O D Ů V O D N Ě N Í

A. Obecná část

a) Vysvětlení nezbytnosti navrhované právní úpravy, odůvodnění jejích hlavních principů

Cílem zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen *„zákon o kybernetické bezpečnosti*“), je od počátku jeho účinnosti zavést do praxe soubor oprávnění a povinností s cílem zvýšit bezpečnost kybernetického prostoru a nastavit mechanismus aktivní spolupráce mezi soukromým sektorem a veřejnou správou za účelem vyšší efektivity řešení kybernetických bezpečnostních incidentů. Zákon o kybernetické bezpečnosti stanovuje ke zvýšení kybernetické bezpečnosti také speciální povinnost pro orgány veřejné moci při uzavírání smlouvy s poskytovatelem služeb cloud computingu. Tento návrh vyhlášky o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (dále jen „*návrh vyhlášky*“) je vydáván v souladu s povinností vydat prováděcí právní předpis dle § 6 písm. e) zákona o kybernetické bezpečnosti a reflektuje mimo jiné povinnost vyplývající z novelizovaného ustanovení § 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, v platném znění (dále jen *„zákon č. 261/2021“*). Novelizované ustanovení § 4 odst. 5 v zákoně o kybernetické bezpečnosti uvádí, že „*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* (...)“. Povinnost zařadit cloud computing využívaný orgánem veřejné moci pro výkon jeho působnosti do bezpečnostní úrovně však není vázána striktně pouze na situace, kdy je uzavírána zcela nová smlouvy s poskytovatelem dané služby cloud computingu. Smyslem tohoto návrhu vyhlášky je umožnit orgánu veřejné moci ohodnocení významnosti daného informačního či komunikačního systému (poptávaného cloud computingu) z hlediska nejhorších možných dopadů v případě narušení důvěrnosti, integrity či dostupnosti daného systému nebo jeho části a zařadit tak poptávaný cloud computing s ohledem na tuto významnost do příslušné bezpečnostní úrovně. Návrh vyhlášky je první částí procesu, na který následně navazuje připravovaná vyhláška o bezpečnostních pravidlech pro využívání služeb cloud computingu orgány veřejné moci (dále jen „*vyhláška o bezpečnostních pravidlech*“), která stanoví pro danou bezpečnostní úroveň konkrétní bezpečnostní pravidla. Aplikací těchto pravidel dojde k zajištění dostatečné úrovně kybernetické bezpečnosti informačních a komunikačních systémů, které jsou využívány orgány veřejné moci v případech, kdy budou provozovány prostřednictvím služeb cloud computingu.

Je nezbytné zmínit, že povinnost zařadit poptávaný cloud computing do odpovídající bezpečnostní úrovně se týká všech orgánů veřejné moci (tedy nejen těch, které jsou *a priori* povinnými orgány podle § 3 zákona o kybernetické bezpečnosti), avšak pouze u takových informačních a komunikačních systémů či jejich částí, které slouží k výkonu působnosti orgánu veřejné moci. Subjekt je orgánem veřejné moci z toho důvodu, že vykonává určitou působnost

jako orgán veřejné moci. Je tedy logické, že nebude do bezpečnostní úrovně zařazovat takový systém, prostřednictvím kterého působnost orgánu veřejné moci není vykonávána. Smyslem novelizace zákona o kybernetické bezpečnosti a vydání návrhu této vyhlášky není zařazovat do bezpečnostních úrovní veškeré informační nebo komunikační systémy subjektů, které by měly být provozovány pomocí cloud computingu, bez ohledu na účel, ke kterému jsou využívány.

Nad rámec zmocnění, které obsahuje zákon o kybernetické bezpečnosti, je návrh vyhlášky relevantní i pro novou úpravu regulace cloud computingu prostřednictvím zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (dále jen „*zákon o informačních systémech veřejné správy*"). V rámci zákona o informačních systémech veřejné správy je stejnou novelizací (zákonem č. 261/2021) zavedeno definiční ustanovení „*bezpečnostní úrovní cloud computingu (se rozumí) bezpečnostní úroveň pro využívání cloud computingu orgány veřejné moci podle právního předpisu upravujícího kybernetickou bezpečnost*", a dále také ustanovení „*Orgán veřejné správy může využívat* (...) *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"*. Zákon o informačních systémech veřejné správy tak odkazuje do zákona o kybernetické bezpečnosti, resp. tohoto návrhu vyhlášky. Lze navíc předpokládat, že mechanismus hodnocení významnosti určitého informačního či komunikačního systému nebo jeho části zakotvený v návrhu vyhlášky může být využit zákonem o informačních systémech veřejné správy pro hodnocení významnosti informačních systémů veřejné správy bez ohledu na to, zda je využívána technologie cloud computingu či nikoliv. Takový postup by samozřejmě musel být předvídán v daném zákoně, respektive reflektován v prováděcích předpisech na něj navazujících.

Navrhovaná právní úprava je z výše uvedených důvodů naprosto stěžejní pro zajištění adekvátní úrovně kybernetické bezpečnosti v souvislosti s využíváním cloudových řešení ze strany orgánů veřejné moci.

b) Zhodnocení souladu návrhu vyhlášky s ústavním pořádkem České republiky a se zákonem, k jehož provedení se navrhuje

Návrh vyhlášky je v souladu s ústavním pořádkem České republiky.

Kybernetická bezpečnost České republiky jako podmnožina bezpečnosti České republiky spadá do rozsahu působnosti ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb. Podle článku 1 uvedeného ústavního zákona je zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot základní povinností státu. Návrh vyhlášky lze považovat za jeden z prostředků plnění této povinnosti. Návrh vyhlášky zároveň reflektuje postavení kybernetické bezpečnosti jako nedílného předpokladu dalšího rozvoje digitální společnosti a ekonomiky, o nějž Česká republika jako členský stát Evropské unie usiluje.

Návrh vyhlášky je v souladu se zákonem o kybernetické bezpečnosti, k jehož provedení se vydává.

