O D Ů V O D N Ě N Í

A. Obecná část

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

Návrh vyhlášky o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „návrh vyhlášky“) usiluje o vytvoření přehledného a jednoduchého rámce pro vstup poskytovatelů cloud computingu a zápis jimi poskytovaných služeb do nově zřizovaného katalogu služeb cloud computingu, odkud následně bude umožněno orgánům veřejné správy pořizování těchto služeb, a tím bude zajištěno zefektivnění provozu orgánů veřejné správy při výkonu jejich působnosti. Návrhem vyhlášky jsou stanoveny požadavky, na jejichž základě je rozhodováno o možnosti nabízet služby cloud computingu orgánům veřejné správy. Úprava bude mít pozitivní dopad na efektivitu ochrany kybernetického prostoru České republiky. Návrh vyhlášky musí být přijat na základě § 12 odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění zákona č. 261/2012 Sb. (dále jen „zákon o informačních systémech veřejné správy“).

Cílem § 12 odst. 2 zákona o informačních systémech veřejné správy, který bude proveden návrhem vyhlášky, bylo od počátku jeho účinnosti zavést seznam oprávnění a povinností, které v souvislosti s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy spravovaných orgány státní správy nebo orgány územních samosprávných celků celkově příznivě ovlivní jejich efektivitu, hospodárnost a v neposlední řadě i kybernetickou bezpečnost.

Zákon o informačních systémech veřejné správy se zaměřuje na komplexní ošetření problematiky životního cyklu informačních systémů napříč státní správou. V tomto ohledu se návrh vyhlášky zaměřuje pouze na konkrétní část předpisu, kterou provádí. Cílem této části předpisu, a tedy i návrhu vyhlášky, je vytvořit jednotné požadavky pro budoucí poskytovatele cloud computingu, kteří je plánují nabízet orgánům veřejné správy. Seznam požadavků poslouží jako první posouzení schopnosti budoucích poskytovatelů cloud computingu nabízet orgánům veřejné správy takové služby cloud computingu, které budou naplňovat základní úroveň důvěrnosti, integrity a dostupnosti.

Zákon o informačních systémech veřejné správy stanovuje proces, na jehož základě je umožněno poskytovatelům cloud computingu tyto služby nabízet orgánům veřejné správy. Součástí tohoto procesu je i vstup poskytovatelů cloud computingu do zákonem zřízeného katalogu, který bude nabídky všech poskytovatelů cloud computingu shromažďovat. Následně si z něj budou orgány veřejné správy podle svých potřeb, na základě vypsání veřejné zakázky, moci zvolit takovou službu cloud computingu, která bude nejvíce vyhovovat jejich specifické potřebě. V celém procesu je klíčovým okamžikem, který má zásadní dopad na kybernetickou

bezpečnost systému orgánů veřejné správy, vstup potenciálních poskytovatelů cloud computingu s nabídkami jednotlivých služeb do katalogu, který je bude shromažďovat. Návrh vyhlášky je předpisem, který tento klíčový krok zabezpečuje z pohledu stanovení a prověření základních požadavků na poskytovatele cloud computingu. Tyto požadavky osvědčují schopnost poskytovatele cloud computingu zajistit alespoň minimální bezpečnostní požadavky a poskytnout tak orgánům veřejné správy záruky k zajištění kybernetické bezpečnosti v rámci využívané služby cloud computingu.

Cílem návrhu vyhlášky je zakotvit v právním řádu České republiky legislativní možnost pro vytvoření jednotného a systematického bezpečnostního základu v podobě seznamu požadavků, který umožní bezpečnostní prověření poskytovatelů cloud computingu ještě před tím, než dojde k samotnému předání potenciálně citlivých dat a informací orgány veřejné správy do správy poskytovatele cloud computingu. Nedostatečné zajištění kybernetické bezpečnosti v této oblasti může mít fatální dopady na fungování orgánů veřejné správy, což je z pozice České republiky nepřijatelné.

Návrh vyhlášky obsahuje seznam požadavků na základní úroveň důvěrnosti, integrity a dostupnosti. Počet poskytovatelů cloud computingu, kterých se úprava požadavků týká, je značný. Proto byly i s ohledem na velký počet systémů orgánů veřejné správy zvoleny jasně definované a všeobecné požadavky, které se odráží od využívané praxe a mezinárodních standardů.

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 čl. 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 rozvoje digitální společnosti a ekonomiky, o nějž Česká republika jako členský stát Evropské unie usiluje.

Návrh vyhlášky je v souladu s § 12 odst. 2 zákona o informačních systémech veřejné správy.

Návrh vyhlášky stanoví požadavky, jejichž naplnění umožní poskytovatelům cloud computingu nabízet tyto služby orgánům veřejné správy, 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 informačních systémech veřejné správy 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 Soudního dvora Evropské unie 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.

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, přinesl do zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, regulaci využívání služeb cloud computingu orgány veřejné správy a zavedl mj. jiné povinnost pro orgány veřejné správy využívat pro informační systémy veřejné správy pouze služby cloud computingu zapsané jako nabídky v katalogu cloud computingu. Ustanovení § 12 odst. 2 zákona o informačních systémech veřejné správy výše zmíněnou regulaci využívání služeb cloud computingu orgány veřejné správy rozvádí a rovněž zmocňuje Národní úřad pro kybernetickou a informační bezpečnost k vydání této vyhlášky. 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 Evropského parlamentu a Rady 2015/1535 v definici technického předpisu podle čl. 1 odst. 1 písm. f) uvádí: „*…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 návrh vyhlášky nepůsobí jako plošná regulace služeb cloud computingu na území České republiky. Návrh vyhlášky stanoví specifické požadavky státu jako zákazníka na služby cloud computingu, a jejich následné využití v rámci specifické množiny informačních systémů orgánů veřejné správy. Jedná se de facto o podmínky pro vstup do výběrového řízení při zadávání veřejných zakázek pro informační systémy orgánů veřejné správy. Tato regulace nijak nebrání uvedení služeb cloud computingu na volný trh v České republice, nepředstavuje obecnou překážku v jejich poskytování na území ČR a nijak nebrání usazení poskytovatele služeb v ČR.

Z výše uvedeného důvodů proto není dotčeno ani nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro

kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“). V případě dotvoření Evropského schématu certifikace kybernetické bezpečnosti služeb cloud computingu (dále jen „EUCS“)[1] lze uvažovat o využití takového schématu komplementárně k návrhu vyhlášky. Pro případ odlišného výkladu aktu o kybernetické bezpečnosti, resp. připravované vyhlášky se uvádí, že návrh vyhlášky koordinuje požadavky s návrhem EUCS, zohledňuje také předpokládaný vývoj v oblasti unijních předpisů. Zároveň požadavky pro bezpečnostní úroveň vysoká a kritická jsou zcela vyloučeny z případné působnosti aktu o kybernetické bezpečnosti, jelikož souvisí mj. s veřejnou a národní bezpečností, která je vyňata z působnosti aktu o kybernetické bezpečnosti.

Pojem „veřejná bezpečnost“ ve smyslu čl. 52 Smlouvy o fungování Evropské unie, jak jej vykládá Soudní dvůr Evropské unie, 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.[2] Protože právním základem aktu o kybernetické bezpečnosti je čl. 114 Smlouvy o fungování EU, tj. sbližování pravidel týkajících se fungování vnitřního trhu, je nutno možnost odchýlení se od tohoto nařízení vnímat právě v kontextu vnitřního trhu a související judikatury Soudního dvora. Za tyto hrozby ohrožující veřejnou bezpečnost jde obecně považovat narušení kontinuity základních veřejných služeb a narušení řádného chodu a fungování orgánů veřejné moci jakožto veřejných institucí.

„Národní bezpečnost“ je podle čl. 4 odst. 2 Smlouvy o fungování Evropské unie výhradní odpovědností každého členského státu. Podle relevantní judikatury Soudního dvora Evropské unie „*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.*“[3] Vymezení bezpečnostních zájmů a opatření k zajištění své vnitřní a vnější bezpečnosti pak náleží členským státům, což Národní úřad pro kybernetickou a informační bezpečnost v návrhu vyhlášky činí při specifikaci jednotlivých kritérií v dílčích dopadových oblastech úrovně dopadu „kritická“.

Návrh vyhlášky je v souladu se směrnicí Evropského parlamentu a Rady 2016/1148 ze dne 6. července 2016 o opatřeních 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,

[1] Návrh zveřejněn 22. 12. 2020. Dostupné z: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/

[2] 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

[3] Bod 135 rozsudku ve spojených věcech C 511/18, C 512/18 a C 520/18 La Quadrature du Net.

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 *digital service provider* (dále jen „DSP“) využívají orgány veřejné správy, může stát přijmout opatření ukládající orgánům veřejné správy v rámci zakázek na služby DSP povinnost požadovat další bezpečnostní opatření nad rámec směrnice NIS. Orgány veřejné správy si následně zajistí další bezpečnostní opatření nad rámec směrnice NIS smluvně s DSP. S ohledem na povahu katalogu cloud computingu a připravovaných vyhlášek je možné konstatovat, že stát návrhem vyhlášky neukládá nad rámec dotčené směrnice NIS další povinnosti, nýbrž stanoví další pravidla zejména pro orgány veřejné správy, které mají zájem o využívání služeb cloud computingu zajištěných formou katalogu cloud computingu.

Návrh vyhlášky není v rozporu s úpravou omezující pohyb neosobních údajů, jejichž lokalizace je upravena nařízením Evropského parlamentu a Rady 2018/1807, o rámci pro volný tok neosobních údajů v Evropské unii. Pro nízkou až vysokou bezpečností 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 Evropského parlamentu a Rady 2018/1807. Podle čl. 2 odst. 3 nařízení Evropského parlamentu a Rady 2018/1807 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*“.

