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 bezpečnostních pravidlech pro využívání služeb cloud computingu orgány veřejné moci (dále jen „návrh vyhlášky“) usiluje o vytvoření přehledného a jednoduchého seznamu bezpečnostních pravidel pro poskytování služeb cloud computingu, jejichž dodržování budou orgány veřejné moci povinné zajistit, pokud budou chtít služby cloud computingu využívat.

Tato pravidla pokrývají celý životní cyklus služby cloud computingu od jejího pořízení, přes provoz, až po ukončení jejího využívání, a v jednotlivých oblastech dopadají na konkrétní oblasti, které je v rámci využívání služeb cloud computingu nutné zabezpečit tak, aby byla zajištěna dostatečná úroveň důvěrnosti, integrity a dostupnosti dat. Úprava bude mít pozitivní dopad na efektivitu ochrany kybernetického prostoru České republiky.

Návrh vyhlášky má za cíl provést § 6 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

Návrh vyhlášky současně reflektuje novelizaci[1] 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“). Zákon o informačních systémech veřejné správy byl mimo jiné proveden vyhláškou č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „vyhláška o vstupních kritériích“) v souvislosti s posuzováním poskytovatele služby cloud computingu (dále jen „poskytovatel“) a služeb cloud computingu využívaných orgány veřejné správy. Jejím cílem je vytvoření seznamu kritérií, jež musí být naplněna poskytovateli proto, aby mohli být zapsáni do katalogu cloud computingu. Z tohoto seznamu si budou orgány veřejné moci, které budou současně spadat pod působnost zákona o informačních systémech veřejné správy, vybírat poskytovatele nabízejícího službu cloud computingu, jež bude nejvíce odpovídat jejich potřebám a na niž budou aplikovat bezpečnostní pravidla upravená v návrhu vyhlášky. Množina orgánů veřejné moci, které pod působnost zákona o informačních systémech veřejné správy spadat nebudou, si bude moci vybírat služby cloud computingu z katalogu cloud computingu s tou výhodou, že poskytovatelé těchto služeb cloud computingu zapsaní v katalogu cloud computingu již deklarují, že umožní naplnění bezpečnostních pravidel podle návrhu vyhlášky.

[1] Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci.

Zákon o informačních systémech veřejné správy, zákon o kybernetické bezpečnosti a s nimi spojené relevantní prováděcí předpisy, upravují oprávnění a povinnosti, jež v souvislosti s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy spravovaných orgány veřejné moci celkově příznivě ovlivní jejich efektivitu, hospodárnost a v neposlední řadě i kybernetickou bezpečnost. Zákon o kybernetické bezpečnosti se zaměřuje na komplexní ošetření problematiky kybernetické bezpečnosti a bezpečnosti informací. V tomto ohledu se návrh vyhlášky zaměřuje pouze na konkrétní část předpisu, kterou provádí.

Cílem návrhu vyhlášky je zakotvit v právním řádu České republiky legislativní možnost pro vytvoření jednotného a systematického bezpečnostního základu v podobě seznamu bezpečnostních pravidel, který umožní bezpečné využívání služeb cloud computingu orgány veřejné moci. Nedostatečné zajištění kybernetické bezpečnosti v této oblasti může mít fatální dopady na fungování orgánů veřejné moci, což je z pozice České republiky nepřijatelné. Využívání služeb cloud computingu orgány veřejné moci s sebou nese potenciální rizika. Orgán veřejné moci svěřuje informace různé úrovně citlivosti poskytovateli, který s nimi pak v rámci poskytování služby cloud computingu nakládá. S ohledem na podstatu služeb cloud computingu často dochází k tomuto nakládání globálně a za účasti třetích stran. Orgán veřejné moci ztrácí nad informacemi část kontroly, kterou svěřuje do rukou poskytovatele. S ohledem na zachování důvěrnosti, integrity a dostupnosti informací je naprosto nezbytné, aby měl orgán veřejné moci k dispozici nástroje, které mu umožní nad informacemi vloženými do služby cloud computingu uplatňovat kontrolu.

Je tedy naprosto zásadní, aby orgán veřejné moci využívající služeb cloud computingu měl dostatek informací o tom, kde jsou jeho data uložena či zpracovávána, a to jak dlouhodobě, tak krátkodobě. Tyto informace pak poslouží k jeho úvaze, zdali je pro něj riziko zpracování dat pomocí konkrétní služby cloud computingu přijatelné, či nikoliv.

