Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

DŮVODOVÁ ZPRÁVA

A. Obecná část

B. Zvláštní část

K § 1 (Předmět úpravy)

Návrh vyhlášky vychází ze speciální úpravy pro využívání cloud computingu orgány veřejné správy obsažené v ustanoveních § 6i a následujících zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen „ZoISVS“).

Původní definice bezpečnostní úrovně cloud computingu v § 2 písm. w) ZoISVS přímo odkazovala na právní předpis upravující kybernetickou bezpečnost, kterým je v České republice zákon o kybernetické bezpečnosti. V důsledku změny této definice v souvislosti s novelizací zákona o kybernetické bezpečnosti je třeba zajistit kontinuitu fungování mechanismu pro zařazení informačních systémů veřejné správy, pro jejichž provoz se využívají služby cloud computingu, do relevantní bezpečnostní úrovně. Návrh vyhlášky definuje proces stanovení této bezpečnostní úrovně tak, aby orgány veřejné správy mohly splnit povinnost vyplývající jim po příslušné novele z § 6l odst. 3 ZoISVS.

Znění tohoto návrhu vyhlášky vychází velmi úzce ze znění vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, tak jak nabyla účinnosti k 1. září 2021. Z důvodu zrušení dosavadní právní úpravy, která vycházela z povinnosti zakotvené v § 6 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a reflektovala specifické povinnosti orgánů veřejné moci uložené v § 4 odst. 5 zákona o kybernetické bezpečnosti dle znění zákona č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci, již není potřeba pracovat v rámci tohoto návrhu vyhlášky s pojmem „orgán veřejné moci“ (původní znění § 4 odst. 5 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, uvádělo: „*Orgány veřejné moci jsou povinny před uzavřením smlouvy s poskytovatelem služeb cloud computingu zařadit poptávaný cloud computing do bezpečnostní úrovně s ohledem na povahu dotčeného informačního nebo komunikačního systému podle prováděcího právního předpisu (...)*“), ale je možné adresovat normu „orgánům veřejné správy“ v souladu se ZoISVS.

Tato změna se pak promítá do celého obsahu navrhovaného předpisu. Návrh vyhlášky totiž odpovídá zcela znění vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, tak jak nabyla účinnosti k 1. září 2021, avšak pojem „orgán veřejné moci“ nahrazuje z výše uvedených důvodů pojmem „orgán veřejné správy“. Novelizace vyhlášky č. 315/2021 Sb., k docílení této změny nebyla možná, protože vyhláška byla jako prováděcí právní předpis zákona zrušena v okamžiku, kdy došlo ke zrušení zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů. Vzhledem k tomu, že je vyhláška prováděcím předpisem k ZoISVS, respektuje její mírně pozměněný text terminologii a definice obsažené právě v ZoISVS.

K § 2 (Vymezení pojmů)

Návrh vyhlášky vychází velmi úzce z pojmů definovaných v ZoISVS. Ústředním pojmem je informační systém veřejné správy, nebo jeho část, k zajištění jejichž provozu by měl být využit cloud computing. V případě tohoto celku nebo části se jedná o takový celek nebo část, které mohou být provozovány pomocí služeb cloud computingu ve smyslu ZoISVS – systém je uvažován v tomto případě jako celek, i když některé jeho specifické části nelze poskytovat prostřednictvím cloud computingu (zaměstnanci či koncové stanice těchto zaměstnanců, které jsou součástí systému, ale není možné je poskytovat prostřednictvím cloud computingu).

Pojmem „část informačního systému veřejné správy" se pro účely vyhlášky rozumí taková část tohoto systému, která je jednoznačně oddělitelná, zabezpečuje cílevědomou a systematickou informační činnost a je definována z hlediska funkčních kategorií, architektury, provozního modelu a bezpečnosti. Cílem odkazu obsaženého v tomto ustanovení je jen prosté využití definice „informační činnosti" tak, jak je dána § 2 písm. a) ZoISVS. Informační činností se rozumí „*získávání a poskytování informací, reprezentace informací daty, shromažďování, vyhodnocování a ukládání dat na nosiče a uchovávání, vyhledávání, úprava nebo pozměňování dat, jejich předávání, šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace dat ukládaných na nosičích*". Obsah tohoto pojmu pak prakticky odkazuje na Národní architektonický plán, který je součástí Informační koncepce České republiky podle § 5a písm. a) ZoISVS.

Definice oblasti dopadu obsahuje výčet celkem devíti oblastí uvedených ve vertikálních sloupcích tabulky obsažené v příloze č. 1 návrhu vyhlášky, v rámci kterých se může projevit dopad kybernetického bezpečnostního incidentu směřujícího vůči danému informačnímu systému veřejné správy nebo jeho části.

Definice úrovně dopadu obsahuje výčet čtyř úrovní dopadu uvedených v horizontálních řádcích tabulky obsažené v příloze č. 1 návrhu vyhlášky. Každá úroveň dopadu kvantifikuje dopad kybernetického bezpečnostního incidentu na informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing v rámci jednotlivých oblastí dopadu. U úrovní dopadů je potřeba mít na paměti, že se nejedná o bezpečnostní úrovně.

K § 3 (Bezpečnostní úrovně)

Návrh vyhlášky stanovuje, že informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, lze a je potřeba zařadit do jedné ze čtyř bezpečnostních úrovní. Bezpečnostními úrovněmi jsou nízká, střední, vysoká, a kritická úroveň. Rozdělení do čtyř úrovní vychází z řešení navrženého v rámci přílohy č. 4 Metodika stanovení požadavků na bezpečnost IS Souhrnné analytické zprávy v souladu se Strategickým rámcem Národního cloud computingu – eGovernment cloud ČR a má svůj předobraz ve Vodítku pro hodnocení dopadů vydaném Úřadem. Přestože se návrh vyhlášky ve svých jiných částech od těchto dokumentů místy odchyluje, rozdělení do čtyř bezpečnostních úrovní zůstalo zachováno. Informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, bude tedy zařazen do jedné bezpečnostní úrovně a s tímto zařazením bude dále nakládáno především pro potřeby katalogu cloud computingu, resp. v rámci dalších povinností plynoucích z § 6i a následujících ZoISVS.

K § 4 (Zařazení informačního systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing do bezpečnostní úrovně)

Proces zařazení informačního systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing je stanoven tak, že orgán veřejné správy posoudí, jakým způsobem informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing naplní jednotlivé úrovně dopadu, kterých je daný informační systém veřejné správy schopen dosáhnout v rámci každé jednotlivé oblasti dopadu. Úroveň dopadu je v rámci každé jednotlivé oblasti dopadu dána dopadem kybernetického bezpečnostního incidentu s nejhorším možným dopadem.

Orgán veřejné správy u informačního systému veřejné správy či jeho části vezme v potaz nejhorší možný dopad kybernetického bezpečnostního incidentu, který může nastat v případě, že bude narušena dostupnost (např. informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing nebude dlouhodobě fungovat), důvěrnost (např. všechny informace obsažené v informačním systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing se stanou veřejnými) či integrita (např. všechny informace v rámci informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing budou změněny, a to bez možnosti zjistit jakým způsobem, čímž ztratí svou vypovídající hodnotu), a zároveň bez ohledu na zavedená bezpečnostní opatření zhodnotí jednotlivé buňky tabulky tak, že v každém sloupci identifikuje nejhorší možný dopad. Dopady narušení důvěrnosti mohou být posuzovány například z hlediska vyzrazení dat v rámci organizace, prozrazení smluvním partnerům či prozrazení vně organizace. Narušení integrity může být posuzováno z hlediska možných dopadů neúmyslné (lidské) chyby, systémové chyby, popřípadě úmyslné modifikace informací. Velikost dopadu se s bezpečnostní úrovní zvyšuje (nejméně závažný dopad odpovídá bezpečnostní úrovni „nízká“, nejhorší dopad odpovídá bezpečnostní úrovni „kritická“). Toto hodnocení provádí orgán veřejné správy s ohledem na povahu informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing, jako celku, nebo pokud je hodnocena pouze určitá část informačního systému veřejné správy, zohlední vztah této části k bezpečnostní úrovni informačního systému veřejné správy jako celku. Tj. orgán veřejné správy musí brát ohledy na smysl toho, jaká část informačního systému veřejné správy má být zajišťována cloud computingem. Nesmí zapomínat ani na to, že i když je určitá část z tohoto systému vyčleněna, je pořád organickou součástí celku. Výsledkem této první části procesu je zjednodušeně tabulka, ve které je v každém sloupci vyznačena jedna ze čtyř úrovní dopadu.