Cílem návrhu vyhlášky je zejména zvýšení důvěrnosti, integrity a dostupnosti dat zpracovávaných s pomocí služeb cloud computingu. Procesy a kroky v ní popsané jsou vždy podmíněny tím, že jejich realizace povede ke zvýšení kybernetické bezpečnosti. 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 neztratí na významu, neboť návrh vyhlášky obsahuje nástroje (například šifrování), které musí zůstat v platnosti i během zálohování. Ke ztrátě důvěrnosti při dodržení podmínek stanovených v návrhu vyhlášky, a s ohledem na aplikaci relevantních zákonných opatření, nedojde.

Návrh vyhlášky vychází ze závěrů strategických dokumentů týkajících se využívání služeb cloud computingu a regulování poskytování služeb cloud computingu. Zpracovatelé návrhu vyhlášky vzali v potaz závěry týkající se strategického významu cloud computingu, digitální transformace, odstraňování překážek na vnitřním trhu či sjednocování legislativy. Návrh vyhlášky se vypořádává s globálním charakterem služeb cloud computingu a implementuje

požadavky na ochranu dat před potenciálními požadavky cizích právních řádů na jejich zpřístupnění v souladu s Evropskou strategií pro data[4] i evropskými bezpečnostními standardy dle *Sdělení Komise k uvolnění potenciálu cloud computingu v Evropě či Evropské cloudové iniciativy – Budování konkurenceschopné ekonomiky v Evropě* založené na datech a znalostní ekonomice.[5] Návrh vyhlášky svým akcentem na bezpečnost a lokalizaci dat navíc vytváří příležitosti pro evropské poskytovatele cloud computingu, kteří mohou přizpůsobit své služby novým bezpečnostním požadavkům a zvýšit tak vlastní konkurenceschopnost v souladu s cíli Komise dle dokumentu *Digitální kompas 2030: evropská cesta pro digitální desetiletí*.[6] V tomto duchu návrh vyhlášky vychází i z dalších již využívaných technických předpisů a skutečného stavu nabízených služeb cloud computingu.

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

Návrh vyhlášky nemá vliv na veřejné rozpočty.

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

Navrhovaná právní úprava nemá přímý vliv na oblast ochrany soukromí a osobních údajů. S ohledem na předpokládanou možnost orgánů veřejné správy vkládat osobní údaje do systémů provozovaných za pomoci služeb cloud computingu byly dopady návrhu vyhlášky konzultovány s Úřadem pro ochranu osobních údajů tak, aby byla v maximální možné míře šetřena práva subjektů údajů a zajištěn soulad s právními předpisy dopadajícími na tuto oblast, zejména pak byl brán v potaz soulad s Nařízením Evropského parlamentu a Rady (EU)

[4] A European strategy for data, ze dne 19. 2. 2020. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN

[5] Unleashing the Potential of Cloud Computing in Europe, ze dne 27. 9. 2012. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012DC0529&from=en; European Cloud Initiative - Building a competitive data and knowledge economy in Europe, ze dne 19. 6. 2016, Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0178&from=en

[6] 2030 Digital Compass: the European way for the Digital Decade, ze dne 9. 3. 2021. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118&from=cs

2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, GDPR). Návrh vyhlášky však nijak nezbavuje ani neomezuje odpovědnost správců osobních údajů za vyhodnocení dopadů na ochranu osobních údajů při využití služeb cloud computingu.

V návrhu vyhlášky nelze stanovit, jaká data budou pomocí služeb cloud computingu zpracovávána. Vzhledem k tomu a k obsahu návrhu vyhlášky, která sama v příloze obsahuje požadavky na zajištění určité úrovně důvěrnosti, integrity a dostupnosti pro využívání služeb cloud computingu, není potřeba podrobněji analyzovat vliv na ochranu osobních údajů v odůvodnění. Návrh vyhlášky však neodstraňuje ani neomezuje odpovědnost správců osobních údajů za vyhodnocení dopadů na ochranu osobních údajů a dodržování GDPR při využití služeb cloud computingu. Povinnosti správce osobních údajů mohou být doplněny na základě rozhodnutí schválených úřady Evropské unie k zajištění ochrany osobních údajů.

h) Zhodnocení korupčních rizik

V této oblasti nebyla shledána žádná nová vazba ani nová rizika. Návrh vyhlášky je jednoznačný a vychází z koncepčního právního rámce. Návrh vyhlášky nastavuje jasné požadavky, přičemž chybí prostor pro korupční jednání.

i) Zhodnocení dopadů na bezpečnost nebo obranu státu

Návrh vyhlášky má pozitivní dopady na bezpečnost a obranu státu. Využívání služeb cloud computingu bude mít pozitivní dopady na bezpečnost a obranu státu zejména proto, že cílí na bezpečné využívání služeb cloud computingu. Lze očekávat, že postup podle návrhu vyhlášky přispěje k posílení zabezpečení systémů orgánů veřejné správy, čímž dojde k posílení zabezpečení českého kybernetického prostoru jako takového. Využívání služeb cloud computingu může mít s ohledem na jejich povahu pozitivní dopad na bezpečnost a obranu státu, zejména díky schopnosti centralizovat a vyhodnocovat informace o bezpečnostních hrozbách a zranitelnostech z celého světa, a na základě toho přijímat potřebné kroky dříve a ve vyšší kvalitě. Návrh vyhlášky, a tedy i regulace služeb cloud computingu, je potom zcela zásadním krokem, neboť jde v konečném důsledku o předávání dat do správy soukromoprávním a často i zahraničním poskytovatelům těchto služeb. Současně s tím je nutné mít na paměti i zvýšené riziko přístupu cizozemských orgánů k datům vloženým do těch služeb cloud computingu, které budou provozovány na území třetích států. Je nezbytné, aby tito poskytovatelé byli prověřeni jako dostatečně důvěryhodní.

j) Konzultace

Návrh vyhlášky byl tvořen Národním úřadem pro kybernetickou a informační bezpečnost jako garantem kybernetické bezpečnosti a Ministerstvem vnitra jako garantem eGovernmentu a informačních systémů veřejné správy, ve spolupráci s dalšími subjekty.

Návrh vyhlášky byl od roku 2018 průběžně konzultován v expertní skupině založené pro tento účel, jejímiž členy byli jak zástupci orgánů veřejné správy, tak zástupci odborné veřejnosti a budoucích poskytovatelů cloud computingu, kteří budou přímými adresáty návrhu

vyhlášky. Na jaře 2020 a následně v průběhu třetího a čtvrtého kvartálu roku 2020 došlo k mnoha jednáním, jejichž výsledkem je návrh vyhlášky. Na finální podobě materiálů se podílela též komunita manažerů kybernetické bezpečnosti.

Dílčí otázky související s oběhem dat a ochranou osobních údajů byly konzultovány s Úřadem pro ochranu osobních údajů.

B) Zvláštní část

K § 1

Ustanovení § 1 definuje, jaké oblasti jsou návrhem vyhlášky regulovány.

K § 2

V § 2 jsou definovány základní pojmy, se kterými návrh vyhlášky pracuje. Pojem poskytovatel vychází ze zákona o informačních systémech veřejné správy. Dle zákona o informačních systémech veřejné správy jím může být jak prodejce, tak i ten, kdo službu fakticky poskytuje.

Vzhledem k významu provozních údajů, jenž byl v minulosti dovozen soudní praxí,[7] byl v návrhu vyhlášky zaveden nový pojem specifických provozních údajů. Ten označuje nejcitlivější provozní údaje, které jsou velice často osobními údaji, a také ty neosobní údaje, které jsou způsobilé identifikovat právnické osoby a další uživatele. Jednat se může například o provozní údaje s vysokou informační hodnotou (jaký uživatel, kdy a jak často přistupuje do informačních systémů/databází a do kterých). Na základě zavedení kategorie specifických provozních údajů může návrh vyhlášky takovým údajům, které se svým významem blíží osobním údajům (a často jimi i jsou), poskytnout adekvátní ochranu a reflektovat tak požadavky vyplývající z práva na informační sebeurčení.

Návrh vyhlášky dále pracuje s pojmem zákaznická data. Ta jsou spolu se specifickými provozními údaji částí informací orgánu veřejné správy ve smyslu zákona o informačních systémech veřejné správy [např. § 6k odst. 2 písm. c) bod 3, § 6m odst. 1 písm. a) zákona o informačních systémech veřejné správy]. Pokud jsou některá zákaznická data obsažena v provozních údajích, neztrácejí tím povahu zákaznických dat. Stále se bude jednat o zákaznická data.

Uživatelem se rozumí jak fyzické osoby, tak i stroje vystupující jako uživatelé.

Pro potřeby GDPR bude zákazník zpravidla správcem osobních údajů (čl. 4 nařízení GDPR) a poskytovatel bude zpracovatelem (čl. 4 nařízení GDPR).

[7] Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10, č. N 52/60 SbNU 625, nebo také spojené věci C-293/12 a C-594/12 Digital Rights Ireland a Seitlinger a další, ECLI:EU:C:2014:238 a spojené věci C-203/15 a C-698/15 Tele2 Sverige AB a Secretary of State for the Home Department, ECLI:EU:C:2016:970.

K § 3

Ustanovení § 3 stanovuje, že požadavky na způsobilost zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6m odst. 1 písm. a) zákona o informačních systémech veřejné správy jsou upraveny v příloze č. 1 návrhu vyhlášky.

K § 4

Ustanovení § 4 stanovuje, že požadavky na dosažení alespoň základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem podle § 6n zákona o informačních systémech veřejné správy jsou upraveny v příloze č. 2 návrhu vyhlášky.

K § 5

Ustanovení § 5 stanovuje, že seznam certifikací a auditů pro oblast ochrany důvěrnosti, integrity a dostupnosti informací podle § 6q odst. 5 písm. c), § 6t odst. 6 písm. b) a § 6t odst. 7 písm. c) zákona o informačních systémech veřejné správy, doklady o jejich splnění a intervaly pro předkládání těchto dokladů podle § 6y odst. 2 zákona o informačních systémech veřejné správy je upraven v příloze č. 3 návrhu vyhlášky.