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., kterým se mění ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění ústavního zákona č. 347/1997 Sb., a ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky. 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 § 6 písm. e) zákona o kybernetické bezpečnosti. Návrh vyhlášky je v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). Tam kde vyhláška o kybernetické bezpečnosti řeší bezpečnost informací (tj. jejich důvěrnost, integritu a dostupnost) přímo ve správě organizace odpovědné za jejich bezpečnost, návrh vyhlášky doplňuje tuto úpravu o řešení bezpečnosti informací vložených do služby cloud computingu.

Povinnost orgánu veřejné moci zajistit dodržování bezpečnostních pravidel obsažených v návrhu vyhlášky tak nijak nezasahuje do povinnosti pro určené povinné osoby aplikovat bezpečnostní opatření ve smyslu § 4 odst. 2 zákona o kybernetické bezpečnosti, resp. bezpečnostní opatření obsažená ve vyhlášce o kybernetické bezpečnosti. Jinak řečeno i v případě, že správce informačního systému provozuje tento informační systém za využití služeb cloud computingu, musí zajistit zavedení a provádění bezpečnostních opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti.

Návrh vyhlášky stanoví obsah a rozsah bezpečnostních pravidel, jejichž naplnění umožní orgánům veřejné moci využívat služeb cloud computingu, 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 stanoví specifické požadavky státu jako zákazníka na služby cloud computingu, a jejich následné využití v rámci specifické množiny informačních systémů orgánů veřejné moci. Regulace 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 v České republice.

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")[2] 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.[3] 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.*"[4] Vymezení bezpečnostních zájmů a opatření k zajištění své vnitřní a vnější bezpečnosti pak náleží členským státům, což Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Úřad") v návrhu vyhlášky činí při specifikaci jednotlivých kritérií v dílčích dopadových oblastech úrovně dopadu „kritická".

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

[3] 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

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

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, 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 moci si následně zajistí další bezpečnostní opatření nad rámec směrnice NIS smluvně s DSP. S ohledem na povahu návrhu vyhlášky je možné konstatovat, že stát návrhem vyhlášky neukládá poskytovatelům nad rámec dotčené směrnice NIS další povinnosti, nýbrž stanoví další pravidla pro orgány veřejné moci, které mají zájem o využívání služeb 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 také ze závěrů strategických dokumentů týkajících se využívání služeb cloud computingu a regulování poskytování služeb cloud computingu. Zpracovatelé vzali v potaz závěry týkající se strategického významu služeb cloud computingu, digitální transformace, odstraňování překážek na vnitřním trhu či sjednocování legislativy. V tomto duchu návrh vyhlášky vychází z již využívaných technických předpisů, skutečného stavu nabízených služeb cloud computingu a zohledňuje i předpokládaný vývoj v oblasti unijních předpisů.

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[5] 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.[6] Návrh vyhlášky svým akcentem na bezpečnost a lokalizaci dat navíc vytváří příležitosti pro evropské poskytovatele, 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*.[7] V tomto duchu návrh vyhlášky vychází i z dalších již využívaných technických předpisů a skutečného stavu nabízených služeb cloud computingu.

d) Zhodnocení souladu navrhované právní úpravy se Zásadami pro tvorbu digitálně přívětivé legislativy

Návrh vyhlášky je v souladu se Zásadami pro tvorbu digitálně přívětivé legislativy.

e) 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.

f) 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.

---

[5] 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

[6] 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

[7] 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

g) 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.

h) 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. Nicméně s ohledem na předpokládanou možnost orgánů veřejné moci vkládat osobní údaje do systémů provozovaných za pomoci služeb cloud computingu bylo při tvorbě návrhu vyhlášky vycházeno z konzultací poskytnutých Úřadem pro ochranu osobních údajů k souvisejícím předpisům (novela zákona o informačních systémech veřejné správy a s ní související vyhláška o vstupních kritériích) tak, aby byla v maximální možné míře šetřena práva subjektů ochrany osobních 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) 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.

i) 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.

j) Zhodnocení dopadů na bezpečnost nebo obranu státu

Návrh vyhlášky má 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 moci, čímž dojde k posílení zabezpečení kybernetického prostoru České republiky jako takového.

k) Konzultace

Vyhláška byla tvořena Úřadem jako garantem kybernetické bezpečnosti ve spolupráci s dalšími subjekty. Návrh vyhlášky vychází z mezinárodně uznávaných standardů v oblasti bezpečnosti využívání služeb cloud computingu zejména Cloud Computing Compliance Criteria Catalogue – C5:2020 nebo norem ISO/IEC 27017.