Návrh vyhlášky obsahuje pravidla pro zařazení poptávaného cloud computingu do relevantní bezpečnostní úrovně s ohledem na povahu dotčeného informačního nebo komunikačního systému, přičemž se ve všech jednotlivých ustanoveních pohybuje v rámci zákonného zmocnění a tento rámec nepřekračuje.

c) Zhodnocení souladu návrhu vyhlášky s mezinárodními smlouvami, jimiž je Česká republika vázána, judikaturou ESLP a s předpisy Evropské unie, judikaturou soudních orgánů Evropské unie nebo obecnými právními zásadami práva Evropské unie

V oblasti kybernetické bezpečnosti nebyla dosud uzavřena žádná mezinárodní smlouva.

Druhotně se kybernetické bezpečnosti dotýká Úmluva Rady Evropy o kyberkriminalitě, rovněž známá jako Budapešťská úmluva. Zákon o kybernetické bezpečnosti a jeho prováděcí předpisy včetně tohoto návrhu vyhlášky jdou rovněž v duchu nezávazných doporučení a závazků chránit důležité informační systémy formulovaných například ve zprávách Skupiny expertů OSN (UN GGE) či v opatřeních pro budování důvěry přijatých účastnickými státy Organizace pro bezpečnost a spolupráci v Evropě.

Návrh vyhlášky není v rozporu s judikaturou Evropského soudního dvora v oblasti ochrany osobních údajů.

Návrh vyhlášky je v souladu s obecnými zásadami práva Evropské unie, jako jsou např. zásada právní jistoty, proporcionality a zákaz diskriminace.

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES se návrh vyhlášky sám o sobě nikterak nedotýká.

Návrh vyhlášky nepodléhá oznamovací povinnosti podle směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti (dále jen *„směrnice 2015/1535“*). Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, přinesl do zákona o informačních systémech veřejné správy regulaci využívání služeb cloud computingu orgány veřejné správy a zavedl mj. povinnost pro orgány veřejné správy využívat pro informační systémy veřejné správy pouze služby cloud computingu zapsané jako nabídky v katalogu cloud computingu. Zákon č. 261/2021 výše zmíněnou regulaci využívání cloud computingu orgány veřejné správy rozvádí a rovněž zmocňuje Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Úřad“) k vydání nezbytných vyhlášek. Tento konkrétní návrh vyhlášky je však vydáván na základě již účinného § 6 písm. e) zákona o kybernetické bezpečnosti. Ani jeden z výše

uvedených předpisů nepodléhá oznamovací povinnosti podle dle čl. 1 odst. 1 písm. f) směrnice 2015/1535, neboť se nejedná o technické předpisy, jak vyplývá z jejich důvodových zpráv.

Směrnice 2015/1535 v definici technického předpisu podle čl. 1 odst. 1 písm. f) uvádí, že *jde o takové technické specifikace a jiné požadavky nebo předpisy pro služby, jejichž dodržování je při uvedení na trh, při poskytování služby, při usazování poskytovatele služeb nebo při používání v členském státě nebo na jeho větší části závazné*. Tyto definiční prvky v případě návrhu vyhlášky nebyly naplněny, jelikož vyhláška nepůsobí jako plošná regulace služeb cloud computingu na území České republiky. Tato vyhláška v konečném důsledku pomáhá stanovit specifické požadavky státu jako zákazníka na služby cloud computingu, a jejich následné využití v rámci specifické množiny informačních systémů orgánů veřejné moci. Tato regulace nijak nebrání uvedení služeb cloud computingu na volný trh v České republice, nepředstavuje obecnou překážku v jejich poskytování na území České republiky a nijak nebrání usazení poskytovatele služeb v České republice.

Návrh vyhlášky je v souladu se směrnicí Evropského parlamentu a Rady 2016/1148 ze dne 6. července 2016 o opatření k zajištění vysoké společné úrovně bezpečnosti sítí informačních systémů v Unii (dále jen „směrnice NIS“). Směrnice NIS v čl. 16 odst. 10 stanoví, že členské státy „*neuloží poskytovatelům digitálních služeb žádné další bezpečnostní požadavky či požadavky na hlášení incidentů"* s dovětkem *„aniž je dotčen čl. 1 odst. 6*“, ten totiž stanoví, že: „*Touto směrnicí nejsou dotčena opatření, jež členské státy přijímají s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, zejména pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti*.“ Navíc v recitálu (54) a (56) směrnice NIS přímo počítá s tím, že v případech, kdy služeb poskytovatelů digitálních služeb (dále jen „DSP“) využívají orgány veřejné správy, může stát přijmout opatření ukládající orgánům veřejné správy v rámci zakázek na služby DSP požadovat další bezpečnostní opatření nad rámec směrnice NIS, a to pouze s tím omezením, že by stát měl tyto povinnosti stanovit orgánům veřejné správy a ty by měly další bezpečnostní opatření nad rámec směrnice NIS zajistit smluvně s DSP. S ohledem na povahu katalogu cloud computingu a připravovaných vyhlášek je možné konstatovat, že stát touto vyhláškou neukládá na rámec dotčené směrnice další povinnosti, nýbrž stanoví další pravidla zejména pro orgány veřejné moci a pro ty poskytovatele, kteří jim mají zájem poskytovat služby cloud computingu zaštiťující formou katalogu.

Návrh vyhlášky není v rozporu s úpravou omezující pohyb neosobních údajů, jejichž lokalizace je upravena nařízením Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii (dále jen „*nařízení 2018/1807*“). Pro nízkou až vysokou bezpečnostní úroveň není pohyb neosobních údajů v rámci členských států Evropské unie omezen. V kritické bezpečnostní úrovni se předpokládá zpracování takových údajů, které budou s ohledem na národní bezpečnost zcela vyjmuty z nařízení 2018/1807. Podle čl. 2 odst. 3 tohoto nařízení se totiž toto nařízení nevztahuje na činnosti, které nespadají do oblasti působnosti práva EU. Tento závěr vyplývá i z čl. 4 odst. 2

Smlouvy o EU, který říká, že „*Unie ctí rovnost členských států před Smlouvami a jejich národní identitu, která spočívá v jejich základních politických a ústavních systémech, včetně místní a regionální samosprávy. Respektuje základní funkce státu, zejména ty, které souvisejí se zajištěním územní celistvosti, udržením veřejného pořádku a ochranou národní bezpečnosti. Zejména národní bezpečnost zůstává výhradní odpovědností každého členského státu*“.