K § 6

Ustanovení § 6 stanovuje, že požadavky na strukturu a náležitosti zprávy o provedení penetračního testu podle § 6t odst. 6 písm. d) a § 6t odst. 7 písm. e) zákona o informačních systémech veřejné správy a intervaly pro její předkládání jsou stanoveny v příloze č. 4 návrhu vyhlášky.

K § 7

Ustanovení § 7 stanovuje náležitosti auditní zprávy osvědčující existenci plánu zajištění kontinuity provozu nabízených služeb cloud computingu a plánu na obnovu poskytování nabízených služeb cloud computingu po havárii podle § 6t odst. 6 písm. e) a § 6t odst. 7 písm. f) zákona o informačních systémech veřejné správy.

K § 8

Ustanovení § 8 stanovuje, že požadavky na strukturu a náležitosti dokladu o zhodnocení zdrojů rizik podle § 6t odst. 6 písm. f) a § 6t odst. 7 písm. g) zákona o informačních systémech veřejné správy jsou stanoveny v příloze č. 5 návrhu vyhlášky.

K § 9

Ustanovení § 9 stanovuje požadavky na strukturu a náležitosti podkladů k ověření splnění požadavku na zajištění důvěrnosti, integrity a dostupnosti informací podle § 6t odst. 6 písm. g) a § 6t odst. 7 písm. h) zákona o informačních systémech veřejné správy.

Podklady k ověření splnění požadavku na zajištění důvěrnosti, integrity a dostupnosti informací budou z povahy věci spíše rozsáhlé, a proto mají zákon i návrh vyhlášky za cíl stanovit požadavky na tyto poklady tak, aby bylo možno je – v relevantní době – posoudit. Proto se v odstavci 1 návrhu vyhlášky stanoví, že struktura podkladů musí být přehledná a srozumitelná, a dále se definuje, jak má být této přehlednosti a srozumitelnosti dosaženo.

Odstavce 2 až 6 stanoví požadavky na náležitosti podkladů.

Podklady je nutné předkládat elektronicky, ve strojově čitelném formátu zaručujícím neměnnost obsahu jednotlivých dokumentů. Splnění každého požadavku pro každou službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, je ve formuláři nutno popsat jasně a srozumitelně.

Národní úřad pro kybernetickou a informační bezpečnost na svých internetových stránkách zveřejní formulář, který bude využit pro předkládání podkladů.

K § 10

Datum nabytí účinnosti návrhu vyhlášky je stanoveno dnem následujícím po jejím vyhlášení ve Sbírce zákonů.

S ohledem na skutečnost, že novela zákona o informačních systémech veřejné správy, nabývá účinnosti na začátku třetího kvartálu 2021, je nezbytné, aby návrh vyhlášky, který je prováděcím předpisem zákona o informačních systémech veřejné správy, rovněž nabyl účinnosti k tomuto datu, resp. co nejdříve po tomto datu. Datum nabytí účinnosti je proto stanoveno odlišně od § 3 odst. 3 zákona č. 309/1999 Sb., o Sbírce zákonů a o Sbírce mezinárodních smluv, ve znění pozdějších předpisů.

K příloze č. 1

V příloze č. 1 se rozumí třídou cloud computingu cloud computing ve formě infrastruktury IaaS, cloud computing ve formě platformy PaaS a cloud computing ve formě aplikačního programového vybavení SaaS. Třída cloud computingu je definována vyhláškou č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu.

K řádku 1

Požadavek je zaveden pro usnadnění jednání a zajištění lepší vymahatelnosti práva (závazky ze smluv, porušení právních předpisů), kdy je v rámci EU předpokládán společný právní rámec pro vymáhání soudních rozhodnutí. S ohledem na charakter poskytovaných služeb je důležité, aby požadavek dopadal na poskytovatele cloud computingu, kteří budou nejčastěji těmi, kdo přistupuje k datům zákazníka. V případě subjektů se sídlem nebo bydlištěm v České republice se budou uvedené informace získávat z veřejných rejstříků a není je tedy třeba dokládat.

K řádku 2

Daný požadavek vyjadřuje určitou spolehlivost v otázkách kybernetické bezpečnosti z pohledu České republiky. Požadavek na trestní bezúhonnost je řešen na úrovni zákona o informačních systémech veřejné správy.

K vyřazení bagatelních přestupků (jako např. nepatrné zmeškání lhůty pro nahlášení kontaktních údajů dle zákona o kybernetické bezpečnosti) byla doplněna hranice závažnosti přestupku.

K řádku 3

V rámci certifikace ISO/IEC 27001 je zkoumán i postoj vedení organizace k zajištění bezpečnosti informací. Z toho důvodu je tento požadavek relevantní i při zkoumání subjektu poskytovatele cloud computingu, v jehož správě následně budou zákaznická data a provozní údaje. Vzhledem k tomu, že splnění požadavků certifikace se může v čase měnit, je platnost certifikace omezena na 3 roky, resp. každý rok se koná dozorový audit, a jednou za 3 roky recertifikační audit (viz ISO/IEC 17021-1, kap. 9.1.3.2). Pro zajištění trvalého plnění požadavků certifikace a ověření tohoto plnění se stanovuje, že poskytovatel cloud computingu dodá každých 15 měsíců do evidence v katalogu cloud computingu auditní zprávu z dozorového, resp. recertifikačního auditu, a spolu s tím doloží i stále platný certifikát. Dokládaná auditní zpráva nesmí být starší než 3 měsíce, aby se zaručilo, že je vždy předkládaná aktuální auditní zpráva. Vzhledem k tomu, že uvedené audity je třeba v daných periodách dle výše uvedené ISO normy provádět, nepředstavuje požadavek na pravidelné předkládání auditních zpráv, resp. certifikátů, nijak zvýšený a zatěžující požadavek.

K příloze č. 2

V příloze č. 2 se rozumí třídou cloud computingu cloud computing ve formě infrastruktury IaaS, cloud computing ve formě platformy PaaS a cloud computing ve formě aplikačního programového vybavení SaaS. Třída cloud computingu je definována vyhláškou o údajích vedených v katalogu.

Příloha č. 2 v označených pasážích v nízké a střední bezpečnostní úrovni vychází z návrhu EUCS. S ohledem na to, že se jedná o návrh, není vyloučena budoucí změna obsahu jednotlivých ustanovení.

K řádkům 1.1 a 1.2

Podstatným prvkem a zároveň rizikem při využívání služeb cloud computingu je skutečnost, že zákazník předává svá data a informace poskytovateli cloud computingu. Poskytovatelem cloud computingu mnohdy může být zahraniční společnost, podléhající jurisdikci cizích států jak v Evropské unii a státech, které jsou členskými státy Evropského sdružení volného obchodu (dále jen „EU/ESVO“), tak ale i mimo EU/ESVO. Zároveň jsou data při využívání služby cloud computingu ukládána na území států v EU/ESVO. Níže se zavádí několik požadavků na poskytovatele cloud computingu, resp. na místo uložení a zpracování dat, které mají do této

oblasti přinést více transparentnosti tak, aby si zákazníci byli uvedeného rizika vědomi a mohli ho zohlednit při rozhodování, zda služby cloud computingu využijí.

V prvé řadě poskytovatel cloud computingu doloží seznam všech lokalit, ve kterých bude docházet ke zpracovávání zákaznických dat a specifických provozních údajů. Lokalitu je nutné doložit minimálně na úroveň státu, ve kterém bude docházet k výše uvedenému zpracovávání.

V souladu s výše uvedeným poskytovatel doloží také seznam všech lokalit, ve kterých je prováděn výkon správy a dohledu nad službou, zákaznickými daty a specifickými provozními údaji.

Požadavky jsou v souladu s ustanovením Annex A, kapitoly DOC-03.2 a DOC-03.3 EUCS.

K řádku 1.3

Podstatným prvkem a zároveň rizikem při využívání služeb cloud computingu je skutečnost, že zákazník předává svá data a informace poskytovateli cloud computingu. Poskytovatelem cloud computingu mnohdy může být zahraniční společnost podléhající jurisdikci cizích států i mimo EU/ESVO. Níže se objasňuje několik požadavků na poskytovatele cloud computingu, resp. na místo uložení a zpracování dat, které mají do této oblasti přinést více transparentnosti tak, aby si zákazníci byli uvedeného rizika vědomi a mohli jej zohlednit při rozhodování, zda služby cloud computingu využijí.

Za neaktivní data (data at rest) lze přitom považovat data uložená a skladovaná v trvalém úložišti. Vedle neaktivních dat jsou aktivní data (data in use), za která se považují data zpracovávaná v daném okamžiku (CPU/RAM). A konečně přenášená data (data in transit, in motion), tedy data přenášená po síti.

Pojem „*uloženo nepřetržitě*“ má za cíl zajistit, aby k ukládání neaktivních dat nedocházelo jen mimo EU/ESVO– tedy, aby byla data vždy nepřetržitě dostupná na území EU/ESVO a slouží tak k zajištění vyšší dostupnosti. Toto sousloví však nebrání tomu, aby k jinému ukládání, než ve stavu neaktivních dat docházelo i mimo EU/ESVO za předpokladu, že současně s tím jsou zákaznická data neustále uložena i na území EU/ESVO.

Z vyjádření poskytovatelů cloud computingu při přípravě návrhu vyhlášky vyplývá, že pro některé služby cloud computingu by omezení místa ukládání neaktivních dat pouze na EU/ESVO představovalo nepřekonatelnou překážku a mnohdy by bylo v rozporu s jejich účelem (např. pokročilé bezpečnostní funkce využívající porovnávání škodlivých vzorků dat, které v případě, že probíhá globálně, je účinnější, protože škodlivý vzorek dat musí být trvale uložen). Proto je zahrnuta možnost neaplikovat toto ustanovení. Taková odchylka však musí být maximálně transparentní, a proto se zavádí nezbytnost uvést takové služby na internetových stránkách Národního úřadu pro kybernetickou a informační bezpečnost. Forma internetových stránek byla zvolena vzhledem k dynamickému vývoji na trhu se službami cloud computingu tak, aby bylo dosaženo co nejsnazší aktualizace takového seznamu. V případě, že poskytovatel cloud computingu bude usilovat o aplikaci takovéto odchylky, postačí, když jasně označí

službu cloud computingu, která neukládá trvale a nepřetržitě neaktivní data na území EU/ESVO.