Bezpečnostní úroveň pro využívání cloud computingu je podle návrhu vyhlášky shodná s nejvyšší úrovní dopadu, které informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing dosáhne při hodnocení jednotlivých oblastí alespoň jednou jako nejvyšší. Pokud informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing např. naplnil v osmi oblastech dopadů úroveň dopadu střední a v jedné oblasti dopadů úroveň dopadu vysokou, je jeho bezpečnostní úroveň stanovena jako vysoká.

Pokud není informačním systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing daný systém jako celek, ale je jím pouze část takového systému, tak tato nebo alespoň jedna jiná část stejného informačního systému veřejné správy musí odpovídat bezpečnostní úrovni systému jako celku. Toto pravidlo reflektuje skutečnost, že bezpečnostní úroveň informačního systému veřejné správy jako celku bude podle způsobu jeho dělení na části buďto odvislá od dopadů části celku zařazené do nejvyšší bezpečnostní úrovně, nebo bude založena na součtu dopadů jednotlivých částí celku (pokud všechny tyto části celku samostatně

dosahují nižších úrovní dopadů, než kterých dosahuje systém jako celek). Pro zajištění adekvátní úrovně zabezpečení celého systému je pak nezbytné, aby alespoň jedna jeho část byla zařazena do bezpečnostní úrovně odpovídající bezpečnostní úrovni systému jako celku. Pokud by toto pravidlo nebylo zavedeno, mohlo by v praxi docházet k účelovému dělení informačních systémů veřejné správy na části samostatně dosahující nižších bezpečnostních úrovní a k úmyslnému podhodnocování relevance a významnosti systému jako celku za účelem snížení bezpečnostních nároků na poskytovatele poptávaných cloud computingových služeb. Tímto by docházelo k obcházení zákonných povinností orgánů veřejné správy spojených s řádným zabezpečováním systémů důležitých pro chod státu.

U procesu stanovení bezpečnostní úrovně informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing počítá návrh vyhlášky s tím, že orgán veřejné správy o výše uvedených krocích provede písemný záznam (tzn. vyplnění tabulky s komentářem).

K § 5 (Účinnost)

Návrh vyhlášky počítá se standardní legisvakanční lhůtou a nabytím účinnosti 15 dní po zveřejnění.

K příloze č. 1 (Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing do bezpečnostní úrovně)

Oblasti dopadů mají svůj předobraz v řešení podle přílohy č. 4 Metodika stanovení požadavků na bezpečnost IS Souhrnné analytické zprávy v souladu se Strategickým rámcem Národního cloud computingu – eGovernment cloud ČR a ve Vodítku pro hodnocení dopadů vydaném Úřadem. S ohledem na vývoj a celkovou úpravu pro potřeby regulace cloud computingu muselo dojít k úpravám stanovených dopadů kybernetických bezpečnostních incidentů z důvodu zachování výše uvedených principů. Naopak základní rozvržení čtyř dopadových úrovní a devíti oblastí dopadů (s výjimkou odstranění původní oblasti dopadu „C. Zákonné a smluvní povinnosti“, jejíž obsah nebylo možno proporčně vydefinovat) zůstalo zachováno (některé doznaly jen jazykových úprav).

U dopadových oblastí „Veřejný pořádek“, „Řízení a provoz“, „Důvěryhodnost“ a “Zajišťování služeb“ je pro kritickou úroveň dopadu stanovena kumulativní podmínka, že musí být dotčen prvek kritické infrastruktury. Informační systémy veřejné správy nebo jejich části, které s kritickou infrastrukturou vůbec nesouvisí, nemohou kritické úrovně v uvedených dopadových oblastech nikdy dosáhnout.

A. Bezpečnost a zdraví lidí

Zraněním se rozumí porucha zdraví fyzické osoby způsobená náhle a vnější příčinou (v tomto případě působením výstupů informačního systému, ať už chybových nebo záměrně směřujících k ohrožení zdraví). Zranění je zde použito jako předstupeň, jak zhoršení zdravotního stavu (zejména např. s dlouhodobými následky), tak také přímého ohrožení života nebo ztráty života. Následkem přímého ohrožení života tedy není „jen“ způsobení zranění (ať už s krátkodobými či dlouhodobými následky), ale smrt fyzické osoby. V případě sousloví „skupina lidí“ je nutno tuto skupinu chápat jako blíže nespecifikovanou množinu, a nikoliv nutně tak, že by se mělo

jednat o skupinu předem omezenou nebo definovanou – vždy bude tato skupina odvislá od konkrétní situace.

Úroveň dopadu nízká: Nemůže vést ke zranění jednotlivce ani skupiny lidí.

Narušením důvěrnosti, integrity ani dostupnosti systému nebo jeho části nemůže dojít ke zranění ani ohrožení života jednotlivce ani skupiny lidí.

Úroveň dopadu střední: Může vést ke zranění jednotlivce nebo skupiny nejvíce 100 lidí.

Narušení důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může způsobit zranění 1–100 lidí, nemůže dojít k ohrožení života jednotlivce ani skupiny lidí. Hranice 100 lidí odpovídá určujícímu kritériu původního znění dnes již zrušené vyhlášky č. 317/2014 Sb., o významných informačních systémech.

Úroveň dopadu vysoká: Může vést ke zranění skupiny více než 100 lidí a nejvíce 2 500 lidí nebo přímému ohrožení nebo ztrátě života jednotlivce nebo skupiny nejvíce 250 lidí.

Narušení důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může způsobit zranění 101 – 2 500 lidí. Hranice 101, resp. 100 lidí odpovídá určujícímu kritériu původního znění vyhlášky o významných informačních systémech. Hranice 2 500 lidí odpovídá průřezovému kritériu nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Narušení důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může také způsobit ohrožení života 1–250 lidí. Hranice 1 člověka vychází z upraveného určujícího kritéria původního znění vyhlášky o významných informačních systémech, které začíná na 10 lidech. Bezpečnostní úroveň střední neodpovídá důležitosti ochrany před dopady na lidský život. Z tohoto důvodu byla možnost dopadu na lidské životy zařazena minimálně do bezpečnostní úrovně vysoká. Hranice 250 lidí odpovídá průřezovému kritériu nařízení vlády o kritériích pro určení prvku kritické infrastruktury.

Úroveň dopadu kritická: Může vést ke zranění více než 2 500 lidí nebo přímému ohrožení nebo ztrátě života více než 250 lidí.

Narušení důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může způsobit zranění 2 501 a více lidí. Hranice 2 501, resp. 2 500 lidí odpovídá průřezovému kritériu nařízení vlády o kritériích pro určení prvku kritické infrastruktury.

B. Ochrana osobních údajů

Návrh vyhlášky zavádí specifickou oblast dopadů, v rámci které se při hodnocení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing přihlíží k v něm obsaženým osobním údajům a jejich povaze. Ochrana osobních údajů je významným prvkem ochrany informačních systémů veřejné správy. Osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby). Subjektem údajů je identifikovaná nebo identifikovatelná fyzická osoba.

Úroveň dopadu nízká: Nemůže ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, nebo může negativně ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, který naplňuje nejvýše dvě kritéria z první skupiny kritérií podle přílohy č. 2.