Návrh vyhlášky počítá s tím, že poptávaný cloud computing spadající do úrovně dopadu „vysoká“ je systémem nebo jeho částí, u kterého by případný kybernetický bezpečnostní incident měl každopádně vliv na veřejnou bezpečnost České republiky. Pojem „veřejná bezpečnost“ ve smyslu článku 52 Smlouvy o fungování EU, jak jej vykládá Soudní dvůr, zahrnuje jak vnitřní, tak vnější bezpečnost členského státu, jakož i otázky ochrany obyvatelstva, zejména pokud jde o usnadnění vyšetřování, odhalení a stíhání trestné činnosti. Předpokládá se existence skutečné a dostatečně vážné hrozby pro některý ze základních zájmů společnosti, jako je např. ohrožení chodu veřejných institucí a základních veřejných služeb a přežití obyvatelstva, a dále rizik vážného narušení zahraničních vztahů, mírového soužití národů nebo vojenských zájmů.[1] Kritéria v jednotlivých oblastech dopadu pro úroveň dopadu „vysoká“ lze vnímat jako účelná a přiměřená, reflektující skutečné a dostatečně závažné hrozby vyplývající z možných dopadů případných kybernetických bezpečnostních incidentů. Za tyto hrozby ohrožující veřejnou bezpečnost lze obecně považovat narušení kontinuity základních veřejných služeb a narušení řádného chodu a fungování orgánů veřejné moci jakožto veřejných institucí. V případě poptávaného cloud computingu, který by spadal do úrovně dopadu „kritická“, je presumováno, že by případný kybernetický bezpečnostní incident měl dopad na národní bezpečnost České republiky, čemuž odpovídá nastavení jednotlivých kritérií v dílčích dopadových oblastech této úrovně dopadu. „Národní bezpečnost“ je podle čl. 4 odst. 2 SEU výhradní odpovědností každého členského státu. Podle relevantní judikatury SDEU „*tato odpovědnost odpovídá prvořadému zájmu chránit základní funkce státu a základní zájmy společnosti a zahrnuje prevenci a represi činností, které by mohly silně destabilizovat základní ústavní, politické, hospodářské nebo společenské uspořádání země, a zejména přímo ohrožovat společnost, obyvatelstvo nebo stát jako takový, jako jsou mimo jiné teroristické činnosti*.“[2] Vymezení bezpečnostních zájmů a opatření k zajištění své vnitřní a vnější bezpečnosti pak náleží členským státům, což Úřad v návrhu vyhlášky činí při specifikaci jednotlivých kritérií v dílčích dopadových oblastech úrovně dopadu „kritická“.

Zařazování poptávaného cloud computingu ze strany orgánů veřejné moci do odpovídající bezpečnostní úrovně dle přílohy č. 1 tohoto návrhu vyhlášky nikterak neomezuje výkon základních svobod vnitřního trhu poskytovatelů služeb cloud computingu. Cílem návrhu vyhlášky je v konečném důsledku zejména zvýšení důvěrnosti, integrity a dostupnosti dat zpracovávaných prostřednictvím služeb cloud computingu. Procesy a kroky v ní popsané jsou vždy podmíněny tím, že ve svém důsledku povede jejich realizace ke zvýšení kybernetické bezpečnosti.

[1] Recitál 19 Nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.
[2] Bod 135 rozsudku ve spojených věcech C 511/18, C 512/18 a C 520/18 La Quadrature du Net.

Návrh vyhlášky vychází ze závěrů strategických dokumentů týkajících se využívání služeb cloud computingu a regulace poskytování cloud computingu. Zpracovatelé vzali v potaz závěry týkající se strategického významu cloud computingu, digitální transformace, odstraňování překážek na vnitřním trhu či sjednocování legislativy. Návrh vyhlášky není v rozporu s úpravou omezující pohyb neosobních údajů. Pro bezpečnostní úrovně nízká až vysoká není pohyb neosobních údajů v rámci členských států Evropské unie omezen. U bezpečnostní úrovně kritická se předpokládá zpracování takových údajů, které budou s ohledem na národní bezpečnost zcela vyjmuty z působnosti nařízení 2018/1807.

d) Předpokládaný hospodářský a finanční dosah navrhované právní úpravy na veřejné rozpočty a dopad na podnikatelské prostředí České republiky

Návrh vyhlášky sám o sobě nebude mít vliv na veřejné rozpočty. Ze zařazení poptávaného cloud computingu do bezpečnostní úrovně nevznikají pro orgán veřejné moci bez dalšího žádné dodatečné výdaje. V případě, že by se orgán veřejné moci rozhodl přesunout určitý systém či jeho část do cloudového řešení, lze předpokládat určitý dopad na veřejné rozpočty, nicméně tento přímo nesouvisí se stanovením bezpečnostní úrovně daného systému nebo jeho části, nýbrž s procesem přechodu na cloudové řešení jako takovým. U méně významných systémů může být přesun do cloudu finančně výhodnější z dlouhodobého hlediska s minimálními vstupními výdaji. U důležitějších informačních systémů orgánu veřejné moci, významných informačních systémů či prvků kritické infrastruktury dle zákona o kybernetické bezpečnosti si přesun do cloudu může vyžádat významnější počáteční investice i náklady na následný provoz a údržbu, nicméně tyto by přímo nesouvisely s návrhem vyhlášky, ale s rozhodnutím subjektu o využití služeb cloud computingu.

Proces samotného posouzení poptávaného cloud computingu, respektive jeho zařazení do relevantní bezpečnostní úrovně dle tohoto návrhu vyhlášky, s sebou nese zcela marginální provozní výdaje.

Návrh vyhlášky nemá dopad na podnikatelské prostředí.

e) Předpokládané sociální dopady, včetně dopadů na rodiny a dopadů na specifické skupiny obyvatel; dopady na životní prostředí

Návrh vyhlášky je z hlediska sociálních dopadů a dopadů na specifické skupiny obyvatel neutrální.