V případě, že některou ze skutečností dokládá poskytovatel cloud computingu předložením auditní zprávy SOC 2® Type 2, nesmí být tato auditní zpráva starší než 24 měsíců k datu podání žádosti o zápis do katalogu.

Nadto je nutné zdůraznit, že byť se pravidla pro uložení a zpracování dat v tomto řádku neuplatní pro bezpečnostní úroveň nízká a střední, musí správci těchto systémů vzít v potaz požadavky vyplývající z regulace na úseku ochrany osobních údajů, pokud jsou do systému vloženy, zejména zajistit nezbytnou úroveň ochrany osobních údajů.

K řádku 1.4

Požadavek na zacházení se specifickými provozními údaji vychází z požadavku na řádku 1.3 a z toho, že i ve specifických provozních údajích se mohou nacházet data a informace, která se svým významem blíží, shodují, nebo dokonce převyšují důležitost zákaznických dat. Viz odůvodnění k § 2 návrhu vyhlášky.

K řádku 1.5

Návrh vyhlášky s ohledem na výše popsané riziko přístupu cizích, zpravidla státních orgánů, preferuje zpracování zákaznických dat na území členských států EU/ESVO, jako prostoru se sdílenými vzájemnými hodnotami a právními nástroji k ochraně a přístupu k datům. Zpracování mimo území EU/ESVO není zakázáno, ale je omezeno na odůvodněné případy, po nezbytně nutnou dobu a v nezbytném rozsahu. Pro úplnost je nutné dodat, že za zpracování se považuje mimo jiné i nepřetržité uložení neaktivních dat dle předchozích řádků.

Zároveň se poskytovatelům cloud computingu ukládá povinnost předložit informace o tom, zda při využívání jimi nabízené služby cloud computingu dochází ke zpracování zákaznických dat a provozních údajů mimo EU/ESVO. V případě, že k tomu dochází, pak vyžaduje uvedení předpokládaných hodnot takového zpracování. Tyto informace zároveň budou uvedeny v katalogu. Opatření má za cíl zvýšit transparentnost a upozornit potenciální zákazníky na riziko zpracování dat mimo území EU/ESVO spojené s využíváním dané služby cloud computingu.

K rozsahu zpracování dat lze uvést, že vzhledem k rozdílnosti jednotlivých služeb cloud computingu, způsobu jejich využití a objemu dat vkládaných zákazníkem do služby cloud computingu se vyjádření rozsahu ponechává na poskytovateli cloud computingu. Může jít o vyjádření v objemových jednotkách (byte), může jít o vyjádření ve zlomcích/procentech z celku zákaznických dat, či může jít o popis oblastí služby, do jejíchž části vložená data budou zpracována mimo EU/ESVO.

Nadto je nutné zdůraznit, že byť se pravidla pro uložení a zpracování dat v tomto řádku neuplatní pro bezpečnostní úroveň nízká a střední, musí správci těchto systémů vzít v potaz požadavky vyplývající z regulace na úseku ochrany osobních údajů, pokud jsou do systému vloženy, tedy zejména zajistit nezbytnou úroveň ochrany osobních údajů.

K řádku 1.6

Požadavek na zacházení se specifickými provozními údaji vychází z požadavků na řádcích 1.4 a 1.5 přílohy č. 2 k návrhu vyhlášky a z toho, že i ve specifických provozních údajích se mohou nacházet data a informace, která se svým významem blíží, shodují, nebo dokonce převyšují důležitost zákaznických dat. Viz odůvodnění k § 2 návrhu vyhlášky.

K řádku 1.7

Jedním z opatření na ochranu před neřízeným předáváním a zpracováváním dat mimo EU/ESVO a jejich případným zneužitím mimo právní rámec EU/ESVO je vyžádání souhlasu zákazníka. Zákazník vyslovením souhlasu akceptuje vystavení se riziku, což může být při některých způsobech využití služeb cloud computingu a při zpracování některých dat přijatelné.

Poskytovatel cloud computingu vyžaduje souhlas zákazníka pro případy zpracování zákaznických dat mimo území EU/ESVO, který je vyjádřen na samostatném dokumentu, nebo vyžaduje v základním nastavení služby svolení v každém jednotlivém případě ke zpracování zákaznických dat mimo území EU/ESVO.

Preferovanou variantou je umožnění vyžádání souhlasu pro každý jednotlivý případ exportu dat zvlášť, nicméně je patrné, že toto nebude vždy technicky zcela možné u všech poskytovaných služeb.

V případě, že zákazník využívá více služeb cloud computingu od jednoho poskytovatele a tyto služby mají shodné místo zpracování dat, je možné udělit souhlas pro všechny tyto služby souhrnně.

V případě, že zákazník využívá více služeb cloud computingu od jednoho poskytovatele a tyto služby mají shodný rozsah, účel a dobu zpracování, je možné informovat zákazníka pro všechny tyto služby se shodnými parametry souhrnně.

V případě, že má dojít ke změně předpokládaného území státu, na němž dochází nebo může docházet k zpracování zákaznických dat a má se jednat o území státu, které není členským státem Evropské unie nebo členským státem Evropského sdružení volného obchodu, musí být nezbytnou součástí informování zákazníka i nová žádost o souhlas zákazníka se zpracováním zákaznických dat na území tohoto státu. Pokud zákazník neudělí souhlas se zpracováváním zákaznických dat na území tohoto státu, nesmí poskytovatel na území tohoto státu zákaznická data zpracovávat.

Má-li být zajištěno dostatečné informování zákazníka, je nezbytné, aby v případě, že má dojít ke změně předpokládaného rozsahu, účelu a doby zpracovávání zákaznických dat, poskytovatel cloud computingu o této změně zákazníka včas informoval tak, aby mohl zákazník vyhodnotit dopad této změny. Pokud zákazník nevysloví nesouhlas v poskytovatelem stanovené přiměřené lhůtě, má se za to, že souhlasí se zpracováním zákaznických dat v nově nastavených parametrech.

Doložení naplnění požadavku lze prokázat dokumentem, jímž je vyžadován souhlas zákazníka pro případy zpracování zákaznických dat mimo území EU/ESVO nebo odkazem na konkrétní část podmínek poskytování služby nebo částí návrhu smlouvy nebo produktové specifikace, ze které bude patrné, že poskytovatel cloud computingu umožňuje vyžádání svolení v každém jednotlivém případě zpracování zákaznických dat mimo území EU/ESVO. Zákazník musí být v každém případě schopen z poskytnutých informací posoudit rizikovost takového předání zákaznických dat mimo území EU/ESVO.

Nadto je nutné zdůraznit, že byť se pravidla pro uložení a zpracování dat v tomto řádku neuplatní pro bezpečnostní úroveň nízká a střední, musí správci těchto systémů vzít v potaz požadavky vyplývající z regulace na úseku ochrany osobních údajů, pokud jsou do systému vloženy, tedy zejména zajistit nezbytnou úroveň ochrany osobních údajů.

K řádku 1.8

Data a informace s nejzávažnějšími dopady v případě narušení jejich bezpečnosti, tedy data a informace v informačních systémech nebo jejich částech zařazených do kritické bezpečnostní úrovně, by neměla vůbec opouštět území České republiky. Za tímto účelem budou moci být taková data zpracovávána pouze v cloud computingu státního poskytovatele cloud computingu, jak stanoví zákon o informačních systémech veřejné správy. Zpracování mimo Českou republiku však nelze zakázat zcela, jelikož v ex ante fázi nelze dohlédnout všechny konkrétní způsoby aplikace využití služeb cloud computingu jednotlivými zákazníky a zároveň je velmi pravděpodobné, že státní poskytovatel cloud computingu bude využívat služeb a produktů zahraničních dodavatelů, jejichž servis by byl v případě úplného zákazu vývozu dat velmi omezen. Proto se ponechává možnost vyslovit souhlas s jejich předáním a zpracováním dat i mimo Českou republiku. Takový souhlas ale musí být výslovný, tedy nikoliv skrytý v rámci ostatních smluvních ustanovení, ale dostatečně odsazený a zdůrazněný od ostatního textu smlouvy, popř. musí tvořit zcela samostatný dokument. Souhlas může být udělen jako generální před zahájením využívání cloud computingu nebo v každém jednotlivém případě. V případě generálního souhlasu musí být tento nezbytně písemný. V případě jednotlivých souhlasů musí být obecný rámec písemný a vyslovení s dílčím zpracováním mimo území České republiky se pak může realizovat skrze prostředky pro komunikaci na dálku.

Požadavky na řádcích 1.5 a 1.7 se zde uplatní obdobně.

V případě kritické bezpečnostní úrovně je na základě požadavků vyplývajících ze SAZ[8] nutné ještě více omezit možné předávání dat mimo území České republiky a podmínit jej kontrolou zákazníka nad tím, která data, v jakém rozsahu a za jakým účelem opustí území České republiky.

[8] Souhrnná analytická zpráva projektu eGovernment cloud schválená usnesením vlády České republiky ze dne 14. listopadu 2018 č. 749 o souhrnné analytické zprávě, výstupu Fáze I. projektu Příprava vybudování eGovernment cloudu.

K řádku 2.1

V případě obdržení žádosti cizozemského orgánu o zpřístupnění či předání zákaznických dat a specifických provozních údajů je nezbytné, aby poskytovatel cloud computingu přesměroval cizozemský orgán přímo na zákazníka, není-li mu to relevantním právním předpisem zakázáno.

Cizozemským orgánem se rozumí státní orgán odlišný od státního orgánu České republiky (viz vládní návrh zákona o občanských průkazech, sněmovní tisk 1043).