K naplnění této úrovně dopadu dojde, pokud by kybernetickým bezpečnostním incidentem mohl být ovlivněn pouze informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, který nemá žádnou z vlastností uvedených v rámci první skupiny kritérií v příloze č. 2 návrhu vyhlášky, nebo má jednu takovou vlastnost, nebo má maximálně dvě z vlastností uvedených v první skupině kritérií přílohy č. 2 návrhu vyhlášky.

Význam a bližší specifikace jednotlivých vlastností (tj. kritérií) je uveden níže v rámci odůvodnění k příloze č. 2 návrhu vyhlášky.

Úroveň dopadu střední: Může negativně ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, který naplňuje tři a více kritérií z první skupiny kritérií nebo jedno kritérium z druhé skupiny kritérií podle přílohy č. 2.

K naplnění této úrovně dopadu dojde, pokud informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing má zároveň tři, čtyři, nebo všech pět vlastností, které jsou uvedeny v rámci první skupiny kritérií v příloze č. 2 návrhu vyhlášky. K naplnění této úrovně dopadu dojde také v případě, že má informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing pouze jednu z vlastností uvedených v druhé skupině kritérií v příloze č. 2 návrhu vyhlášky. Toto nastavení zabraňuje situacím, kdy by informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing splňující pouze jedno kritérium z druhé skupiny kritérií a například pouze dvě kritéria z první skupiny kritérií naplňoval nízkou úroveň dopadu. Zároveň však platí, že informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing splňující pouze jediné kritérium z druhé skupiny kritérií nebude automaticky naplňovat vysokou úroveň dopadu. Prakticky to znamená, že bude-li orgán veřejné správy provádět např. zpracování zvláštní kategorie osobních údajů, aniž by informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing splňoval jakákoli další kritéria z druhé skupiny kritérií, bude naplňovat střední úroveň dopadu. V momentě, kdy splní jakékoliv další kritérium z druhé skupiny kritérií, bude naplňovat vysokou úroveň dopadu.

Význam a bližší specifikace jednotlivých vlastností (tj. kritérií) je uveden níže v rámci odůvodnění k příloze č. 2 návrhu vyhlášky.

Úroveň dopadu vysoká: Může negativně ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, který naplňuje dvě a více kritérií z druhé skupiny kritérií podle přílohy č. 2.

K naplnění této úrovně dopadu dojde, pokud informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing má zároveň dvě nebo všechny tři vlastnosti, které jsou uvedeny v rámci druhé skupiny kritérií v příloze č. 2 návrhu vyhlášky (např. se zpracovávají zvláštní kategorie osobních údajů nebo údaje vysoce osobní povahy o subjektech údajů, přičemž je zpracováním dotčeno více než 10 000 subjektů údajů). Význam a bližší specifikace jednotlivých vlastností (tj. kritérií) je uveden níže v rámci odůvodnění k příloze č. 2 návrhu vyhlášky.

Kritéria uvedená v rámci druhé skupiny kritérií v příloze č. 2 návrhu vyhlášky navazují na kritéria stanovená v první skupině kritérií v téže příloze. Naplnění kritérií z druhé skupiny předznamenává větší riziko zásahu do práv a oprávněných zájmů dotčených subjektů údajů, proto je s jejich naplněním spojena vyšší úroveň dopadu, a tedy potřeba důkladnějšího zabezpečení (vyšší bezpečnostní úroveň).

Úroveň dopadu kritická: Může vést k omezení či narušení zpracování osobních údajů, které je nezbytné pro zajišťování obranných a bezpečnostních zájmů České republiky.

K naplnění této úrovně dopadu dojde bez ohledu na kritéria stanovená v příloze č. 2 tohoto návrhu vyhlášky, a to v případě, kdy by v rámci informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing mělo docházet ke zpracování osobních údajů významného pro zajišťování národní bezpečnosti, tedy obranných a bezpečnostních zájmů České republiky. Lze předpokládat, že většina systémů této významnosti spíše nebude provozována prostřednictvím služeb cloud computingu, nicméně kdyby mělo v konkrétním případě k této situaci dojít, počítá návrh vyhlášky se zařazením takového informačního systému veřejné správy do kritické úrovně dopadu, a tedy nejvyšší bezpečnostní úrovně.

C. Trestněprávní řízení

Návrh vyhlášky obsahuje oblast dopadů zaměřující se na možné trestněprávní důsledky narušení bezpečnosti informací v informačním systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing. Smyslem tohoto ustanovení je zaprvé považovat za větší dopad narušení systému, v rámci kterého může dojít k neoprávněnému vykonávání úkonů, a které jsou vyhrazeny orgánu veřejné správy, a zadruhé stanovit větší dopad v těch případech, kde může dojít k přímému dopadu na orgány činné v trestním řízení.

Pro potřeby stanovení trestněprávních dopadů nepracuje návrh vyhlášky zcela záměrně se všemi trestnými činy, avšak pouze s těmi, které přímo souvisí s výkonem působnosti orgánu veřejné správy a jsou pro něj specifické. Jde o trestný čin přisvojení pravomoci úřadu, trestný čin zneužití pravomoci úřední osoby a trestný čin padělání a pozměnění veřejné listiny, protože tyto trestné činy mohou mít významné dopady na orgán veřejné správy a narušení bezpečnosti informací v informačním systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing. Jiné trestné činy, které souvisí obecně s informačními systémy, jako např. neoprávněné nakládání s osobními údaji, neoprávněný přístup k počítačovému systému a nosiči informací nebo opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a další, nejsou pro svůj přesah nad rámec výkonu působnosti orgánu veřejné správy použity. Přesto, jak také vyplynulo ze vstupů Národní centrály proti organizovanému zločinu při tvorbě návrhu vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, by uvedené vymezení nemělo orgánům veřejné správy dávat falešný pocit bezpečí, že nejedná-li se o skutkové podstaty trestněprávního jednání výslovně uvedených v tomto kritériu, takže tzv. „o nic nejde“. Naopak, orgán veřejné správy si musí být vědom, že v rámci kybernetického bezpečnostního incidentu (průnik neznámé osoby do cloudového systému s tím, že uložená data budou kompromitována) je následně nezpochybnitelně možné vytvářet podmínky pro rozsáhlou trestnou činnost (což se může také mimo jiné promítnout i do dopadů v rámci ostatních posuzovaných odvětví).

Vedle toho však byl Úřad nucen omezit stanovená kritéria tak, aby byla prakticky použitelná a plnila svůj diverzifikační smysl. Národní centrálou proti organizovanému zločinu navržené

rozdělení u úrovně dopadu „nízká“ obecně na „Nemůže vytvořit podmínky pro páchání trestné činnosti“ a u úrovně dopadu „střední“ obdobně na „Může vytvořit podmínky pro páchání trestné činnosti“ byl výchozí stav se kterým Úřad při tvorbě návrhu vyhlášky začal, avšak došel k zjištění, že např. ve spojení s trestným činem § 230 „Neoprávněný přístup k počítačovému systému a nosiči informací“ by to znamenalo, že by se úroveň dopadu „nízká“ nikdy nepoužila a ztratila svůj význam. V případě úrovní dopadu „vysoká“ a „kritická“ by navržené rozšíření naopak už jen doplňovalo aktuálně široce nastavené kritérium, což by mohlo vést k interpretačním komplikacím pro orgán veřejné správy (původně „moci“).

Úroveň dopadu nízká: Nemůže vytvořit podmínky pro páchání trestných činů přisvojení pravomoci úřadu, zneužití pravomoci úřední osoby nebo padělání a pozměnění veřejné listiny ani nemůže ztížit jejich vyšetřování.

Narušením důvěrnosti, integrity ani dostupnosti systému nebo jeho části nemůže dojít k vytvoření takových podmínek, které by umožnily nebo napomohly realizaci uvedených trestných činů vymezených v trestním zákoníku. Jedná se o trestné činy, které jsou potenciálně spjaty s důležitými činnostmi orgánu veřejné správy.