Návrh vyhlášky je z hlediska dopadů na životní prostředí neutrální.

f) Zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Návrh vyhlášky je z hlediska zákazu diskriminace a z hlediska rovnosti mužů a žen neutrální.

g) Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů a dopadů na výkon státní statistické služby

Navrhovaná právní úprava nemá zásadní přímý vliv na oblast ochrany soukromí a osobních údajů. Jednou z dopadových oblastí návrhu vyhlášky je i oblast ochrany osobních údajů. Významnost systému je tudíž posuzována i s ohledem na počet subjektů údajů, jejichž údaje jsou zpracovávány v posuzovaném systému nebo jeho části, a citlivost těchto údajů. Návrh vyhlášky nespecifikuje žádná konkrétní opatření pro ochranu soukromí či osobních údajů, respektuje však princip maximalizace ochrany osobních údajů, když systémy obsahující větší počet osobních údajů nebo zvláštní kategorie osobních údajů obecně považuje za významnější, tedy zařazené do vyšší bezpečnostní úrovně.

Tento přístup má veskrze pozitivní nepřímé dopady na ochranu soukromí a osobních údajů.

Navrhovaná úprava nebude mít dopad na výkon státní statistické služby.

h) Zhodnocení korupčních rizik

V této oblasti nebyla shledána žádná korupční rizika. Návrh vyhlášky je jednoznačný, vychází z koncepčního právního rámce a objektivně stanovuje postup a jednotlivé možné dopady kybernetických bezpečnostních incidentů pro určení bezpečnostní úrovně poptávaného cloud computingu, přičemž jejich posuzování provádí orgán veřejné moci sám a z tohoto důvodu zde není prostor pro jakékoliv korupční jednání.

i) Zhodnocení dopadů na bezpečnost nebo obranu státu

Návrh vyhlášky má pozitivní dopady na bezpečnost a obranu státu.

Návrh vyhlášky v koexistenci s vyhláškou o bezpečnostních pravidlech a také v následné návaznosti s postupem podle zákona o informačních systémech veřejné správy přispěje k posílení zabezpečení systémů orgánů veřejné moci, čímž dojde k posílení zabezpečení českého kyberprostoru jako takového.

j) Konzultace

Návrh vyhlášky byl vytvořen Úřadem jako garantem kybernetické bezpečnosti a Ministerstvem vnitra jako garantem eGovernmentu a informačních systémů veřejné správy ve spolupráci s dalšími subjekty.

Návrh vyhlášky částečně vychází z přílohy č. 4 (Metodika stanovení požadavků na bezpečnost IS) Souhrnné analytické zprávy v souladu se Strategickým rámcem Národního cloud computingu – eGovernment cloud ČR v gesci Ministerstva vnitra a má svůj předobraz v materiálu Vodítka pro hodnocení dopadů vydaném Úřadem.

Návrh vyhlášky byl v prosinci 2020 zaslán elektronicky k připomínkám členům expertní skupiny založené v roce 2018 pro účely konzultací vznikající regulace cloud computingu. Členy této expertní skupiny jsou jak zástupci orgánů veřejné správy, tak zástupci odborné veřejnosti

a budoucích poskytovatelů cloud computingu. Stejně tak byl návrh vyhlášky zaslán komunitě manažerů kybernetické bezpečnosti. Zaslané připomínky byly na začátku ledna 2021 vypořádány, a to jak písemně, tak prostřednictvím společného jednání k vypořádání připomínek s těmi, kdo své připomínky uplatnili. Vypořádání připomínek bylo zapracováno do obsahu návrhu znění vyhlášky i jeho odůvodnění.

Stanovení kritérií dopadové oblasti „B. Osobní údaje“ bylo konzultováno s Úřadem pro ochranu osobních údajů a vychází z jeho doporučení.

Dílčí vstupy do stanovení kritérií dopadové oblasti „C. Trestněprávní řízení“ poskytla také Národní centrála proti organizovanému zločinu, Služba kriminální policie a vyšetřování. Tyto vstupy nakonec Úřad z níže uvedených důvodů nezapracoval.

B. Zvláštní část

K § 1 (Předmět úpravy)

Vydání návrhu vyhlášky vychází z povinnosti zakotvené v § 6 písm. e) zákona o kybernetické bezpečnosti vydat tento prováděcí právní předpis a reflektuje obecně povinnost orgánu veřejné moci zařadit využívaný cloud computing do adekvátní bezpečnostní úrovně, z čehož následně vyplývá povinnost aplikace odpovídajících bezpečnostních pravidel. Vedle toho návrh vyhlášky umožňuje splnění specifické povinnosti orgánů veřejné moci uložené v § 4 odst. 5 zákona o kybernetické bezpečnosti dle znění zákona č. 261/2021. Novelizované znění § 4 odst. 5 zákona o kybernetické bezpečnosti uvádí, že „*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* (...)*“*. Návrh vyhlášky definuje proces stanovení bezpečnostní úrovně tak, aby orgány veřejné moci mohly splnit výše předestřené povinnosti vyplývající ze zákona o kybernetické bezpečnosti, potažmo ze zákona o informačních systémech veřejné správy, případně z dalších relevantních předpisů. Smyslem návrhu vyhlášky je, aby se povinnost zařadit poptávaný cloud computing do odpovídající bezpečnostní úrovně týkala pouze systémů či jejich částí, které slouží k výkonu působnosti orgánu veřejné moci. Orgán veřejné moci nemusí do bezpečnostní úrovně zařazovat systém, prostřednictvím kterého není vykonávána působnost orgánu veřejné moci.

K § 2 (Vymezení pojmů)

Návrh vyhlášky používá jako jeden z hlavních pojmů „*poptávaný cloud computing*“. Poptávaný cloud computing je zastřešující pojem, který v rámci návrhu vyhlášky reprezentuje buď informační nebo komunikační systém jako celek, nebo část informačního nebo komunikačního systému (tato část byla v rámci procesů přípravy této vyhlášky označována také jako tzv. *„dekompozice systému“*). V případě tohoto celku nebo části se jedná o takový celek nebo část, které mohou být provozovány pomocí služeb cloud computingu – např. 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).