Podléháním právnímu řádu se rozumí stav, kdy si cizozemský orgán může vynutit splnění právních předpisů daného právního řádu.

Požadavek je v souladu s ustanovením Annex A, kapitoly INQ-02.1 EUCS.

K řádkům 2.2

Tyto požadavky upřesňují, jak má poskytovatel cloud computingu postupovat v případě obdržení žádosti o zpřístupnění nebo předání dat, a zajistit, aby se tak dělo po náležitém prověření žádosti a vyvinout úsilí k jejímu rozporování v případě potřeby. Úsilím se rozumí postup v souladu s právním řádem státu, dle něhož byla žádost podána a jemuž poskytovatel cloud computingu podléhá. Nejčastěji se bude jednat o podávání žalob a odvolání proti příkazu data zákazníka vydat nebo zpřístupnit. Uvedené má za cíl omezit případy, kdy dojde ke zpřístupnění dat a případně k omezení rozsahu zpřístupňovaných zákaznických dat třetím stranám, především z řad zpravodajských služeb. Pokud již má ke zpřístupnění dojít, je nezbytné, aby se to nestalo jinak, než jak je předvídáno mezinárodními smlouvami (na základě justiční spolupráce), právním řádem státu, dle něhož byla žádost podána a jemuž poskytovatel cloud computingu podléhá, a v návrhu vyhlášky popsaným procesem, především tedy po právním posouzení žádosti, provedeným poskytovatelem cloud computingu. Pokud je to možné, zákazník by se měl vždy o takové žádosti dozvědět a podílet se na jejím vyřízení.

Postup uvedený v požadavku směřuje na všechny žádosti cizozemských orgánů bez ohledu na jejich formu (soudní příkaz, správní příkaz, neformální žádost).

Cizozemským orgánem se rozumí státní orgán odlišný od státního orgánu České republiky (viz vládní návrh zákona o občanských průkazech, sněmovní tisk 1043).

Podléháním právnímu řádu se rozumí stav, kdy si cizozemský orgán může vynutit splnění právních předpisů daného právního řádu.

K řádku 2.3

Požadavek rozvádí povinnost poskytovatele na řádku 2.1 tak, že v případě obdržení žádosti cizozemského orgánu o zpřístupnění či vydání dat zákazníka, musí poskytovatel cloud computingu tuto žádost přezkoumat všemi vhodnými způsoby. Pouze v případě, že z posouzení poskytovatele cloud computingu vyplyne, že je taková žádost proveditelná, aplikovatelná, má právní základ, je právně závazná a rozsah, v jakém je požadován přístup k datům zákazníka či

jejich vydání odpovídá účelu, za jakým byla žádost podána, zákaznická data nebo specifické provozní údaje zpřístupní či vydá.

O provedeném posouzení je poskytovatel cloud computingu povinen provést záznam, ze kterého bude patrné zejména to, proč shledal či neshledal předmětnou žádost proveditelnou, aplikovatelnou, postavenou na právním základu, právně závaznou a rozsahem odpovídající jejímu účelu. Tento záznam musí poskytovatel uchovat alespoň 5 let, případně jej prokazatelně předat zákazníkovi.

Požadavek je v souladu s ustanovením Annex A, kapitoly INQ-02.1 EUCS.

K řádku 2.4

Požadavek rozvádí povinnost poskytovatele cloud computingu na řádku 2.3 tak, že v případě obdržení žádosti cizozemského orgánu o zpřístupnění či vydání dat zákazníka přezkoumá všemi vhodnými způsoby tuto žádost. I v případě, že z posouzení poskytovatele cloud computingu vyplyne, že je taková žádost proveditelná, aplikovatelná, má právní základ, je právně závazná a rozsah, v jakém je požadován přístup k datům či jejich vydání, odpovídá účelu, za jakým byla žádost podána, je poskytovatel cloud computingu povinen vyvinout veškeré možné úsilí v mezích relevantních zákonů (například rozporování žádosti o zpřístupnění či vydání před nezávislým soudem) vedoucí k tomu, aby zabránil předání či zpřístupnění zákaznických dat nebo specifických provozních údajů bez souhlasu zákazníka.

Pouze pro úplnost se uvádí, že v případě, že poskytovatel cloud computingu zrušení povinnosti zpřístupnění nebo předání zákaznických dat a specifických provozních údajů nedosáhne, předá či zpřístupní pouze nezbytně nutná zákaznická data a specifické provozní údaje, které odpovídají rozsahu žádosti o předání či zpřístupnění zákaznických dat a specifických provozních údajů.

O provedeném posouzení je poskytovatel cloud computingu povinen provést záznam, ze kterého bude patrné zejména to, proč shledal či neshledal předmětnou žádost proveditelnou, aplikovatelnou, postavenou na právním základu, právně závaznou a rozsahem odpovídající jejímu účelu. Tento záznam musí poskytovatel cloud computingu uchovat alespoň 5 let, případně jej prokazatelně předat zákazníkovi.

K řádku 2.5

Zákazník by měl před využitím služeb cloud computingu vyhodnotit mj. i rizika spojená s využitím takových služeb, kdy podstatným rizikem je přístup cizích státních orgánů k datům vloženým do služby cloud computingu. Proto, aby měl zákazník pro své hodnocení maximum dostupných informací o potenciálních právních závazcích a povinnostech poskytovatele cloud computingu, které se týkají zpřístupnění a předávání zákaznických dat a provozních údajů, a zároveň, aby měly tyto informace i Ministerstvo vnitra České republiky a Národní úřad pro kybernetickou a informační bezpečnost, se zavádí požadavek na poskytovatele cloud computingu tyto závazky a povinnosti jasně a srozumitelně popsat. Takovou informaci pak může zákazník od poskytovatelů cloud computingu žádat při jejich výběru.

Zákazník musí být schopen na základě předložené informace vyhodnotit vliv právního řádu na poskytování služby cloud computingu a posoudit tak vhodnost nabízené služby pro jeho potřeby.

Požadavek je v souladu s ustanovením Annex A, kapitoly DOC-03.1 a DOC-03.2 EUCS, protože oproti požadavkům v EUCS, které se zaměřují na všechny informace pro vyhodnocení vhodnosti dané jurisdikce (např. informace o dodržování lidských práv, ústavnosti či obecně právního pořádku), se zde požadují pouze informace o povinnostech k předání a zpřístupnění dat.

K řádku 2.6

V případě služeb poskytovaných systémům zařazeným do kritické bezpečnostní úrovně je s ohledem na skutečnost, že data budou trvale umístěna na území České republiky v rámci státního poskytovatele cloud computingu, poskytovatel cloud computingu oprávněn a povinován žádosti třetích stran, především z řad zpravodajských služeb a orgánů činných v trestním řízení cizích států, odmítnout a odkázat je na příslušný orgán rozhodující o zpřístupnění dat v rámci justiční spolupráce. Zároveň s tím se poskytovatel cloud computingu nemusí obávat represivních kroků ze strany jurisdikce, z níž žádost pochází, protože státní poskytovatel cloud computingu bude umístěn na území České republiky.

K řádku 3.1

Požadavek slouží k ověření dodržování povinnosti poskytovatele cloud computingu vyplývající ze zákona o informačních systémech veřejné správy, která spočívá v poskytování pouze takové služby cloud computingu, která umožňuje dosažení alespoň základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánů veřejné správy. Ověřuje, zda poskytovatel cloud computingu splňuje ustanovení návrhu vyhlášky i po zápisu do katalogu cloud computingu. Dále je jeho účelem ověřit dodržování povinnosti poskytovatele cloud computingu spočívající v poskytování pouze těch služeb cloud computingu, které umožňují orgánu veřejné správy postupovat podle bezpečnostních pravidel pro orgány veřejné moci využívající služby cloud computingu. V zákoně o informačních systémech veřejné správy je již zakotveno kontrolní oprávnění pro Ministerstvo vnitra ČR a Národní úřad pro kybernetickou a informační bezpečnost. Zároveň je záměrem uvedeného ustanovení vyjádřit obecně platnou zásadu, že kontrolní oprávnění nelze zneužívat a aplikovat šikanózně.

Ministerstvo vnitra či Národní úřad pro kybernetickou a informační bezpečnost a poskytovatel cloud computingu se vzájemně předem dohodnou na rozsahu, datu, době trvání, požadavcích na kontrolu a požadovaných podkladech, ledaže by tento požadavek na vzájemnou dohodu umožňoval poskytovateli cloud computingu bezdůvodně zdržovat průběh šetření. Kontrola na místě nebo zařízení souvisejícím s poskytováním služby cloud computingu bude provedena pouze v těch bodech, které nebude možné vyřešit vzdáleným přístupem, videokonferencí, nebo předložením bezpečnostní dokumentace poskytovatele cloud computingu.

Kontrolní práva poskytované Ministerstvu vnitra či Národnímu úřadu pro kybernetickou bezpečnost mohou být dále podmíněna následujícím:

- Vstup do prostor podléhá zajištění zdraví, bezpečnosti a ochrany všech osob zúčastněných na kontrole.

- V rozsahu, v jakém mohou být informace vyžadované pro účely kontroly poskytnuty prostřednictvím auditních zpráv, dokumentace či jiných podkladů připravených zákazníkem či poskytovatelem cloud computingu předem pro kontrolní účely, včetně kontroly ze strany Národního úřadu pro kybernetickou a informační bezpečnost, nebo které mohou být zpřístupněné virtuálně dálkovým způsobem, budou strany usilovat o splnění těchto požadavků prostřednictvím dálkové virtuální komunikace a sdílení dokumentace prostřednictvím zabezpečených protokolů.

- Jakákoliv kontrola na místě bude provedena za dozoru koordinátora a dozorující osoby ze strany poskytovatele cloud computingu, která je pověřena vedením šetřených prostor poskytovatele cloud computingu.