Úroveň dopadu střední: Může vytvořit podmínky pro páchání trestných činů přisvojení pravomoci úřadu, zneužití pravomoci úřední osoby nebo padělání a pozměnění veřejné listiny nebo může ztížit jejich vyšetřování.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k vytvoření takových podmínek, které by umožnily nebo napomohly realizaci uvedených trestných činů vymezených v trestním zákoníku. Jedná se o trestné činy, které jsou potenciálně spjaty s důležitými činnostmi orgánu veřejné správy, tj. s tím, proč je orgán veřejné správy orgánem veřejné správy. Narušením systému může dojít k neoprávněnému vykonávání úkonů, které jsou vyhrazeny orgánu veřejné správy. Úřední osoba může (v úmyslu způsobit jinému škodu nebo jinou závažnou újmu anebo opatřit sobě nebo jinému neoprávněný prospěch) vykonat svou pravomoc způsobem odporujícím právnímu předpisu nebo svou pravomoc překročit nebo může dojít k padělání veřejné listiny nebo podstatné změně jejího obsahu.

Úroveň dopadu vysoká: Může vést k narušení vyšetřování trestné činnosti nebo soudního řízení v rámci orgánů činných v trestním řízení.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části u orgánů veřejné správy, které jsou orgány činnými v trestním řízení, může dojít k vytvoření takových podmínek, že může dojít k narušení jejich řádných činností.

Úroveň dopadu kritická: Může vést k závažnému a dlouhodobému narušení schopnosti vyšetřovat trestnou činnost nebo zpochybnění soudního řízení v rámci orgánů činných v trestní řízení.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části u orgánů veřejné správy, které jsou orgány činnými v trestním řízení, může dojít k vytvoření takových podmínek, že může dojít k závažnému a dlouhodobému narušení jejich řádných činností.

D. Veřejný pořádek

Veřejný pořádek je souhrn společenských vztahů, které vznikají, rozvíjejí se a zanikají na místech veřejných a veřejnosti přístupných. Veřejný pořádek (angl. public order; v jiném významu public policy, fr. ordre public, něm. öffentliche Ordnung) patří mezi tzv. neurčité pojmy správního práva. Ačkoli není v žádném právním předpisu definován, operuje s ním celá řada právních norem. Obvykle je jím míněn ideální stav společnosti, který se vyznačuje řádem, bezpečností a klidem – takovou definici však v právní normě použít nelze, protože jde fakticky o definici kruhem. Pojem veřejného pořádku lze v kontextu vyhlášky chápat i jako ochranu demokracie, základních principů právního státu a respektování ústavního pořádku České republiky. V případě informačních systémů veřejné správy, jejichž narušení bezpečnosti by na tyto hodnoty mohlo mít jakékoli negativní důsledky, je potřeba tyto možné dopady náležitě posoudit. S postupně se zvyšujícím rozsahem narušení veřejného pořádku se dopady zhoršují.

Úroveň dopadu nízká: Nemůže zapříčinit hromadné nepokoje nebo jinak narušit veřejný pořádek.

Narušením důvěrnosti, integrity ani dostupnosti systému nebo jeho části nemůže dojít k narušení veřejného pořádku. Veřejný pořádek je souhrn společenských vztahů, které vznikají, rozvíjejí se a zanikají na místech veřejných a veřejnosti přístupných. Jsou upraveny právními i neprávními normativními systémy a jejich zachování je významné pro zajištění klidného a bezporuchového chodu společnosti.

Úroveň dopadu střední: Může zapříčinit hromadné nepokoje nebo jinak narušit veřejný pořádek s lokálními dopady.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k narušení veřejného pořádku s lokálními dopady. Lokálními dopady se myslí negativní dopad na úzce vymezeném území (např. obce).

Úroveň dopadu vysoká: Může zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s regionálními dopady.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k narušení veřejného pořádku s regionálními dopady. Regionálními dopady se myslí negativní dopad na široce vymezeném území (např. kraje).

Úroveň dopadu kritická: Může být dotčen prvek kritické infrastruktury provozovaný orgánem veřejné správy, který informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing zařazuje do bezpečnostní úrovně, a může zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s celostátními dopady.

Může být dotčen prvek kritické infrastruktury provozovaný orgánem veřejné správy, který daný systém zařazuje do relevantní bezpečnostní úrovně, a zároveň musí platit, že narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k narušení veřejného pořádku s celostátními dopady. Celostátními dopady se myslí negativní dopad na více místech České republiky. Celostátní dopad není nezbytně spjat se skutečností, že je veřejný pořádek narušen na celém území státu, ale je naplněn i tím, že nepokoje budou soustředěny pouze na jednom místě, ovšem jejich důvod bude celorepublikový (např. demonstranti z různých částí státu budou demonstrovat v Praze).

Je velmi důležité, že všechny výše uvedené dílčí podmínky musí být splněny kumulativně, tedy současně. Naplnění pouze některé z nich nemůže vést k zařazení posuzovaného informačního systému veřejné správy do kritické úrovně dopadu.

E. Mezinárodní vztahy

Pojem mezinárodních vztahů je velmi heterogenní, avšak pro potřeby výkladu této oblasti dopadů je vhodné pohlížet na něj zejména z pohledu možného vyvolání negativního zájmu o Českou republiku z pohledu jiných subjektů mezinárodního práva a jejich reprezentantů.

Úroveň dopadu nízká: Nemůže negativně ovlivnit obraz České republiky v zahraničí.

Narušení důvěrnosti, integrity ani dostupnosti systému nebo jeho části nemůže mít takové dopady, které by se projevily v zahraničí.

Úroveň dopadu střední: Může negativně ovlivnit obraz České republiky v sousedních státech.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k vytvoření takových dopadů, které budou mít negativní vliv na obraz České republiky v sousedních státech. Může se jednat o situace velkých měst nebo krajů, které mají při výkonu své agendy vztah k sousedním státům. Stejně tak se může jednat o celorepublikové systémy, kde však dopad spíše nebude omezen na sousední státy.

Úroveň dopadu vysoká: Může negativně ovlivnit obraz České republiky ve světě.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k takovým dopadům, které budou mít negativní vliv na obraz České republiky ve světě. Může se především jednat o celorepublikové systémy, jejichž obsah je z části veřejný a případný incident způsobující jejich nedostupnost nebo narušení integrity vyvolá zájem v zahraničí.

Úroveň dopadu kritická: Může negativně ovlivnit nebo poškodit diplomatické vztahy České republiky.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k takovým dopadům, které mohou ovlivnit diplomatické vztahy České republiky. Může se především jednat o specializované systémy týkající se výhradně nebo z části mezinárodního působení České republiky, jejichž obsah je neveřejný a případný incident způsobující jejich nedostupnost nebo narušení důvěrnosti negativně ovlivní postavení České republiky ve světě.

F. Řízení a provoz

Návrh vyhlášky zohledňuje dopad také v oblasti, která reprezentuje vztah k řádnému fungování, řízení a provozu orgánu veřejné správy. Důležitým prvkem této oblasti je pojem „řádné fungování“ orgánu veřejné správy a „provádění důležitých činností“. V tomto případě je potřeba akcentovat, že za „řádné fungování“ se považuje běžný stav, ve kterém by měl za normálních okolností orgán veřejné správy své povinnosti plnit. Narušení bezpečnosti informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing tento běžný stav naruší (až na výjimečné případy) a je tedy otázkou, zda se toto narušení projeví do provádění důležitých činností. Za důležitou činnost není možné považovat

činnosti „specifické“ nebo „výjimečné“, ale naopak činnosti, které jsou pro většinu orgánů veřejné správy běžné a slouží především veřejnosti. Ve vyšších úrovních dopadů přibude k provádění důležitých činností také prvek řízení, rozvoje nebo prosazování cílů a zájmů orgánu veřejné správy. Řízením, rozvojem a prosazováním cílů a zájmů se rozumí fungování orgánu z dlouhodobější či komplexnější strategické perspektivy nejen vůči veřejnosti, ale především interně a celkově v rámci systému veřejné správy. Kritérium přesahuje schopnost plnění agendy dotčeného orgánu. Pokud by narušení bezpečnosti určitého systému nebo jeho části vedlo ke ztrátě či narušení integrity dokumentů řešících strategický rozvoj a plánování činnosti orgánu veřejné správy, nemělo by to vliv pouze na běžnou agendu tohoto orgánu, ale také na jeho řízení, rozvoj a prosazování cílů a zájmů. Systémy či jejich části s takovými potenciálními dopady proto spadají do vyšších bezpečnostních úrovní.