Je potřeba mít na paměti, že tato definice není stejná jako definice poptávaného cloud computing podle zákona o informačních systémech veřejné správy, a to z důvodu, že v době vzniku tohoto návrhu vyhlášky užívají zákon o kybernetické bezpečnosti a zákon o informačních systémech veřejné správy pojem *„poptávaný cloud computing“* odlišně. Zákon o kybernetické bezpečnosti pod tímto pojmem rozumí informační nebo komunikační systém jako celek nebo jeho část, které mohou být provozovány pomocí cloud computingu, zatímco zákon o informačních systémech veřejné správy pod tímto pojmem označuje naopak plnění, které poskytuje poskytovatel cloud computingu. Protože je návrh vyhlášky prováděcím právním předpisem zákona o kybernetické bezpečnosti a povinnost ji vydat je dána tímto zákonem, je nutno k definici tohoto pojmu přistoupit výlučně z pohledu zákona o kybernetické bezpečnosti. Pojem „*poptávka cloud computingu“* objevující se v novelizovaném znění zákona o informačních systémech veřejné správy pak souvisí výlučně s procesem pořizování cloud computingu prostřednictvím katalogu cloud computingu. Nejde o pojem, se kterým by pracoval zákon o kybernetické bezpečnosti, potažmo tento návrh vyhlášky. Poptávkou cloud computingu se v kontextu zákona o informačních systémech veřejné správy rozumí výzva orgánů veřejné správy poskytovatelům, aby si nechali zapsat do katalogu cloud computingu své relevantní služby cloud computingu. Tuto procesní část vztahující se výlučně k informačním systémům veřejné správy zákon o kybernetické bezpečnosti ani tento návrh vyhlášky neřeší.

Pojmem *„část informačního nebo komunikačního systému“* se 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) zákona o informačních systémech veřejné správy, ovšem bez vztahu k zákonné úpravě informačních systémů veřejné správy. 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) zákona o informačních systémech veřejné správy.

Definice oblasti dopadu obsahuje výčet celkem devíti oblastí uvedených ve vertikálních sloupcích tabulky obsažené v příloze č. 1 návrhu vyhlášky, na které může mít kybernetický bezpečnostní incident dopad.

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 poptávaný 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 poptávaný 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. Poptávaný cloud computing bude tedy zařazen do jedné bezpečnostní úrovně a s tímto zařazením bude dále nakládáno především pro potřeby aplikace bezpečnostních pravidel.

Samotný proces zařazení poptávaného cloud computingu do bezpečnostní úrovně je pro větší přehlednost vyčleněn do následujícího § 4. Souvisí s ním také příloha č. 1 návrhu vyhlášky, která obsahuje zejména tabulku „Úrovně a oblasti dopadu pro zařazení poptávaného cloud computingu do bezpečnostní úrovně“.

K § 4 (Zařazení poptávaného cloud computingu do bezpečnostní úrovně)

Proces zařazení poptávaného cloud computingu do bezpečnostní úrovně je stanoven tak, že orgán veřejné moci posoudí, jakým způsobem poptávaný cloud computing naplní jednotlivé úrovně dopadu, kterých je poptávaný cloud computing schopen dosáhnout v rámci každé jednotlivé oblasti dopadu v souladu s tabulkou obsaženou v příloze č. 1 návrhu vyhlášky. Úroveň dopadu je v rámci každé jednotlivé oblasti dopadu dána dopadem kybernetického bezpečnostního incidentu s nejhorším možným dopadem.

Jak již bylo zmíněno výše, povinnost zařadit poptávaný cloud computing do odpovídající bezpečnostní úrovně se týká pouze systémů či jejich částí, které slouží k výkonu působnosti orgánu veřejné moci. Orgán veřejné moci nemusí do bezpečnostní úrovně zařazovat systém, prostřednictvím kterého není vykonávána působnost orgánu veřejné moci.

Orgán veřejné moci u informačního nebo komunikačního systému či jeho části vezme v potaz nejhorší možný dopad kybernetického bezpečnostního incidentu, který může nastat v případě, že bude narušena dostupnost (např. poptávaný cloud computing nebude dlouhodobě fungovat), důvěrnost (např. všechny informace obsažené v poptávaném cloud computingu se stanou veřejnými) či integrita (např. všechny informace v rámci poptávaného cloud computingu budou změněny, a to bez možnosti zjistit jakým způsobem, čímž ztratí svou vypovídající hodnotu), a zároveň bez ohledu na zavedená bezpečnostní opatření[3] 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,

[3] Ta budou zavedena na základě bezpečnostních pravidel, pro jejichž identifikaci je potřeba zjistit bezpečnostní úroveň poptávaného cloud computingu.

popřípadě úmyslné modifikace informací. Velikost dopadu se s bezpečnostní úrovní zvyšuje (nejméně závažný dopad odpovídá bezpečnostní úrovni „*nízká*“, nejzávažnější dopad odpovídá bezpečnostní úrovni „*kritická*“). Toto hodnocení provádí orgán veřejné moci s ohledem na povahu informačního nebo komunikačního systému, který je poptávaným cloud computingem, jako celku, nebo v případě, že je poptávaným cloud computingem pouze určitá část informačního nebo komunikačního systému, provede toto hodnocení a zohlední vztah této části k bezpečnostní úrovni informačního nebo komunikačního systému jako celku. Tj. orgán veřejné moci musí brát ohledy na smysl toho, co poptávaný cloud computing zajišťuje. 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 orgánem veřejné moci je podle návrhu vyhlášky shodná s nejvyšší úrovní dopadu, které poptávaný cloud computing dosáhne při hodnocení jednotlivých oblastí alespoň jednou jako nejvyšší. Pokud poptávaný 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.