- Kontrola bude provedena během běžných pracovních hodin, a to na základě předchozího včasného oznámení poskytovateli cloud computingu a bude provedena přijatelně důvěrným postupem, který bude způsobilý ochránit důvěrnost aktiv poskytovatele cloud computingu.

- Ministerstvo vnitra či Národní úřad pro kybernetickou a informační bezpečnost nebudou oprávněny přistupovat k jakýmkoliv datům patřícím zákazníkovi nebo poskytovateli cloud computingu bez souhlasu daného zákazníka, včetně zákazníka, který je kontrolovanou osobou.

Z textu § 6i odst. 3 zákona o informačních systémech veřejné správy vyplývá, že kontrolující (Národní úřad pro kybernetickou a informační bezpečnost či Ministerstvo vnitra) je oprávněn kontrolovat službu cloud computingu poskytovanou orgánům veřejné správy. Výše uvedené podmínky realizace kontroly nelze proto považovat za omezení tohoto kontrolního oprávnění, které podzákonným předpisem není ani dobře možné, ale za upřesnění, za jakých podmínek nedojde k nesplnění požadavku na řádku 3.1 přílohy č. 2 k této vyhlášce, a z toho vyplývajícího potenciálního výmazu poskytovatele z katalogu cloud computingu. Není tedy nutné v textu vyhlášky upravovat znemožnění přístupu k zákaznickým datům jiných zákazníků, než jsou právě orgány veřejné správy a zároveň nelze vyhláškou omezit právo kontrolujících nahlížet na data zákazníků, kterým je poskytována služba cloud computingu, a kteří jsou orgány veřejné správy.

Zákon o informačních systémech veřejné správy stanoví v § 6i odst. 3, že Národní úřad pro kybernetickou a informační bezpečnost kontroluje, zda cloud computing poskytovaný orgánům veřejné správy splňuje požadavky podle § 6n v případě, že je využíván k provozování informačního systému veřejné správy, který je informačním nebo komunikačním systémem

kritické informační infrastruktury, významným informačním systémem nebo informačním systémem základní služby podle právního předpisu upravujícího kybernetickou bezpečnost.

Z uvedeného tedy vyplývá, že informační systémy nepodléhající zákonu o kybernetické bezpečnosti bude kontrolovat v celém rozsahu Ministerstvo vnitra ČR. Informační systémy podléhající zákonu o kybernetické bezpečnosti a zároveň zákonu o informačních systémech veřejné správy bude v rozsahu splnění § 6n kontrolovat Národní úřad pro kybernetickou a informační bezpečnost. Plnění ostatních povinností vyplývajících ze zákona o informačních systémech veřejné správy bude dozorovat Ministerstvo vnitra ČR.

K řádkům 4.1 a 4.2

Dostupnost je jedním ze základních aspektů bezpečnosti informací zpracovávaných za účelem využití služby cloud computingu. Hodnoty dostupnosti vyjádřené v návrhu vyhlášky odráží závěry učiněné v SAZ a reflektují předpokládané potřeby zákazníků. Pojmem „nepřetržitá provozní doba“ v řádku 6 je myšlena dostupnost 24 hodin denně, 7 dní v týdnu (dále jen „režim 24x7“). Poskytovatel cloud computingu usilující o zápis nabídky v dané bezpečnostní úrovni musí být schopen tyto limity dodržet. Při jednání s konkrétním zákazníkem však v rámci nasazení konkrétní služby cloud computingu bude možné sjednat limity vyšší či nižší tak, aby odrážely skutečnou potřebu zákazníka.

K řádku 5.1

Dalším z opatření pro zajištění vyšší dostupnosti služby cloud computingu je požadavek na zajištění připojení poskytovatele cloud computingu do peeringového uzlu v České republice. Připojení do peeringového uzlu v České republice může mít pozitivní vliv i na důvěrnost informací v případě, že je do stejného peeringového uzlu připojen i zákazník.

K řádku 6.1 a 6.2

Plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu jsou nástroje sloužící pro zajištění dostupnosti uvedené v řádcích 4.1 a 4.2 přílohy č. 2 k návrhu vyhlášky. Zákazník musí být schopen posoudit, jak bude s jemu poskytovanou službou cloud computingu zacházeno poskytovatelem cloud computingu v případě nenadálé či krizové situace. Na základě tohoto posouzení si zákazník vypracuje vlastní plány zajišťující provoz služby cloud computingu. Aby byl zákazník schopen uvedeného posouzení, je třeba, aby měl poskytovatel cloud computingu takové plány vůbec vytvořeny.

Rozdíl mezi řádky 6.1 a 6.2 potom spočívá v tom, že poskytovatel, na kterého dopadá povinnost stanovená na řádku 6.2 musí k prokázání souladu předložit plnou auditní zprávu.

Požadavek je v souladu s ustanovením Annex A, kapitoly BC-01.1, EUCS.

K řádku 6.3

Tento požadavek je zaměřen na ochranu datacenter, ze kterých je poskytována služba cloud computingu tak, aby byla chráněna před vnějšími vlivy a byla tak zachována dostatečná dostupnost služby cloud computingu.

Dostatečná vzdálenost je individuální v každém případě a je nutné zohlednit všechny okolnosti zejména s ohledem na vzdálenost datového centra od zdrojů naturogenních a antropogenních vlivů. S ohledem na požadavek na řádku 6.4 lze také považovat za takovou vzdálenost 50 km vzdušnou čarou.

Požadavek je v souladu s ustanovením Annex A, kapitoly PS-05.5 EUCS.

K řádku 6.4

Pro zachování kontinuity poskytování služby cloud computingu a zajištění její dostatečné dostupnosti je nezbytné, aby měl poskytovatel cloud computingu možnost v případě potřeby přenést poskytování služby cloud computingu na alespoň jedno jiné datacentrum. Pro možnost okamžitého poskytování služby cloud computingu ze záložního datacentra musí docházet k synchronní (okamžité, real-time) replikaci dat. Z uvedeného je tedy patrné, že poskytovatel cloud computingu musí mít alespoň dvě datacentra, kdy obě jsou dostatečně kapacitní k převzetí služeb druhého datacentra.

Za primární a záložní datacentrum lze považovat dvě redundantní datová centra, kdy z obou z nich je poskytovatel cloud computingu schopen zajistit funkčnost služby cloud computingu.

K řádku 6.5

Tento požadavek je zaměřen na ochranu datacenter, ze kterých je poskytována služba cloud computingu tak, aby byla chráněna před vnějšími vlivy, a byla tak zachována dostatečná dostupnost služby cloud computingu.

Za tím účelem je možné předložit buď zprávu o posouzení zdrojů rizik, ze které vyplývá dostatečná vzdálenost datových center, a jejíž náležitosti jsou uvedeny v příloze, nebo alternativně doložit vzájemnou vzdálenost datacenter nejméně 50 km vzdušnou čarou, kdy lze s jejich rostoucí vzájemnou vzdáleností předpokládat snižující se pravděpodobnost jejich vystavení stejným zdrojům rizik. S ohledem na ustanovení zákona o archivnictví (viz § 61 odst. 2 písm. f zákona č. 499/2004 Sb.) byla zvolena stejná minimální vzdálenost, a to 50 km vzdušnou čarou. V obou případech lze naplnění požadavku prokázat odkazem do příslušné auditní zprávy obsahující požadované informace.

Za primární a záložní datacentrum lze považovat dvě redundantní datová centra, kdy z obou z nich je poskytovatel cloud computingu schopen zajistit funkčnost služby cloud computingu.

K řádku 6.6

Požadavek na umístění datacenter v rámci České republiky nebo dvou různých státech EU/ESVO zajišťuje zabezpečení provozu datacenter i v případě neočekávaných geopolitických událostí, např. omezení provozu datacenter v důsledku vyhlášených karanténních opatření.

Toto ustanovení nebrání odlišnému smluvnímu ujednání. Vzhledem k tomu, že ve službách cloud computingu využívaném orgány veřejné správy České republiky budou převážně „státní“ data veřejné správy, není důvodné ošetřovat situaci geopolitické změny v České republice.

K řádku 6.7

V případě kritické bezpečnostní úrovně je s ohledem na kritickou povahu dat nutné, aby byla všechna datacentra umístěna na území České republiky, a to i s ohledem na požadavek uvedený v řádku 1.8 přílohy č. 2 k návrhu vyhlášky. Lze však brát v potaz výjimečné situace (např. hrozby konfliktu s cizími státy, válečný stav, přírodní katastrofa velkého rozsahu atp.), pro které by nebylo vhodné zcela zakázat využití záložních datových center v zahraničí. Ke zpracování dat mimo území ČR tak může dojít pouze za účelem servisu a/nebo zajištění funkčnosti služby cloud computingu. Nemůže se však jednat o samotné poskytování služby. I v takovém případě data musí být šifrována, a to bez možnosti jejich rozšifrování poskytovatelem cloud computingu. Toto ustanovení není v rozporu s pravidlem na řádku 1.8 přílohy č. 2 k návrhu vyhlášky, protože v případě poskytování servisních a jiných služeb z datacentra mimo území ČR se nebude jednat o primární ani záložní datacentrum. Za primární a záložní datacentrum lze považovat dvě redundantní datová centra, kdy z obou z nich je poskytovatel cloud computingu schopen zajistit funkčnost služby cloud computingu.

K řádku 6.8

Poskytovatel cloud computingu musí být schopen nabídnout zákazníkovi nástroje nebo služby pro zvýšení odolnosti vůči těmto typům útoků. Zákazník následně zváží, jestli tyto nástroje bude vyžadovat při konkrétním využití služby cloud computingu.

K řádku 6.9

Služba management portálu případně jiné formy administrátorské konzole umožňující vzdálenou obsluhu služby cloud computingu v nepřetržitém režimu je nástrojem, který umožní zákazníkovi pružně reagovat na jakékoliv nutné události a jevy spojené s poskytováním služby cloud computingu. Konkrétní nasazení tohoto nástroje si upřesní zákazník s poskytovatelem cloud computingu.