Hodnocení možných dopadů kybernetického bezpečnostního incidentu v rámci této dopadové oblasti nepředpokládá vyhodnocování dopadů v konkrétních časových intervalech. Tzn., jaký dopad by měl výpadek dostupnosti trvající 8 hodin, 1 den, 1 týden a tak podobně. Takto podrobné hodnocení musí být prováděno toliko při analýze rizik u relevantních povinných subjektů dle zákona o kybernetické bezpečnosti, nikoliv u všech orgánů veřejné správy. Nejsou tedy zohledňovány garantované parametry smluv o úrovni poskytovaných služeb (service-level agreement - SLA), případně další podmínky servisních a obdobných smluv. Orgán veřejné správy posuzující informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing musí zhodnotit významnost a potřebnost daného systému či jeho části zejména s ohledem na možnost svého řádného fungování, provádění důležitých činností a řízení, rozvoj a prosazování svých cílů a zájmů.

Úroveň dopadu nízká: Nemůže narušit řádné fungování nebo řízení ani části orgánu veřejné správy, nebo může narušit řádné fungování části nebo celého orgánu veřejné správy, avšak nemůže závažně omezit nebo zastavit provádění důležitých činností orgánu veřejné správy.

Narušením důvěrnosti, integrity ani dostupnosti systému nebo jeho části nemůže dojít k vytvoření takových podmínek, které by mohly narušit řádné fungování nebo řízení, byť jen části orgánu veřejné správy, nebo může dojít k narušení fungování (ale ne řízení), avšak toto narušení se neprojeví u důležitých činností orgánu veřejné správy (zákonné povinnosti bude možno provádět mimo systém při zachování jejich kvality). Takové situace budou spíše výjimečné a budou se týkat menších orgánů veřejné správy.

Úroveň dopadu střední: Může narušit řádné fungování části nebo celého orgánu veřejné správy, přičemž může závažně omezit nebo zastavit provádění důležitých činností orgánu veřejné správy.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k vytvoření takových podmínek, které by mohly narušit řádné fungování orgánu veřejné správy, případně jeho části, a tato skutečnost bude mít vliv na provádění důležitých činností (plnění zákonných povinností vůči veřejnosti nebo jiným orgánům veřejné správy bude narušeno ve své kvalitě) do té míry, že by mohlo dojít k závažnému omezení těchto činností nebo až k zastavení takových činností orgánu veřejné správy. K této situaci může běžně dojít při narušení důvěrnosti, integrity nebo dostupnosti většiny systémů.

Úroveň dopadu vysoká: Může narušit řádné fungování části nebo celého orgánu veřejné správy, přičemž může závažně omezit nebo zastavit provádění důležitých činností orgánu veřejné

správy a narušit řízení, poškodit rozvoj nebo poškodit prosazování cílů a zájmů orgánu veřejné správy.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k vytvoření takových podmínek, které by mohly narušit řádné fungování orgánu veřejné správy a tato skutečnost bude mít vliv na provádění důležitých činností (plnění zákonných povinností vůči veřejnosti nebo jiným orgánům veřejné správy bude narušeno ve své kvalitě) – viz předcházející úroveň. Zároveň musí platit, že narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části by mohlo dojít také k narušení řízení, poškození rozvoje nebo prosazování cílů a zájmů daného orgánu veřejné správy.

Úroveň dopadu kritická: Může být dotčen prvek kritické infrastruktury provozovaný orgánem veřejné správy, který informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing zařazuje do bezpečnostní úrovně, a může narušit řádné fungování části nebo celého orgánu veřejné správy, přičemž může závažně omezit nebo zastavit provádění důležitých činností orgánu veřejné správy a narušit řízení, poškodit rozvoj nebo poškodit prosazování cílů a zájmů orgánu veřejné správy.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k vytvoření takových podmínek, které by mohly narušit řádné fungování orgánu veřejné správy a tato skutečnost bude mít vliv na provádění důležitých činností (plnění zákonných povinností vůči veřejnosti nebo jiným orgánům veřejné správy bude narušeno ve své kvalitě). Zároveň musí platit, že je dotčen prvek kritické infrastruktury provozovaný orgánem veřejné správy, který daný systém zařazuje do relevantní bezpečnostní úrovně, a současně by narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části mohlo dojít také k narušení řízení, poškození rozvoje nebo prosazování cílů a zájmů daného orgánu veřejné správy.

Je velmi důležité, že všechny výše uvedené dílčí podmínky musí být splněny kumulativně, tedy současně. Naplnění pouze některé z nich nemůže vést k zařazení posuzovaného informačního systému do kritické úrovně dopadu.

G. Důvěryhodnost

Důvěryhodnost je vlastností, která by měla v rámci orgánu veřejné správy vést k jeho spolehlivému a respektovanému postavení nejen ve vztazích s ostatními organizacemi, ale i vůči široké veřejnosti. Vyznačuje se nejen tím, že není poškozeno dobré jméno orgánu veřejné správy, ale také tím, že nedochází k porušení zásad, na kterých je výkon působnosti orgánu veřejné správy postaven. V případě zásahu do důvěryhodnosti orgánu veřejné správy lze očekávat ztížení výkonu jeho zákonné působnosti jak ve smyslu kooperace s dalšími orgány veřejné správy, tak ve smyslu rozhodování o právech a povinnostech jednotlivců. Byť se jedná o poměrně flexibilní kritérium, které z povahy věci nemůže být reflektováno žádnými objektivními hodnotami, je na důkladném uvážení každého jednotlivého orgánu veřejné správy, do jaké míry může být ovlivněna jeho kredibilita v případě narušení zejména důvěrnosti a integrity jeho informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing. Jednotlivé úrovně dopadu uvedené níže jsou odstupňovány dle územního rozsahu působnosti daných orgánů. Lze totiž předpokládat, že ztráta důvěry bude v případě narušení bezpečnosti informačního systéme veřejné správy, k zajištění jehož provozu má být využíván cloud computing vždy spíše dlouhodobá.

Úroveň dopadu nízká: Nemůže negativně ovlivnit vztahy s jinými částmi orgánu veřejné správy, jinými organizacemi nebo vztahy s veřejností, nebo může vztahy s nimi negativně ovlivnit, avšak negativní následky mohou být nejvýše lokální.

Narušení důvěrnosti, integrity ani dostupnosti systému nebo jeho části nemůže mít vliv na vztahy s jinými organizacemi nebo veřejností, nebo takové dopady mít může, ale nejvýše lokálního charakteru. Lokálními dopady se myslí negativní dopad na úzce vymezeném území (např. obce).

Úroveň dopadu střední: Může negativně ovlivnit vztahy s jinými částmi orgánu veřejné správy, jinými organizacemi nebo vztahy s veřejností, avšak negativní následky mohou být nejvýše regionální.

Narušení důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může mít vliv na vztahy s jinými organizacemi nebo veřejností s regionálními dopady. Regionálními dopady se myslí negativní dopad na široce vymezeném území (např. kraje).

Úroveň dopadu vysoká: Může negativně ovlivnit vztahy s jinými částmi orgánu veřejné správy, jinými organizacemi nebo vztahy s veřejností, avšak negativní následky mohou být nejvýše celostátní nebo krátkodobě mezinárodní.

Narušení důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může mít vliv na vztahy s jinými organizacemi nebo veřejností s celostátními nebo krátkodobě mezinárodními dopady. Celostátními dopady se myslí negativní dopad na více různých místech České republiky.

