

Návrh zákona upravuje vymezení množiny veřejných funkcionářů pro potřeby zákona č. 159/2006 Sb., o střetu zájmů, ve znění zákona č. 216/2008 Sb., zákona č. 158/2009 Sb., zákona č. 350/2009 Sb., zákona č. 131/2015 Sb., zákona č. 190/2016 Sb., zákona č. 302/2016 Sb., zákona č. 14/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 180/2022 Sb., konkrétně zužuje osobní působnost zákona o střetu zájmů o vybranou skupinu zaměstnanců Národního úřadu pro kybernetickou a informační bezpečnost. Důvodem pro tuto změnu je především duplicita při poskytování údajů o nabytém majetku a dalších příjmech, darech nebo jiném prospěchu, popřípadě závazcích, které všichni zaměstnanci Úřadu podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, poskytují Národnímu bezpečnostnímu úřadu při podání žádosti o vydání osvědčení fyzické osoby, a to nejen po dobu výkonu

zaměstnání (tedy i výkonu funkce vedoucího zaměstnance Úřadu), ale také zpětně (10, 15, 20 let, popř. od věku 15 let). Zaměstnanci Úřadu následně uvedené údaje v pravidelných intervalech doplňují (9, 7 a 5 let).

Navrhovaná úprava by měla přispět, s ohledem na možná bezpečnostní rizika, k lepšímu vyvážení práva na soukromí vedoucích zaměstnanců Úřadů obecně na straně jedné a práva veřejnosti na informace na straně druhé. Tato bezpečnostní rizika plynou především z toho, že dotčení vedoucí zaměstnanci disponují citlivými informacemi (především obsahem evidencí obsahujících citlivé údaje, údaji o kybernetických bezpečnostních incidentech, informacemi o možných hrozbách) a znalostmi specifických prostředků a postupů pro získávání těchto informací. Není proto v bezpečnostním zájmu zveřejňovat osobní údaje, včetně domovních adres, těchto vedoucích zaměstnanců.

K § X – Zrušovací ustanovení

Protože tímto návrhem zákona dochází ke zrušení a nahrazení dosavadního znění zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, je nutné v souladu s čl. 10 odst. 3 větou první Legislativních pravidel vlády (*„Je-li v návrhu zákona navrženo zrušit zákon (nebo jeho část), k jehož provedení je vydán prováděcí právní předpis, navrhne se ve zrušovacích ustanoveních návrhu zákona zrušení i tohoto prováděcího předpisu.“*) v tomto ustanovení uvést nejen zrušení samotného zákona, ale také všech jeho dosavadních prováděcích právních předpisů. Tímto návrhem zákona tedy nutně dochází k nahrazení všech dosavadních zákonných i podzákonných právních předpisů upravujících komplexně kybernetickou bezpečnost v České republice a k jejich nahrazení předpisy novými.

K § X – Účinnost

Protože podstatnou část návrhu zákona tvoří transpozice směrnice NIS2, je s požadavky této směrnice úzce spojeno také stanovení účinnosti nové právní úpravy. V souladu s obsahem čl. 41 odst. 1 jsou členské státy povinny přijmout a zveřejnit opatření nezbytná pro dosažení souladu s uvedenou směrnicí do 17. října 2024, tato opatření se použijí od 18. října 2024. Z tohoto důvodu je nutné, aby byla právní úprava podle tohoto návrhu zákona a jeho prováděcích právních předpisů přijata nejpozději k 18. říjnu 2024 a zároveň ještě předtím byla zajištěná dostatečná legisvakanční lhůta, aby se povinné orgány a osoby stihly připravit na veškeré povinnosti.

K Příloze zákona

Příloha zákona obsahuje výčet trestných činů podle zákona č. 40/2009 Sb., trestní zákoník, pro účely prokázání splnění základní způsobilosti podle ustanovení o základní způsobilosti žadatele o registraci členství v Komunitě kompetencí pro kybernetickou bezpečnost upravené tímto zákonem a 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.