K řádku 7.1

Ve službách cloud computingu může být orgánem veřejné správy zpracováváno velké množství dat, přičemž za velký objem dat lze považovat například přenosy dat v řádu jednotek terabytů. Je proto třeba ošetřit situace jako např. ukončení smlouvy nebo změny politicko-právního prostředí v zemi, kde jsou data uložena. V takovém případě bude třeba data rychle od poskytovatele cloud computingu stáhnout tak, aby je bylo možné využít v jiné službě cloud computingu nebo systému provozovaném zákazníkem či jiným poskytovatelem cloud computingu. Pro takové situace se zavádí uvedené ustanovení, kdy nahrání dat na vyměnitelné médium může být násobně rychlejší než jejich zasílání prostřednictvím sítě internet.

Podstatným prvkem cloud computingu je, že je vzdáleně přístupný. Umožňuje tak import a export dat prostřednictvím sítě internet, což lze považovat za standard. Požadavek obsažený v návrhu vyhlášky pak stanoví vyšší standard pro služby vysoké a kritické bezpečnostní úrovně.

Daný požadavek míří na schopnost poskytovatele cloud computingu takové řešení nabídnout. Neznamená však, že ho zákazník v konečné situaci využije, a to s ohledem na způsob využití služby cloud computingu a typ a objem dat vkládaných do dané služby cloud computingu.

Při přenosu a zpracovávání dat musí být poskytovatel cloud computingu schopen zajistit ochranu zákaznického obsahu v souladu s pravidly stanovenými v řádku 1.4, přílohy č. 2 k návrhu vyhlášky. V případě, že to zákazník vyžaduje, musí si využití ochrany zákaznického obsahu sjednat smluvně.

K řádku 7.2

Šifrování je jedním z nástrojů zvýšení ochrany důvěrnosti dat. Poskytovatel cloud computingu musí chránit zákaznický obsah šifrováním při přenosu a uložení.

K řádku 7.3

Šifrování je jedním z nástrojů zvýšení ochrany důvěrnosti dat tak, aby byl omezen neoprávněný přístup k těmto datům jak ze strany administrátorů poskytovatele cloud computingu, uživatelů s nedostatečným oprávněním, tak osobami s nekalými úmysly. Proto se stanovuje povinnost data zákazníků šifrovat. Vzhledem k tomu, že při využití šifrování je klíčový i způsob šifrování dat a kvalita šifrovacích algoritmů, připojuje se odkaz na materiál, ve kterém je udržován přehled aktuálně doporučovaných algoritmů. Poskytovatel cloud computingu musí být schopen uvedené algoritmy nabídnout. Vedle doporučených algoritmů však mohou existovat i jiné, novější, účinnější, které nebyly zahrnuty do doporučení. Konečné řešení o využití konkrétního algoritmu je pak volbou zákazníka.

Šifrováním v úložištích se rozumí situace, kdy jsou data na discích šifrována. Nevyjadřuje to úroveň šifrování (úložištěm vs. operačním systémem vs. aplikací).

V současné chvíli neexistují relevantní vodítka podle EUCS, které by podobně jako doporučení Národního úřadu pro kybernetickou a informační bezpečnost stanovovaly vhodné šifrovací metody. Z toho důvodu zatím doporučujeme ponechat pravidlo v původním znění a až budou existovat relevantní vodítka, bude možné na něj odkázat.

K řádku 7.4

Šifrování je jedním z nástrojů zvýšení ochrany důvěrnosti dat. Je však třeba mít na paměti, že žádný způsob šifrování nemůže data zcela ochránit před poskytovatelem cloud computingu v případě, že je klíč k rozšifrování uložen v prostorách poskytovatele cloud computingu. Pro zvýšení jistoty před nechtěným přístupem poskytovatele cloud computingu k datům zpracovávaným ve službě cloud computingu se zavádí možnost zákazníka využívat vlastní šifrovací klíče, a nikoliv klíče poskytnutého samotným poskytovatelem cloud computingu.

HSM modul bude zpravidla uložen v datacentru a bude ve vlastnictví poskytovatele cloud computingu. Poskytovatel cloud computingu umožní vzdálenou instalaci vlastního klíče. Bude na rozhodnutí zákazníka, zda takovou službu využije.

K řádku 7.5

Pro kritickou bezpečnostní úroveň je nutné, aby poskytovatel umožňoval ukládání šifrovacích klíčů v certifikovaném HSM modulu stanovené úrovně ochrany a současně s tím umožňoval zákazníkovi jeho vzdálenou správu.

Je také možné podle pokynů zákazníka instalovat patřičný HSM modul do infrastruktury poskytovatele.

Bude na rozhodnutí zákazníka, zda takovou službu využije.

K řádku 7.6

Zlikvidování kryptografického klíče je jednou z podmínek zabezpečení zákaznických dat, neboť neumožní poskytovateli cloud computingu přistupovat k datům po skončení poskytování služby cloud computingu, která se vztahuje k těmto konkrétním datům.

K řádku 7.7

Likvidace dat je jednou z podmínek zabezpečení zákaznických dat, neboť neumožní poskytovateli cloud computingu přistupovat k datům po skončení poskytování služby cloud computingu, která se vztahuje k těmto konkrétním datům.

Je třeba mít na paměti, že tím není dotčen právní předpis upravující kybernetickou bezpečnost. Vyhláška o kybernetické bezpečnosti stanoví, že přípustný způsob likvidace dat pro služby cloud computingu by měl být upraven smluvním ujednáním. Je na zákazníkovi, jaký způsob likvidace dat zvolí. Poskytovatel cloud computingu musí být schopen odstranění všech zákaznických dat včetně předchozích verzí.

K řádku 7.8 a 7.9

Zaznamenávání zákazníkem neodsouhlaseného, resp. nevyžádaného přístupu k nešifrovaným zákaznickým datům je v každém jednotlivém případě velmi důležitým nástrojem. Poskytovateli umožňuje zpětně prověřit případné neoprávněné přístupy. Zákazníkům, ve spojení s ustanoveními, která zajišťují zpřístupnění takových záznamů zákazníkovi, umožňuje tento nástroj si ověřit a vyhodnotit jednotlivé přístupy poskytovatele k zákaznickým datům. V případě nejasností si pak zákazník může vyžádat od poskytovatele cloud computingu objasnění konkrétních přístupů. Tento nástroj slouží k navýšení kontroly zákazníka nad jeho daty. K tomu, aby přístup zákazníka mohl být efektivně zajištěn, se stanoví, že poskytovatel cloud computingu musí záznam uchovat po přiměřenou dobu. Řádově půjde o hodiny až dny, což umožní zákazníkovi (tj. orgánu veřejné správy) si záznam stáhnout a zpracovat.

Z vyjádření poskytovatelů služeb cloud computingu vyplynulo, že požadavek na vyhotovování záznamů o přístupu pracovníků a zejm. zpřístupňování takovýchto záznamů

zákazníkovi není aktuálně zcela běžné a vyžádá si technické úpravy v jednotlivých službách cloud computingu. Z toho důvodu mají tato ustanovení odloženou aplikovatelnost tak, aby poskytovatelům služeb cloud computingu byl poskytnut čas na provedení technických úprav a zajištěna dostatečná předvídatelnost právní úpravy. Samozřejmě je možné doložit splnění příslušného požadavku i před stanoveným datem.

K řádku 8.1

Pro bezpečnostní úroveň nízká je v souladu se zněním návrhu EUCS požadován alespoň soulad s certifikací ČSN EN ISO/IEC 27001, EN ISO ISO/IEC 27001 nebo ISO/IEC 27001. Tento soulad je potřeba prokázat čestným prohlášením, jehož bude součástí popis zavedených bezpečnostních opatření.

K řádkům 8.2 a 8.3

Certifikace ISO/IEC 27001 představuje základní množinu požadavků týkajících se bezpečnosti informací, které by měl splnit každý poskytovatel cloud computingu alespoň v rozsahu nabízeného cloud computingu.

Požadavek na certifikace, resp. certifikace samotné, představují jediný způsob ověření splnění požadavků třetí stranou. Ostatní požadavky závisí pouze na prohlášeních samotného poskytovatele cloud computingu. Vzhledem k tomu, že splnění požadavků certifikace se může v čase měnit, je platnost certifikace omezená na 3 roky, resp. každý rok se koná dozorový audit a jednou za 3 roky recertifikační audit (viz ISO/IEC 17021-1, kap. 9.1.3.2). Pro zajištění trvalého plnění požadavků certifikace a ověření tohoto plnění se stanovuje, že poskytovatel cloud computingu dodá každých 15 měsíců do evidence v katalogu cloud computingu auditní zprávu z dozorového, resp. recertifikačního auditu, a spolu s tím doloží i stále platný certifikát. Dokládaná auditní zpráva nesmí být starší než 3 měsíce, aby se zaručilo, že je vždy předkládána aktuální auditní zpráva. Vzhledem k tomu, že uvedené audity je třeba v daných periodách dle výše uvedené ISO normy provádět, nepředstavuje požadavek na pravidelné předkládání auditních zpráv, resp. certifikátů, nijak zvýšený a zatěžující požadavek.

Pro kladné vyhodnocení naplnění tohoto požadavku je klíčové předložení platného certifikátu, do jehož rozsahu jednoznačně náleží nabízená služba cloud computingu.

Řádek 8.3 pak nad rámec řádku 8.2 vyžaduje po poskytovateli cloud computingu předložení plné auditní zprávy.

IAF se rozumí International Accreditation Forum (dostupné z: https://www.iaf.nu/).

K řádku 8.4

Certifikace ISO/IEC 27017 přináší specifikaci standardu ISO/IEC 27001 z hlediska využití služeb cloud computingu a stanovuje dodatečná opatření pro poskytovatele cloud computingu i zákazníka využívajícího služeb cloud computingu. V návrhu certifikačního schématu kybernetické bezpečnosti cloudových služeb (EUCS) není stanoven požadavek na certifikace dle ISO/IEC 27017. Nicméně v návrhu EUCS je jasně deklarováno, že z této normy

v některých svých požadavcích vychází. Z toho důvodu je pro bezpečnostní úroveň střední požadována certifikace na ISO/IEC 27017.