Proces hodnocení dopadů není potřeba provádět v případě, že je poptávaným cloud computingem informační nebo komunikační systém určený jako kritická informační infrastruktura podle zákona o kybernetické bezpečnosti jako celek. V takovém případě je tento poptávaný cloud computing automaticky zařazen do bezpečnostní úrovně kritická. Z části odlišná situace platí v případě, že je poptávaným cloud computingem informační nebo komunikační systém identifikovaný jako významný informační systém podle zákona o kybernetické bezpečnosti jako celek. V takovém případě je poptávaný cloud computing automaticky zařazen do bezpečnostní úrovně vysoká, pokud ovšem svými charakteristikami nenaplní bezpečnostní úroveň kritická. Bezpečnostní úrovně nízká nebo střední tak naplnit nikdy nemůže. Pokud by se nejednalo o informační nebo komunikační systém, který je kritickou informační infrastrukturou nebo významným informačním systémem, jako celek, ale jednalo by se o jeho část, ustanovení o automatickém zařazení do konkrétní bezpečnostní úrovně se neuplatní a taková část se posuzuje klasickým postupem.

Současně, pokud není poptávaným cloud computingem informační nebo komunikační systém jako celek, ale je jím pouze část informačního nebo komunikačního systému, tak tato nebo alespoň jedna jiná část informačního nebo komunikačního systému musí odpovídat bezpečnostní úrovni informačního nebo komunikačního systému jako celku. Toto pravidlo reflektuje skutečnost, že bezpečnostní úroveň informačního nebo komunikačního systému 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 a komunikačních systémů 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 moci spojených s řádným zabezpečováním systémů důležitých pro chod státu.

U procesu stanovení bezpečnostní úrovně poptávaného cloud computingu počítá návrh vyhlášky s tím, že orgán veřejné moci o výše uvedených krocích provede písemný záznam (tzn. vyplnění tabulky s komentářem). Dokumentaci procesu stanovení bezpečnostní úrovně by však musel orgán veřejné moci provést i bez výslovného zakotvení této povinnosti ve vyhlášce, a to především z důvodu zpětné přezkoumatelnosti jeho kroků i praktické použitelnosti. Úřad může v této věci přinést větší jistotu a metodicky sjednotit tuto praxi tím, že vzor písemného záznamu zveřejní na svých internetových stránkách.

K § 5 (Účinnost)

Návrh vyhlášky si klade za cíl, aby vyhláška nabyla účinnosti dnem následujícím po dni jejího vyhlášení. Tento postup je v souladu se zákonem o Sbírce zákonů (§ 3 odstavec 4 zákona č. 309/1999 Sb., o Sbírce zákonů a o Sbírce mezinárodních smluv, ve znění pozdějších předpisů) možný „*vyžaduje-li to naléhavý obecný zájem*“. Tento naléhavý obecný zájem je nutno spatřovat v možných legislativních problémech vyvstávajících v souvislosti s nesourodými lhůtami u novelizací, v jejichž prostředí tento návrh vyhlášky vzniká. Vydání této vyhlášky je důležitou součástí komplexního procesu regulace cloud computingu podle zákona o informačních systémech veřejné správy a její přijetí v co nejkratším možném čase tak s dalšími vznikajícími právními předpisy umožní fungování celého tohoto komplexu. Návrhem vyhlášky není a nemůže být stanoveno přechodné období pro plnění povinností (*„Orgány veřejné moci jsou povinny* (...) *zařadit poptávaný cloud computing do bezpečnostní úrovně* (...) *podle prováděcího právního předpisu a zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu* (...)*“*), které jsou uloženy zákonem bez dalšího. K jejich aplikaci navíc nedochází automaticky s účinností právního předpisu, ale až v situaci, kdy se dotčený orgán veřejné moci sám rozhodne využít služeb poskytovatele cloud computingu, tzn. poptávaný cloud computing zařadí do bezpečnostním úrovně před uzavřením smlouvy s tímto poskytovatelem. Stanovení lhůty a zavedení přechodného období do návrhu vyhlášky by nebylo způsobilé odložit plnění povinnosti uložené zákonem. Naopak by její plnění ztížilo, a to v tom smyslu, že orgány veřejné moci by i nadále neměly k dispozici účinný prováděcí právní předpis, v souladu s kterým by mohly svou zákonnou povinnost plnit.

K příloze č. 1 (Úrovně a oblasti dopadu pro zařazení poptávaného cloud computingu 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 a komunikační systémy nebo jejich části, které s kritickou infrastrukturou vůbec nesouvisí, nemohou kritické úrovně v uvedených dopadových oblastech nikdy dosáhnout. Zcela záměrně není použito kritérium kritické informační infrastruktury. Formální neurčení poptávaného cloud computingu jakožto prvku kritické informační infrastruktury by totiž nemělo orgánu veřejné moci zabránit v zařazení poptávaného cloud computingu do kritické úrovně dopadu zvláště v případech, kdy se určení prvku kritické informační infrastruktury očekává v blízké budoucnosti. Toto pojetí umožňuje subjektům kritické infrastruktury dle § 2 písm. k) zákona č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, které jsou orgány veřejné moci, zařadit svůj poptávaný cloud computing v uvedených dopadových oblastech do úrovně dopadu kritická již v momentě, kdy zhodnotí, že by použitím poptávaného cloud computingu mohla být dotčena kritická infrastruktura a zároveň by nastala podmínka uvedená v řešené dopadové oblasti.

A. Bezpečnost a zdraví lidí

Návrh vyhlášky touto oblastí dopadu navazuje na obsah dalších prováděcích právních předpisů, které při hodnocení informačního nebo komunikačního systému zohledňují dopady kybernetických bezpečnostních incidentů v oblasti ohrožení lidského zdraví a života. 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 vyhlášky 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 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 skupiny více než 2 500 lidí nebo přímému ohrožení nebo ztrátě života skupiny 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 poptávaného cloud computingu přihlíží k v něm obsaženým osobním údajům a jejich povaze. Ochrana osobních údajů je významným prvkem informačních a komunikačních systémů, se kterými nakládají orgány veřejné moci. 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 poptávaný cloud computing, nebo může negativně ovlivnit poptávaný cloud computing, který naplňuje nejvýše dvě kritéria z první skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů.