Úroveň dopadu kritická: Může být dotčen prvek kritické infrastruktury provozovaný orgánem veřejné správy, který informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing zařazuje do bezpečnostní úrovně, a může negativně ovlivnit vztahy s jinými částmi orgánu veřejné správy, jinými organizacemi nebo vztahy s veřejností, negativní následky mohou být dlouhodobě mezinárodní.

Může být dotčen prvek kritické infrastruktury provozovaný orgánem veřejné správy, který daný systém zařazuje do relevantní bezpečnostní úrovně, a zároveň může mít narušení důvěrnosti, integrity nebo dostupnosti systému nebo jeho části vliv na vztahy s jinými organizacemi nebo veřejností s celostátními nebo dlouhodobě mezinárodními dopady. Opět zdůrazňujeme, že obě tato kritéria musí být naplněna současně. Nestačí naplnění pouze některého z nich.

H. Finanční model

Za finanční ztrátu je považován široký výčet škod, zejména hospodářské ztráty vzniklé přerušením poskytování služby, sankcemi nebo náklady na sanaci škod. Do výpočtu finanční ztráty je zahrnuto především následující: hospodářská ztráta z přerušení činnosti; předpokládaná sankce v případě porušení norem, předpisů, smluv, včetně pokuty za znečištění životního prostředí; náklady na sanaci škod na životním prostředí; škody na majetku nebo zdraví; případné další specifické náklady. Kritérium „Finančního modelu“ nezahrnuje ani nijak neodráží vstupní investici do daného cloud computingu, resp. informačního systému veřejné správy. Zvažovaná ztráta musí odpovídat skutečně vzniklé škodě, a to v souladu s pravidly pro vyčíslování škody/újmy (např. ve smyslu § 2894 a násl. zákona č. 89/2012 Sb.,

občanský zákoník, ve znění pozdějších předpisů, nebo např. zákona č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem, ve znění pozdějších předpisů).

V rámci stanovení kritérií pro dané úrovně dopadů se více než kde jinde projevují rozdíly dané tím, že pod regulaci v rámci návrhu vyhlášky spadají jak běžné systémy, tak specifické systémy s celorepublikovým přesahem. Z tohoto důvodu je v rámci kritérií stanoveno od střední úrovně dopadu také speciální kritérium snižující úroveň dopadu, a tím i případně bezpečnostní úroveň v případě menších orgánů veřejné správy s menším ročním rozpočtem. Referenční kritérium běžných výdajů bylo zvoleno, jelikož nejpřesněji a nejstabilněji reflektuje možné dopady finančních ztrát na běžný chod daného subjektu. Referenční kritérium příjmů nebylo vhodné, jelikož řada organizačních složek státu příjmy jako takové nemá buď vůbec, případně má příjmy v marginální hodnotě; vyčlenění prostředků ze státního rozpočtu na provoz takového subjektu nelze považovat za jeho příjem. V případě posuzování finančních ztrát oproti celkovému rozpočtu orgánu může docházet k výkyvům v situacích, kdy budou danému orgánu přiděleny prostředky pro kapitálové výdaje (například menší obci bude přidělena mimořádná dotace na rekonstrukci školky ve výši jednotek milionů korun, čímž dojde ke znásobení běžného rozpočtu této obce). Ze stejného důvodu by nebylo vhodné posuzovat možné dopady vzhledem k celkovým výdajům subjektu, kam by spadaly právě i výdaje kapitálové. Kritérium běžných výdajů tak nejlépe reflektuje, s jakými částkami subjekt běžně disponuje pro účely svého řádného provozu. Dělení výdajů na běžné a kapitálové respektuje terminologii přílohy vyhlášky Ministerstva financí č. 323/2002 Sb., o rozpočtové skladbě, ve znění pozdějších předpisů.

Úroveň dopadu nízká: Nemůže ani nepřímo vést k finančním ztrátám, nebo může vést k finančním ztrátám menším než 1 % běžných výdajů ročního rozpočtu orgánu veřejné správy.

Narušením důvěrnosti, integrity ani dostupnosti systému nebo jeho části nemůže dojít k finančním ztrátám, nebo se bude jednat o ztráty menší než 1 % běžných výdajů ročního rozpočtu. Oproti původní výši tohoto kritéria (0,05 %) došlo k navýšení daného kritéria, především kvůli orgánům veřejné správy, jejichž běžné výdaje jsou v řádu milionů korun. Jakýkoliv incident by pak vždy vedl k překročení takto nízko stanoveného kritéria a informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing by bylo potřeba hodnotit ve vyšších bezpečnostních úrovních. Z tohoto důvodu není v tomto případě nutné zavádět speciální kritérium, jako je tomu u vyšších úrovní dopadů.

Úroveň dopadu střední: Může vést k finančním ztrátám ve výši mezi 1 % a 5 % běžných výdajů ročního rozpočtu orgánu veřejné správy a tyto ztráty odpovídají částce 100 000 Kč a vyšší. V případě, že výše finanční ztráty odpovídá částce nižší než 100 000 Kč, použije se úroveň dopadu nízká.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k finančním ztrátám, které budou tvořit 1 % až 5 % běžných výdajů ročního rozpočtu. Oproti původní výši tohoto kritéria (2 %) došlo k navýšení daného kritéria. Součástí této úrovně dopadu je také speciální kritérium snižující úroveň dopadu ze střední do nízké v případě, že by finanční ztráta nižší než 100 000 Kč tvořila více než 1 % běžných výdajů ročního rozpočtu orgánu veřejné správy.

Úroveň dopadu vysoká: Může vést k finančním ztrátám ve výši přesahující 5 % a maximálně 10 % běžných výdajů ročního rozpočtu orgánu veřejné správy a tyto ztráty odpovídají částce

1 000 000 Kč a vyšší, nebo může způsobit hospodářské ztráty státu ve výši mezi 0,1 % a 0,5 % hrubého domácího produktu. V případě, že výše finanční ztráty odpovídá částce nižší než 1 000 000 Kč, použije se úroveň dopadu střední.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k finančním ztrátám, které budou tvořit více než 5 % a maximálně 10 % běžných výdajů ročního rozpočtu. Hranice 10 % běžných výdajů ročního rozpočtu zůstala v souladu se Souhrnnou analytickou zprávou zachována. Druhou částí tohoto kritéria je možné naplnění hospodářské ztráty státu ve výši mezi 0,1 % a 0,5 % hrubého domácího produktu. Hranice 0,5 % hrubého domácího produktu odpovídá průřezovému kritériu nařízení vlády o kritériích pro určení prvku kritické infrastruktury. Hranice 0,1 % byla zvolena jako počáteční hodnota z důvodu nutnosti stanovení kritéria od určité hranice, jinak by došlo k narušení předchozích kritérií. Hodnota 0,1 % hrubého domácího produktu se pohybuje ve výši přes 5 mld. Kč. Součástí této úrovně dopadu je také speciální kritérium snižující úroveň dopadu z vysoké do střední v případě, že by finanční ztráta nižší než 1 000 000 Kč tvořila více než 5 % běžných výdajů ročního rozpočtu orgánu veřejné správy.

Úroveň dopadu kritická: Může vést k finančním ztrátám přesahujícím 10 % běžných výdajů ročního rozpočtu orgánu veřejné správy a tyto ztráty odpovídají částce 10 000 000 Kč a vyšší, nebo může způsobit hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu. V případě, že výše finanční ztráty odpovídá částce nižší než 10 000 000 Kč, použije se úroveň dopadu vysoká.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k finančním ztrátám, které budou tvořit více než 10 % běžných výdajů ročního rozpočtu. Druhou částí tohoto kritéria je možné naplnění hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu. Hranice 0,5 % hrubého domácího produktu, která v tomto případě musí být překročena, odpovídá průřezovému kritériu nařízení vlády o kritériích pro určení prvku kritické infrastruktury. Součástí této úrovně dopadu je také speciální kritérium snižující úroveň dopadu z kritické do vysoké v případě, že by finanční ztráta nižší než 10 000 000 Kč tvořila více než 10 % běžných výdajů ročního rozpočtu orgánu veřejné správy.