K řádku 8.5

Certifikace ISO/IEC 27017 přináší specifikaci standardu ISO/IEC 27001 z hlediska využití služeb cloud computingu a stanovuje dodatečná opatření pro poskytovatele cloud computingu i zákazníka využívajícího služeb cloud computingu.

Požadavek na řádku 8.5 pak nad rámec požadavku na řádku 8.4 přílohy č. 2 k návrhu vyhlášky vyžaduje po poskytovateli cloud computingu předložení plné auditní zprávy.

K řádku 8.6

Certifikace ISO/IEC 27018 přináší specifikaci standardu ISO/IEC 27001 z hlediska ochrany osobních údajů a stanovuje dodatečná opatření pro poskytovatele cloud computingu.

K řádku 8.7

Požadavek stanovený na řádku 8.7 vychází ze SAZ[9] a vyžaduje pravidelné auditování požadavků na bezpečnost informací, kdy takový audit probíhá po určitou dobu a přináší hlubší pohled na dodržování požadavků na bezpečnost informací.

Z vyjádření poskytovatelů služeb cloud computingu vyplynulo, pravidelné auditování SOC 2® Type 2[10] nebo C5 Type 2[11] není aktuálně zcela běžné a vyžádá si čas, než ho poskytovatelé zavedou. Z toho důvodu má toto ustanovení odloženou aplikovatelnost tak, aby poskytovatelům služeb cloud computingu byl poskytnut čas na zavedení pravidelného auditování a zajištěna dostatečná předvídatelnost právní úpravy. Samozřejmě je možné doložit splnění příslušného požadavku i před stanoveným datem.

K řádku 9.1 a 9.2

Monitoring bezpečnostních událostí, jejich vyhodnocování a následné předávání informací o nich, je pro zákazníka nezbytné s ohledem na přijímání rozhodnutí týkajících se jeho dat vložených do služby cloud computingu. Zákazník si s poskytovatelem cloud computingu dohodne, které monitorované informace jej zajímají a jakým způsobem si o nich přeje být informován. Nástrojem pro sledování a vyhodnocování kybernetických bezpečnostních událostí se rozumí např. Security Information and Event Management (SIEM).

Řádek 9.2 pak nad rámec řádku 9.1 vyžaduje po poskytovateli cloud computingu umožnění vzdáleného přístupu k záznamům o kybernetických událostech týkajících se konkrétního

[9] Souhrnná analytická zpráva projektu eGovernment cloud schválená usnesením vlády České republiky ze dne 14. listopadu 2018 č. 749 o souhrnné analytické zprávě, výstupu Fáze I. projektu Příprava vybudování eGovernment cloudu.
[10] SOC for Service Organizations. *AICPA* [online]. Dostupné z: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html
[11] C5:2020, *BSI.* [online]. Dostupné z: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020.pdf

zákazníka. Nové kybernetické události pak zpřístupňuje zákazníkovi bez zbytečného odkladu tak, aby měl zákazník možnost na tyto události reagovat vhodnými opatřeními.

K řádku 9.3 a 9.4

Narušení bezpečnosti informací zákaznických dat a provozních údajů je závažným bezpečnostním incidentem, o kterém musí být zákazník periodicky informován tak, aby mohl přijmout adekvátní opatření.

Řádek 9.4 pak nad rámec řádku 9.3 vyžaduje, aby byl zákazník informován nikoliv periodicky, ale bez zbytečného odkladu.

K řádku 10.1

Penetrační testování a skeny zranitelností slouží jako nástroje zjištění a následného odstranění slabých míst v nabízené službě cloud computingu.

Z pohledu Národního úřadu pro kybernetickou a informační bezpečnost je klíčové, zda poskytovatel cloud computingu nabízený cloud computing pravidelně testuje a odstraňuje zjištěné zranitelnosti. Pro doložení je přijatelné předložení záznamu o provedení testu zranitelností na datové centrum/komerční balíček služeb a separátní připojení čestného prohlášení s výčtem služeb poskytovaných z daného datového centra obsaženého v komerčním balíčku služeb.

Sken zranitelností je pouze částí penetračního testu. Sken zranitelností nemůže nahradit komplexní penetrační test.

Záznamem se rozumí zpravidla výstup z nástrojů pro provádění skenů zranitelnosti, ze kterého bude patrné datum provedení skenu.

Skeny zranitelností lze považovat za podmnožinu penetračních testů, a proto požadavkem na záznam o provedení skenu zranitelnosti není překračován požadavek zákona o informačních systémech veřejné správy na předložení zpráv o provedení penetračních testů. V případě, že záznam obsahuje citlivé informace, lze takové informace ve zprávě neuvést/zakrýt (začernit). I v tom případě musí být patrné, že je to sken zranitelností či penetrační test.

K řádkům 10.2 a 10.3

Penetrační testování provedené subjektem nezávislým na poskytovateli cloud computingu podle mezinárodně uznávaných standardů umožní zákazníkovi ověřit zabezpečení poskytovaných služeb cloud computingu. Pro doložení je přijatelné předložení zprávy o penetračním testu na datacentrum nebo komerční balíček služeb a separátní připojení čestného prohlášení s výčtem služeb poskytovaných z daného datacentra. Problematika penetračních testů není jednoznačně zakotvena do jednoho široce akceptovaného standardu. V rámci jednání odborné skupiny připravující návrh vyhlášky proto byly identifikovány určité základní metodiky nebo základní zranitelnosti, ze kterých je třeba při provádění penetračního testu vycházet.

V případě, že zpráva obsahuje citlivé informace, lze takové informace ve zprávě neuvést/zakrýt (začernit). I v tom případě musí být patrné, že je to sken zranitelností či penetrační test.

Vzhledem k tomu, že neexistuje jeden celosvětově uznávaný standard obdobný ISO standardům pro provádění penetračních testů a vytváření záznamů o jejich provedení, což není s ohledem na smysl a povahu penetračních testů ani dobře možné, se za účelem sjednocení výstupů z penetračních testů a vyhodnocování takových výstupů v návrhu vyhlášky identifikují standardy využívané odbornou komunitou. Vedle standardů uvedených v návrhu vyhlášky a na odkazech níže, existuje řada dalších standardů, které však především pro svou přílišnou konkrétnost nebo naopak obecnost nebyly vyhodnoceny jako vhodné pro účel ex ante posuzování poskytovatelů cloud computingu.

Technical Guide to Information Security Testing and Assessment, NIST SP 800-115: https://csrc.nist.gov/publications/detail/sp/800-115/final

The Open Source Security Testing Methodology Manual (OSSTMM): https://www.isecom.org/OSSTMM.3.pdf ;https://www.isecom.org/research.html#content5-9d

OWASP Top ten web application security risks:https://owasp.org/www-project-top-ten/

K příloze č. 3

V současné době není v platnosti žádné akreditační schéma, na základě kterého by bylo možné akreditovat certifikační orgány, které by mohly následně certifikovat poskytovatele cloud computingu na jejich soulad s požadavky ISO/IEC 27017 a ISO/IEC 27018. Nejedná se tedy o samostatné certifikace ani o akreditované certifikáty. Návrhem vyhlášky je však požadováno, v odpovídajících bezpečnostních úrovních, přihlédnutí k požadavkům těchto norem při certifikačních, dozorových a recertifikačních auditech.

Vzhledem k tomu, že splnění požadavků certifikace se může v čase měnit, je platnost certifikace omezená na 3 roky, resp. každý rok se koná dozorový audit a jednou za 3 roky recertifikační audit (viz ISO/IEC 17021-1, kap. 9.1.3.2). Pro zajištění trvalého plnění požadavků certifikace a ověření tohoto plnění se stanovuje, že poskytovatel cloud computingu dodá každých 15 měsíců do evidence v katalogu cloud computingu auditní zprávu z dozorového, resp. recertifikačního auditu a spolu s tím doloží i stále platný certifikát. Dokládaná auditní zpráva nesmí být starší než 3 měsíce, aby se zaručilo, že je vždy předkládaná aktuální auditní zpráva. Vzhledem k tomu, že uvedené audity je třeba v daných periodách dle výše uvedené ISO normy provádět, nepředstavuje požadavek na pravidelné předkládání auditních zpráv, resp. certifikátů nijak zvýšený a zatěžující požadavek.

K příloze č. 4

Penetrační testování a skeny zranitelností slouží jako nástroje zjištění a následného odstranění slabých míst v nabízené službě cloud computingu.

Je klíčové, zda poskytovatel cloud computingu nabízenou službu cloud computingu pravidelně testuje a odstraňuje zjištěné zranitelnosti.

Požadavky na strukturu a náležitosti zprávy o provedení penetračního testu stanoví časové úseky, standardy a periodicitu v rozsahu dohodnutém na jednáních expertní skupiny.

K příloze č. 5

Struktura zprávy vychází z obecných principů auditní zprávy podle standardu ISO/IEC 20000 nebo ISO 22301. Alternativně je možné doložit auditní zprávu vyhotovenou subjektem nezávislým na poskytovateli cloud computingu, která obsahuje jasný a srozumitelný popis plánu zajištění kontinuity provozu nabízené služby cloud computingu a plánu na obnovu poskytování nabízeného cloud computingu po havárii, včetně popisu ověření jejich aplikace. Výčet zdrojů rizik vychází z Analýzy hrozeb pro ČR, která byla schválena usnesením vlády ČR ze dne 27. dubna 2016 č. 369. Riziko dlouhodobého sucha je relevantní zejména v případě využívání vody pro chlazení datacentra. Závažné narušení bezpečnosti komunikační sítě a ztráta integrity komunikační sítě je myšleno ve smyslu § 98 zákona č. 127/2005 Sb., o elektronických komunikacích.