K naplnění této úrovně dopadu dojde, pokud by kybernetickým bezpečnostním incidentem mohl být ovlivněn pouze poptávaný cloud computing, který nemá žádnou z vlastností uvedených v rámci první skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů v příloze č. 1 návrhu vyhlášky, nebo má jednu takovou vlastnost, nebo má maximálně dvě z vlastností uvedených v první skupině těchto kritérií.

Význam a bližší specifikace jednotlivých vlastností (tj. kritérií) je uveden níže v rámci odůvodnění druhé části přílohy č. 1 návrhu vyhlášky nazvané „Skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů“.

Úroveň dopadu střední: Může negativně ovlivnit poptávaný cloud computing, který naplňuje tři a více kritérií z první skupiny kritérií nebo jedno kritérium z druhé skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů.

K naplnění této úrovně dopadu dojde, pokud poptávaný cloud computing má zároveň tři, čtyři, nebo všech pět vlastností, které jsou uvedeny v rámci první skupiny kritérií ve Skupinách kritérií pro oblast dopadu B. Ochrana osobních údajů v příloze č. 1 návrhu vyhlášky. K naplnění této úrovně dopadu dojde také v případě, že má poptávaný cloud computing pouze jednu z vlastností uvedených ve druhé skupině kritérií pro oblast dopadu B. Ochrana osobních údajů. Toto nastavení zabraňuje situacím, kdy by poptávaný 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 poptávaný cloud computing splňující pouze jediné kritérium z druhé skupiny kritérií nebude automaticky naplňovat vysokou úroveň dopadu. Prakticky to znamená, že bude-li orgán veřejné moci provádět např. zpracování zvláštní kategorie osobních údajů, aniž by poptávaný 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 druhé části přílohy č. 1 návrhu vyhlášky nazvané „Skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů“.

Úroveň dopadu vysoká: Může negativně ovlivnit poptávaný cloud computing, který naplňuje dvě a více kritérií z druhé skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů.

K naplnění této úrovně dopadu dojde, pokud poptávaný cloud computing má zároveň dvě nebo všechny tři vlastnosti, které jsou uvedeny v rámci druhé skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů v příloze č. 1 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 druhé části přílohy č. 1 návrhu vyhlášky nazvané „Skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů".

Kritéria uvedená v rámci druhé skupiny kritérií navazují na kritéria stanovená v první skupině kritérií v rámci Skupin kritérií pro oblast dopadu B. Ochrana osobních údajů. 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 nebo 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 ve Skupinách kritérií pro oblast dopadu B. Ochrana osobních údajů v příloze č. 1 návrhu vyhlášky, a to v případě, kdy by v rámci poptávaného cloud computingu 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 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 poptávaném cloud computingu. 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 moci (tedy tomu, proč je orgán veřejné moci orgánem veřejné moci), 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 moci a jsou pro něj specifické. Jde o trestný čin přisvojení pravomoci úřadu[4], trestný čin zneužití pravomoci úřední osoby[5] a trestný čin padělání a pozměnění veřejné listiny[6],

[4] *„Kdo neoprávněně vykonává úkony, které jsou vyhrazeny orgánu státní správy, územní samosprávy, soudu nebo jinému orgánu veřejné moci, nebo kdo vykoná úkon, který může být vykonán jen z moci úřední orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci."*

[5] *„Úřední osoba, která v úmyslu způsobit jinému škodu nebo jinou závažnou újmu anebo opatřit sobě nebo jinému neoprávněný prospěch vykonává svou pravomoc způsobem odporujícím jinému právnímu předpisu, překročí svou pravomoc, nebo nesplní povinnost vyplývající z její pravomoci"*

[6] *„Kdo padělá veřejnou listinu nebo podstatně změní její obsah v úmyslu, aby jí bylo užito jako pravé, nebo takovou listinu užije jako pravou, kdo takovou listinu opatří sobě nebo jinému nebo ji přechovává v úmyslu, aby jí bylo užito jako pravé, nebo kdo vyrobí, nabízí, prodá, zprostředkuje* nebo *jinak zpřístupní, sobě nebo jinému opatří nebo přechovává nástroj, zařízení nebo jeho součást, postup, pomůcku nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k padělání nebo pozměnění veřejné listiny"*

protože tyto trestné činy mohou mít významné dopady na orgán veřejné moci a narušení bezpečnosti informací v poptávaném cloud computingu. 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 moci použity. Přesto, jak také vyplynulo ze vstupů Národní centrály proti organizovanému zločinu při tvorbě tohoto návrhu vyhlášky, by uvedené vymezení nemělo orgánům veřejné moci 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 moci 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 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 moci.

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 moci, tj. s tím, proč je orgán veřejné moci orgánem veřejné moci. Narušením systému může dojít k neoprávněnému vykonávání úkonů, které jsou vyhrazeny orgánu veřejné moci. 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 moci, 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 moci, 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 nebo komunikačních systémů, 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 moci, který poptávaný 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 moci, 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 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 moci. Důležitým prvkem této oblasti je pojem „*řádné fungování*“ orgánu veřejné moci 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 moci své povinnosti plnit. Narušení bezpečnosti poptávaného cloud computingu 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 moci 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 moci. 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 informačního systému nebo jeho části vedlo ke ztrátě či narušení integrity dokumentů řešících strategický rozvoj a plánování činnosti orgánu veřejné moci, 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 moci. Nejsou tedy zohledňovány garantované parametry smluv o úrovni poskytovaných služeb (service-level agreement - SLA), případně další podmínky servisních a obdobných smluv. Orgán veřejné moci posuzující poptávaný 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 moci, nebo může narušit řádné fungování části nebo celého orgánu veřejné moci, avšak nemůže závažně omezit nebo zastavit provádění důležitých činností orgánu veřejné moci.

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 moci, nebo může dojít k narušení fungování (ale ne řízení), avšak toto narušení se neprojeví u důležitých činností orgánu veřejné moci (zákonné povinnosti bude možno provádět mimo systém při zachování jejich kvality). Takové situace budou spíše výjimečné a budou se týkat menších orgánů veřejné moci.