I. Zajišťování služeb

Omezením či narušením služby se rozumí skutečnost, kdy dochází k narušení či omezení rozsahu nebo kvality, tzn. může docházet k nárůstu čekací doby, nejsou uspokojeni všichni odběratelé, může docházet k omezení dostupnosti, některé podpůrné služby nejsou dostupné, nemožnost provádění úkonů, nutno poskytovat službu náhradním způsobem apod. Omezení a narušení je předstupněm nedostupnosti, kdy daná služba není dostupná v žádném rozsahu ani kvalitě.

Úroveň dopadu nízká: Nemůže způsobit omezení, narušení či nedostupnost žádných poskytovaných služeb, nebo může způsobit omezení, narušení či nedostupnost poskytovaných služeb pro 5 000 a méně osob.

Narušením důvěrnosti, integrity ani dostupnosti systému nebo jeho části nemůže dojít k dopadům nebo může dojít k narušení kvality plnění zákonných povinnosti orgánu veřejné správy, což se projeví na kvalitě služeb poskytovaných pro maximálně 5 000 osob. Hranice 5 000 osob byla oproti původnímu znění kritéria změněna, a to na desetinu hodnoty kritéria pro významné informační systémy, aby došlo k rozložení dopadů do více úrovní.

Úroveň dopadu střední: Může způsobit omezení, narušení či nedostupnost služeb pro více než 5 000, nejvíce však 50 000 osob.

Narušení důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může narušit kvalitu plnění zákonných povinnosti orgánu veřejné správy, což se projeví na kvalitě služeb poskytovaných pro 5 001 až 50 000 osob. Hranice 50 000 osob odpovídá určujícímu kritériu znění vyhlášky o významných informačních systémech.

Úroveň dopadu vysoká: Může způsobit omezení, narušení či nedostupnost služeb pro více než 50 000 osob.

Narušení důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může narušit kvalitu plnění zákonných povinnosti orgánu veřejné správy, což se projeví na kvalitě služeb poskytovaných pro 50 001 osob a více.

Úroveň dopadu kritická: Může být dotčen prvek kritické infrastruktury provozovaný orgánem veřejné správy, který informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing zařazuje do bezpečnostní úrovně, a může dojít k rozsáhlému omezení poskytování nezbytných služeb nebo jinému závažnému zásahu do každodenního života postihujícího více než 125 000 osob.

Narušení důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může narušit kvalitu plnění zákonných povinnosti orgánu veřejné správy, což se projeví na kvalitě služeb poskytovaných pro více než 125 000 osob, přičemž musí zároveň platit, že je potenciálním kybernetickým bezpečnostním incidentem dotčen prvek kritické infrastruktury provozovaný orgánem veřejné správy, který daný systém zařazuje do relevantní bezpečnostní úrovně. Hranice 125 000 osob odpovídá průřezovému kritériu pro určení kritické informační infrastruktury podle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů. Opět zdůrazňujeme, že obě tato kritéria musí být naplněna současně. Nestačí naplnění pouze některého z nich.

Pro úplnost dodáváme, že v případě narušení dostupnosti určité služby nelze za závažný zásah či omezení poskytování nezbytných služeb považovat situace, kdy existují a jsou dostupné alternativní služby či komunikační kanály. V případě narušení důvěrnosti či integrity by se však o závažný zásah do každodenní života jednat mohlo. Na takový zásah by existence alternativní služby neměla žádný vliv.

K příloze č. 2 (Skupiny kritérií v oblasti dopadu B. Ochrana osobních údajů)

V prvé řadě je nutno uvést, že obsah přílohy č. 2 k vyhlášce odpovídá znění přílohy č. 2 k vyhlášce č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, a tato skutečnost má proto odraz také v tomto odůvodnění.

Přestože bylo původním cílem při stanovování úrovní dopadů zachovat ucelený a jednoduchý přístup, přílohu č. 2 návrhu vyhlášky bylo potřeba vytvořit z důvodu komplexnějšího posouzení možných dopadů s ohledem na oblast ochrany osobních údajů. Původně zamýšlené kritérium počtu subjektů údajů bez dalšího dostatečně nereflektovalo kontext, rozsah a rizikovost zpracování osobních údajů v rámci posuzovaných systémů a v konečném důsledku ani významnost možných dopadů v případě narušení bezpečnosti systému. Kritéria zakotvená

v příloze č. 2 návrhu vyhlášky umožňují orgánu veřejné správy lépe posoudit celkový rozsah, kontext, povahu a účely zpracování osobních údajů v informačním systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing, a tedy i přesnější a relevantnější určení úrovně dopadu a případně z toho vyplývající bezpečnostní úrovně.

Jednotlivá kritéria rámcově vycházejí z materiálu Úřadu pro ochranu osobních údajů „Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů – verze 1.0“, a to včetně rozdělení na první a druhou skupinu kritérií. Úřad pro ochranu osobních údajů vycházel při tvorbě tohoto dokumentu z materiálu Evropského sboru pro ochranu osobních údajů (EPDB) „WP248 Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679“ ze dne 14. října 2017. Do přílohy č. 2 návrhu vyhlášky však nebyla přijata úplně všechna kritéria z citovaného materiálu a některá kritéria bylo potřeba upravit, jelikož bylo nutné zohlednit specifika zpracovávání osobních údajů v rámci výkonu působnosti orgánů veřejné správy. Byla tak vyřazena kritéria, která by byla z povahy věci naplněna skoro vždy, což by mohlo vést k neproporcionálnímu nadhodnocování dopadů, a dále kritéria, která v případě systémů sloužících k výkonu působnosti orgánů veřejné správy nepřipadala v úvahu vůbec. Zůstala však zachována některá kritéria, jejichž naplnění se očekávají spíše ve výjimečných případech, případně k jejichž naplnění může dojít spíše v budoucnosti s ohledem na neustálý technologický vývoj a nově vznikající způsoby zpracování osobních údajů.

Dle Pokynů Evropského sboru pro ochranu osobních údajů WP243 a WP248 je při hodnocení celkového rozsahu zpracování osobních údajů vhodné vzít v úvahu především následující faktory: počet dotčených subjektů údajů, objem údajů a rozsah zpracovávaných údajů, délka nebo trvání činnosti zpracování osobních údajů a zeměpisný rozsah činnosti zpracování údajů nebo počet zaměstnanců správce přistupujících k těmto osobním údajům. Dle Evropského sboru pro ochranu osobních údajů naopak není optimální uvádět konkrétní hraniční hodnoty počtu subjektů pro hodnocení rozsahu zpracování.

Předmětem této vyhlášky nemá být a nemůže být zakotvení komplexní metodiky pro hodnocení rozsahu zpracování osobních údajů při důkladném zohlednění všech výše zmíněných faktorů. Nepředpokládá se, že v rámci určení bezpečnostní úrovně informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing bude každým orgánem veřejné správy zpracováno komplexní posouzení vlivu na ochranu osobních údajů (DPIA) dle čl. 35 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.

Účelem nastavení obou kategorií kritérií v příloze č. 2 návrhu vyhlášky a navazujících podmínek v jednotlivých dopadových úrovních přílohy č. 1 návrhu vyhlášky v dopadové oblasti ochrany osobních údajů je proporcionální přístup při hodnocení informačních systémů veřejné správy, k zajištění jehož provozu má být využíván cloud computing ze strany orgánů veřejné správy. Zvolená kritéria umožňují posoudit dopady na oblast ochrany osobních údajů jak ze strany těch nejmenších orgánů veřejné správy, tak ze strany orgánů s celostátní působností a zohlednit konkrétní kontext zpracování u každého orgánu. Níže jsou vysvětlena jednotlivá kritéria s ohledem na specifika výkonu působnosti orgánů veřejné správy.