Návrh vyhlášky vychází také mimo jiné z konzultací o návrhu vyhlášky o některých požadavcích pro zápis do katalogu cloud computingu v souvislosti s posuzováním poskytovatele a služeb cloud computingu využívaných orgány veřejné správy, která byla od roku 2018 průběžně konzultována v expertní skupině založené pro tento účel, jejímiž členy byli jak zástupci orgánů veřejné správy, tak zástupci odborné veřejnosti a budoucích poskytovatelů. Dne 1. 8. 2020 byl zveřejněn na internetových stránkách předkladatele věcný záměr návrhu vyhlášky k veřejným konzultacím a připomínkám.

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. Podle zákona o informačních systémech veřejné správy jím může být jak prodejce, tak i ten, kdo službu cloud computingu fakticky poskytuje.

Vzhledem k významu provozních údajů, jenž byl v minulosti dovozen soudní praxí,[8] 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 částí informací orgánu veřejné moci. 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 koncová zařízení nebo aplikace, jejichž běh je iniciován a nadále spojen s konkrétním uživatelem – fyzickou osobou využívající služby cloud computingu prostřednictvím nebo jménem orgánu veřejné moci.

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

Návrh vyhlášky pracuje s pojmem zpracování. To představuje využití zákaznických dat nebo provozních údajů v jejich elektronické podobě ať už jednotlivě nebo hromadně, v samostatných nebo v po sobě následujících řetězcích úkonů sloužících k dalším činnostem orgánu veřejné moci. Demonstrativní výčet těchto činností je obsažen v návrhu vyhlášky.

Návrh vyhlášky dále pracuje s pojmem subdodavatele. Subdodavatel a jeho dodávky mohou být významnou součástí poskytování služeb cloud computingu poskytovatelem. Jeho vliv na může být velmi významný zejména s ohledem na bezpečnost informací. Návrh vyhlášky tedy vyžaduje po poskytovatelích relevantní informace o jejich subdodavatelích. Zároveň s ohledem

[8] 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.

na zajištění bezpečnosti informací stanoví některá bezpečnostní pravidla vázající se právě na tyto subdodavatele.

Návrh vyhlášky rovněž definuje pojem technických aktiv, která bezprostředně zajišťují funkčnost služeb cloud computingu. Odtud logicky vyplývá, že selhání takového technického aktiva by mohlo mít nepříznivý dopad na poskytování konkrétní služby cloud computingu.

K § 3

Ustanovení § 3 odst. 1 stanovuje, že minimální požadavky pro využívání služby cloud computingu jsou stanoveny bezpečnostními pravidly pro příslušné bezpečnostní úrovně[9]. Z tohoto ustanovení vyplývá, že orgány veřejné moci mohou aplikovat i bezpečnostní pravidla určená pro vyšší bezpečnostní úrovně.

Ustanovení § 3 odst. 3 stanovuje, že u bezpečnostních pravidel, zařazených v příslušné bezpečnostní úrovni, musí být orgánem veřejné moci zajištěno jejich splnění, a to způsobem vyplývajícím ze znění konkrétního bezpečnostního pravidla či jiným doložitelným způsobem, který však prokazatelně zajistí stejnou nebo vyšší úroveň bezpečnosti. Při posouzení, zda jiný způsob splnění zajistí stejnou nebo vyšší úroveň bezpečnosti informací je nutné vyjít zejména z účelu konkrétního bezpečnostního pravidla. Orgán veřejné moci musí být schopen prokazatelně doložit, že jiný způsob splnění bezpečnostního pravidla zajistí stejnou nebo vyšší úroveň zabezpečení. Volba jiného způsobu splnění, než je uvedeno přímo v bezpečnostním pravidle, klade na orgán veřejné moci vyšší nároky a zároveň může představovat určitou nejistotu, zda jiný způsob splnění bezpečnostního pravidla bude kontrolním orgánem vyhodnocen jako dostatečný. I přesto je však na místě, s ohledem na různé služby cloud computingu, různé poskytovatele, a především rychlý technologický vývoj v oblasti cloud computingu, takovou alternativní možnost splnění připustit. Jelikož hlavním cílem návrhu vyhlášky je zajištění bezpečnosti informací, tak v případě, že v budoucnu budou dostupné i jiné možnosti (levnější, rychlejší, účinnější) k dosažení tohoto cíle než ty, které jsou uvedené v návrhu vyhlášky formou jednotlivých pravidel, je účelné je připustit. Připouští se tedy splnění jednotlivých pravidel i alternativními způsoby v návrhu vyhlášky neuvedenými. Zajištění stejné nebo vyšší úrovně bezpečnosti informací prostřednictvím jiného splnění bezpečnostního pravidla vyhodnocuje orgán veřejné moci a dále kontrolní orgán v rámci případné kontroly dodržování bezpečnostních pravidel při využívání služby cloud computingu orgánem veřejné moci.