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

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k vytvoření takových podmínek, které by mohly narušit řádné fungování orgánu veřejné moci, případně jeho části, a tato skutečnost bude mít vliv na provádění důležitých činností (plnění zákonných povinností vůči veřejnosti nebo jiným orgánům veřejné moci 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 moci. 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 moci, přičemž může závažně omezit nebo zastavit provádění důležitých činností orgánu veřejné moci a narušit řízení, poškodit rozvoj nebo poškodit prosazování cílů a zájmů orgánu veřejné moci.

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k vytvoření takových podmínek, které by mohly narušit řádné fungování orgánu veřejné moci a tato skutečnost bude mít vliv na provádění důležitých činností (plnění zákonných povinností vůči veřejnosti nebo jiným orgánům veřejné moci 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 moci.

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

Narušením důvěrnosti, integrity nebo dostupnosti systému nebo jeho části může dojít k vytvoření takových podmínek, které by mohly narušit řádné fungování orgánu veřejné moci a tato skutečnost bude mít vliv na provádění důležitých činností (plnění zákonných povinností vůči veřejnosti nebo jiným orgánům veřejné moci bude narušeno ve své kvalitě). Zároveň musí platit, že je dotčen prvek kritické infrastruktury provozovaný orgánem veřejné moci, 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 moci.

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. Pokud by tak narušením bezpečnosti informací v posuzovaném systému mohlo dojít k závažnému omezení nebo zastavení provádění důležitých činností orgánu veřejné moci a narušení řízení, poškození rozvoje nebo poškození prosazování cílů a zájmů orgánu veřejné moci, ale nemohlo by dojít k dotčení prvku kritické infrastruktury provozovaného orgánem veřejné moci, který poptávaný cloud computing zařazuje do bezpečnostní úrovně, nebudou kritéria pro tuto dopadovou úroveň naplněna.

G. Důvěryhodnost

Důvěryhodnost je vlastností, která by měla v rámci orgánu veřejné moci 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 moci, ale také tím, že nedochází k porušení zásad, na kterých je výkon působnosti orgánu veřejné moci postaven. V případě zásahu do důvěryhodnosti orgánu veřejné moci lze očekávat ztížení výkonu jeho zákonné působnosti jak ve smyslu kooperace s dalšími orgány veřejné moci, 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 moci, do jaké míry může být ovlivněna jeho kredibilita v případě narušení zejména důvěrnosti a integrity jeho poptávaného cloud computingu. Jednotlivé úrovně dopadu uvedené níže jsou odstupňovány dle územního rozsahu působnosti daných orgánů. Lze totiž předpokládat, že ztráta důvěry bude v případě narušení bezpečnosti poptávaného cloud computingu vždy spíše dlouhodobá.

Úroveň dopadu nízká: Nemůže negativně ovlivnit vztahy s jinými částmi orgánu veřejné moci, 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 moci, 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 moci, 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 moci, který poptávaný cloud computing zařazuje do bezpečnostní úrovně, a může negativně ovlivnit vztahy s jinými částmi orgánu veřejné moci, jinými organizacemi nebo vztahy s veřejností, negativní následky mohou být dlouhodobě mezinárodní.

Může být dotčen prvek kritické infrastruktury provozovaný orgánem veřejné moci, 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 či komunikačního systému. 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 malých obcí, 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 moci 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 moci.

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 moci, jejichž běžné výdaje jsou v řádu milionů korun. Jakýkoliv incident by pak vždy vedl k překročení takto nízko stanoveného kritéria a poptávaný 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 moci 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 moci.

Úroveň dopadu vysoká: Může vést k finančním ztrátám ve výši přesahující 5 % a maximálně 10 % běžných výdajů ročního rozpočtu orgánu veřejné moci 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 moci.

Úroveň dopadu kritická: Může vést k finančním ztrátám přesahujícím 10 % běžných výdajů ročního rozpočtu orgánu veřejné moci 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 moci.

I. Zajišťování služeb

Omezením či narušením služby se rozumí skutečnost, kdy dochází k narušení či omezení rozsahu nebo kvality. To znamená, že 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 nebo nedostupnost žádných poskytovaných služeb, nebo může způsobit omezení, narušení nebo 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 moci, 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 nebo 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 moci, 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 nebo 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 moci, 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 moci, který poptávaný 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 moci, 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 moci, 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.

Skupiny kritérií v oblasti dopadu B. Ochrana osobních údajů

Původním cílem při stanovování úrovní dopadů bylo zachovat ucelený a jednoduchý přístup. Kvůli nezbytnosti komplexnějšího posouzení možných dopadů s ohledem na oblast ochrany osobních údajů byla vytvořena druhá část přílohy č. 1 návrhu vyhlášky nazvaná „Skupiny kritérií v oblasti dopadu B. Ochrana 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 ve druhé části přílohy č. 1 návrhu vyhlášky umožňují orgánu veřejné moci lépe posoudit celkový rozsah, kontext, povahu a účely zpracování osobních údajů v poptávaném cloud computingu, 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 druhé části přílohy č. 1 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 moci. 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 moci 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 poptávaného cloud computingu bude každým orgánem veřejné moci 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 obsažených ve druhé části přílohy č. 1 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 poptávaných cloud computingů ze strany orgánů veřejné moci. Zvolená kritéria umožňují posoudit dopady na oblast ochrany osobních údajů jak ze strany těch nejmenších obcí, 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 moci.

První skupinu kritérií tvoří tato kritéria:

a) zpracovávají se osobní údaje umožňující bez dalšího vystupovat nebo jednat jménem subjektu údajů v souvislostech znamenajících poškození cti, pověsti nebo 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 s časově omezenou nebo situačně danou zranitelností

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 obsažených ve druhé části přílohy č. 1 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 poptávaného cloud computingu.

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 poptávaným cloud computingem 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 poptávaný cloud computing (např. zcela nová evidence), kde dochází k dosud neprováděnému zpracování osobních údajů, je na orgánu veřejné moci (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, popřípadě 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 nebo 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 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 dotýkat, což bude v případě rozhodování orgánů veřejné moci skoro vždy. Byť není jasné, zda v současné

době některý orgán veřejné moci systém pro automatizované rozhodování používá, vyhláška v tomto kritériu reflektuje potenciální technologický vývoj v dané oblasti.