První skupinu kritérií tvoří tato kritéria:

a) zpracovávají se osobní údaje umožňující bez dalšího vystupovat či jednat jménem subjektu údajů v souvislostech znamenajících poškození cti, pověsti či charakteru nebo umožňující na účet subjektu údajů odebírat služby, zboží, popřípadě vybírat peníze nebo jiné majetkové hodnoty

Údaje umožňující bez dalšího vystupovat či jednat jménem subjektu údajů v souvislostech znamenajících poškození cti, pověsti či charakteru zahrnují například přístupové údaje subjektu do určité evidence, heslo či PIN, role, pseudonym, zaznamenané přestupky nebo pokuty, účast na některých akcích apod. Údaji umožňujícími na účet subjektu údajů odebírat služby, zboží, popřípadě vybírat peníze či jiné majetkové hodnoty bude typicky jméno a příjmení subjektu, datum narození, číslo platební karty, zákaznické číslo apod.

b) zpracovávají se osobní údaje, podle kterých je subjekt údajů zařaditelný jako člen skupiny se zvláštní časově omezenou zranitelností, zejména vážně nemocní, velmi staří lidé, děti či mladiství nebo jako členové skupiny se zvláštní situačně danou zranitelností, zejména žadatelé o mezinárodní ochranu, zaměstnanci ve vztahu k zaměstnavatelům, příjemci vůči poskytovatelům nezbytných zdravotních či sociálních služeb a podobně

V tomto kritériu je rozlišována časově omezená a situačně daná zranitelnost. V případě časově omezené zranitelnosti jsou subjekty údajů zařaditelné jako členové vymezené skupiny podle toho, zda jde např. o vážně nemocné, velmi staré lidi, děti, mladistvé a podobně. Tedy osoby, které lze považovat za zranitelné s ohledem na konkrétní období života, ve kterém se daná osoba nachází nebo které daná osoba prožívá. O situačně danou zranitelnost subjektů údajů se jedná v případě, že jsou osoby zařaditelné jako členové vymezené skupiny podle toho, zda jde např. o žadatele o mezinárodní ochranu, zaměstnance ve vztahu k zaměstnavateli, o příjemce vůči poskytovatelům zdravotních či sociálních služeb, odběratele léčiv a podobně, zranitelnost dané osoby tedy vyplývá či lze dovodit z konkrétního kontextu zpracování osobních údajů.

Je na úvaze správce, aby zhodnotil konkrétní kontext a rozsah svého zpracovávání osobních údajů a dovodil tak možnou zranitelnost osob, jejichž osobní údaje jsou zpracovávány.

c) dochází ke zpracování osobních údajů, kterým je dotčeno nebo lze důvodně předpokládat, že bude dotčeno 5 000 až 10 000 subjektů údajů

Kritérium rozsahu zpracování bylo v návrhu vyhlášky zjednodušeno pouze na posouzení počtu subjektů údajů dotčených daným zpracováním. Další faktory, které je při hodnocení rozsahu zpracování třeba brát v potaz jsou zakomponovány v ostatních kritériích přílohy č. 2 návrhu vyhlášky. Konkrétní počty subjektů údajů respektují údaje obsažené v již zmiňovaném z materiálu Úřadu pro ochranu osobních údajů „Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů – verze 1.0“. Použití zjednodušeného objektivního kritéria počtu subjektů údajů je s ohledem na předmět a působnost návrhu vyhlášky dostačující, a to vzhledem k tomu, že jsou hodnocena také další kritéria obsažená v příloze č. 2. Tato část vyhlášky nemá jakkoli suplovat metodické materiály Úřadu pro ochranu osobních údajů a nemá a nemůže sloužit k ničemu jinému než k určení bezpečnostní úrovně informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing.

Část znění kritéria „nebo lze důvodně předpokládat, že bude dotčeno“ je třeba chápat v tom smyslu, že není možné vždy přihlížet pouze k aktuální situaci (respektive k aktuálnímu počtu dotčených subjektů údajů). Jestliže správce může důvodně předpokládat, že v dohledné době

může být naplněna hodnota 5 000 až 10 000 subjektů, je třeba toto kritérium považovat za naplněné. Pokud bude informačním systémem veřejné správy, k zajištění jehož provozu má být využíván cloud computing evidence obsahující údaje 4 700 subjektů údajů s každoročním průměrným přírůstkem 350 nových subjektů, lze důvodně předpokládat, že následující rok bude toto kritérium naplněno. Cloud computingové řešení zpravidla nebude pořizováno pouze na dobu jednoho roku, ale na více let, je proto nutné vzít v úvahu časový horizont, na který je dané řešení pořizováno, popřípadě při prodlužování smlouvy provést opětovné posouzení naplnění některých kritérií. V případě, kdy je pořizován zcela nový informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing (např. zcela nová evidence), kde dochází k dosud neprováděnému zpracování osobních údajů, je na orgánu veřejné správy (správci), aby provedl kvalifikovaný odhad možného počtu dotčených subjektů.

d) osobní údaje jsou veřejně přístupné neomezenému počtu orgánů nebo osob

Jde o situaci, kdy jsou zpracovávané údaje správcem zpřístupňované veřejnosti např. na základě právních předpisů. Zásah do integrity takto zveřejněných údajů subjektů může mít zásadnější dopad na práva subjektů, než např. v případě neveřejných evidencí. Počet osob, které by se mohly s pozměněnými či zcela smyšlenými osobními údaji seznámit je totiž v tomto případě mnohem větší.

e) jedná se o zpracování osobních údajů systémem s propojením na jiná zpracování prováděná stejným správcem osobních údajů nebo se jedná o osobní údaje získané od jiných správců osobních údajů

Jde o způsob zpracování, kdy dochází ke slučování či sdružování údajů získaných za různými účely, případně jsou kombinovány osobní údaje získané od jiných správců. Narušení zejména integrity takového systému by se tak vzhledem k propojení s jinými systémy mohlo projevit i v těchto navazujících systémech, což by mohlo mít závažnější celkový dopad na práva a oprávněné zájmy dotčených subjektů údajů.

Druhou skupinu kritérií tvoří tato kritéria:

a) zpracovávají se zvláštní kategorie osobních údajů nebo údaje vysoce osobní povahy, zejména finanční údaje o stavu majetku, výši finančních prostředků, dluzích nebo půjčkách či platební morálce, záznamy o historii soukromých volání subjektů údajů, údaje z elektronické pošty subjektů údajů a podobně

Zvláštní kategorie osobních údajů jsou definovány v čl. 9 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. Jde zejména o osobní údaje o rasovém nebo etnickém původu, o politických názorech, o náboženském vyznání, o filozofickém přesvědčení, o členství v odborech, o zdravotním stavu, o sexuálním životě a sexuální orientaci fyzické osoby, ale také genetické údaje či biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby.

Za údaje vysoce osobní povahy lze v určitém kontextu považovat například údaje o historii navštívených stránek konkrétní osoby, údaje o uskutečněných voláních konkrétní osoby, důvěrné údaje z elektronické pošty, finanční údaje o stavu majetku, výši finančních prostředků, dluzích nebo půjčkách, platební morálce a podobně. Tedy osobní údaje, u nichž by narušení

důvěrnosti či integrity mohlo mít velmi závažné důsledky pro práva a oprávněné zájmy subjektů údajů.

b) dochází ke zpracování osobních údajů, kterým je dotčeno nebo lze důvodně předpokládat, že bude dotčeno více než 10 000 subjektů údajů

Pro toto kritérium a jeho hodnocení platí shodně vše co bylo uvedeno výše u kritéria c) z první skupiny kritérií. V tomto případě je pouze větší rozsah dotčených subjektů údajů, tedy více než 10 000 subjektů údajů.

c) dochází k automatizovanému rozhodování, které se významně dotýká subjektu údajů.

Toto kritérium míří na zpracování osobních údajů při automatizovaném rozhodování o právech a povinnostech subjektů (srov. článek 22 GDPR), které by se jich mohlo významně dotýkat, což bude v případě rozhodování orgánů veřejné správy skoro vždy. Byť není jasné, zda v současné době některý orgán veřejné správy systém pro automatizované rozhodování používá, vyhláška v tomto kritériu reflektuje potenciální technologický vývoj v dané oblasti.