K § 4

Ustanovení § 4 reaguje na změnu zákona o informačních systémech veřejné správy provedenou zákonem č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci, a upravuje případy, kdy orgán veřejné moci může využívat po stanovenou dobu službu cloud computingu u níž není povinen zajistit dodržování bezpečnostních pravidel obsažených v návrhu vyhlášky.

[9] Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.

K § 5

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

Zákonem č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci došlo k výraznému rozšíření regulace cloud computingu v České republice. Nová úprava zejména zákona o informačních systémech veřejné správy zavádí ucelený systém posuzování kvality a bezpečnosti využívání služeb cloud computingu orgány veřejné správy, přičemž bezpečnostní pravidla pro využívání služeb cloud computingu jsou jeho nedílnou součástí.

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 návrhu vyhlášky

V příloze návrhu vyhlášky (dále jen „Příloha“) se rozumí bezpečnostní úrovní cloud computingu bezpečnostní úroveň pro využívání cloud computingu orgány veřejné moci vyjadřující možné dopady kybernetického bezpečnostního incidentu na poptávaný cloud computing. Bezpečnostní úrovně jsou definovány vyhláškou č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.

Příloha obsahuje bezpečnostní pravidla (minimální bezpečnostní požadavky), jejichž naplnění musí orgán veřejné moci zajistit vždy, chce-li zvolenou službu cloud computingu využívat, vyjma výjimečných případů objektivní nesplnitelnosti, kterou však z povahy věci není třeba uvádět s ohledem na obecnou právní zásadu „nemožné nezavazuje“.

Bezpečnostní pravidla v Příloze jsou tematicky rozdělena do 15 oblastí tak, aby byl pokryt celý životní cyklus služby cloud computingu během jejího využívání orgánem veřejné moci.

K řádku 1

Oblast „*Obecné podmínky pro službu cloud computingu*“ stanovuje bezpečnostní pravidla, která upravují obecné podmínky pro využívání služby cloud computingu tak, aby byla zajištěna důvěrnost, integrita a dostupnost informací vložených do služby cloud computingu.

K řádku 1.1

Znalost polohy zpracování zákaznických dat a znalost rizik z toho vyplývajících, jsou nutným minimem. Je doporučené být seznámen s těmito informacemi i informacemi ohledně zpracování provozních údajů a specifických provozních údajů spojených s orgánem veřejné moci či zákaznickými daty. Aby nebylo pochyb, co se myslí polohou zpracování, využívá se poloha systémových komponent. Dostatečná je obecnější informace, zda je požadavek konkretizován na znalost všech míst, kam se mohou data dostat tak, aby byl orgán veřejné moci schopen vyhodnotit rizika, která plynou z daného umístění. Za přiměřené určení polohy lze považovat označení státu.

K řádku 1.2

Cílem bezpečnostního pravidla je zajistit posouzení rizikovosti případného předávání zákaznických dat a specifických provozních údajů cizozemským orgánům orgánem veřejné moci tak, aby orgán veřejné moci výsledky této analýzy mohl zohlednit během životního cyklu využití služby cloud computingu. Analýza by měla zohlednit to, jaká data se orgán veřejné moci rozhodne prostřednictvím služby cloud computingu zpracovávat, či zdali je vůbec vhodné konkrétní data službu cloud computingu pro zpracování dat orgánu veřejné moci využívat. Písemný záznam o provedení vyhodnocení rizik slouží k auditovatelnosti činnosti orgánu veřejné moci. Další bezpečnostní pravidla vztahující se k předávání dat cizozemským orgánům jsou upraveny v oblasti „*Žádosti cizozemských orgánů o zpřístupnění nebo předání dat*“ Přílohy.

K řádku 1.3

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

Za neaktivní data (data at rest) lze 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 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 neaktivní data byla vždy nepřetržitě dostupná i na území EU/ESVO a slouží tak k zajištění vyšší dostupnosti. Toto sousloví však nebrání tomu, aby k ukládání jiných dat než neaktivních dat (aktivní data, přenášená data), 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 regulace cloud computingu 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. Poskytovatel jasně službu cloud computingu označuje s tím, že neukládá neaktivní data na území EU/ESVO. Vyhláška nestanoví, kde by mělposkytovatel uvádět místo uložení zákaznických dat ve stavu neaktivních dat, s ohledem na výše zmiňovaný požadavek transparentnosti by se mělo jednat o snadno dostupnou informaci. Za vhodné lze tedy považovat uvedení informace na webových stránkách poskytovatele nebo ve smlouvě s orgánem veřejné moci o poskytnutí služby cloud computingu (dále jen „smlouva“).

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 bez ohledu na bezpečnostní úroveň brát v potaz požadavky vyplývající z regulace na úseku ochrany osobních údajů, pokud jsou do systému vloženy, zejména zajistit nezbytnou úroveň ochrany osobních údajů.

Ze znění pravidla pak také vyplývá, že v případě, že služba cloud computingu umožňuje volbu místa nepřetržitého a výlučného ukládání zákaznických dat, musí orgán veřejné moci zvolit takovou možnost, aby k nepřetržitému ukládání docházelo výlučně na území členských států EU/ESVO, a bylo tak zajištěno dodržení bezpečnostního pravidla.

K řádku 1.4

Odůvodnění bezpečnostního pravidla na zacházení se specifickými provozními údaji vychází z odůvodnění bezpečnostního pravidla 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.

K řádku 1.5

Bezpečnostní pravidlo, s ohledem na riziko přístupu cizích zpravidla státních orgánů, míří na zpracování zákaznických dat na území členských států EU/ESVO jako prostoru se sdílenými hodnotami a právními nástroji k ochraně a přístupu k datům. Zpracování mimo území EU/ESVO není zakázáno, je ale 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 podle předchozích řádků.

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

Bezpečnostní pravidlo týkající se zacházení se specifickými provozními údaji vychází z bezpečnostních pravidel na řádcích 1.4 a 1.5 Přílohy 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.

K řádku 1.7

V případě kritické bezpečnostní úrovně je na základě požadavků vyplývajících ze Souhrnné analytické zprávy[10] (dále jen „SAZ“) nutné ještě více omezit možné předávání dat mimo území České republiky a podmínit jej kontrolou orgánem veřejné moci nad tím, která data, v jakém rozsahu a za jakým účelem opustí území České republiky.

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. Lze však očekávat, že provoz služby cloud computingu bude záviset i na službách, u nichž by byla v případě úplného zákazu vývozu dat velmi omezena až znemožněna možnost jejich servisu. Zároveň se také nechce znemožnit ukládání některých dat mimo území České republiky např. v situacích ozbrojeného konfliktu a ztráty kontroly nad územím. Proto se ponechává možnost vyslovit souhlas s předáním a zpracováním dat i mimo Českou republiku.

[10]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.

Takový souhlas ale musí být výslovný, tedy nikoliv skrytý v rámci ostatních smluvních ustanovení, dostatečně odsazený a zdůrazněný od ostatního textu smlouvy, popřípadě může tvořit zcela samostatný dokument. Souhlas může být udělen jako generální před zahájením využívání cloud computingu nebo v každém jednotlivém případě. Zároveň i v případě vyslovení takového souhlasu nejsou nijak dotčena bezpečnostní pravidla upravená na řádcích 1.3 až 1.6 Přílohy.

K řádku 1.8

Konkrétní požadavky na dostupnost služby cloud computingu se značně liší pro každý jednotlivý případ využití služby cloud computingu. Je proto na orgánu veřejné moci, aby si stanovil jasně a srozumitelně požadavky na dostupnost služby cloud computingu podle svých potřeb.

Součástí smlouvy by mělo být i místo měření dostupnosti, kterým zpravidla bude peeringový uzel deklarovaný poskytovatelem nebo perimetr datacentra, ze kterého je služba cloud computingu poskytována.

K řádku 1.9

Pro bezpečnostní úroveň nízká je v souladu se zněním EUCS a vyhláškou o vstupních kritériích požadován alespoň soulad s certifikací ČSN EN ISO/IEC 27001, EN ISO ISO/IEC 27001 nebo ISO/IEC 27001. K ověření splnění tohoto bezpečnostního pravidla je vhodné od poskytovatele žádat alespoň čestné prohlášení, jehož součástí bude popis zavedených bezpečnostních opatření.

K řádku 1.10

Certifikace ISO/IEC 27001 představuje základní množinu požadavků týkajících se bezpečnosti informací, jejichž plnění by měl orgán veřejné moci požadovat po poskytovatelích cloud computingu alespoň v rozsahu využívané služby cloud computingu.

Požadavek na certifikace, resp. certifikace samotné, představují jediný způsob ověření splnění požadavků třetí stranou. Vzhledem k tomu, že splnění požadavků ověřených certifikací 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 souladu s tímto bezpečnostním pravidlem se tedy doporučuje orgánu veřejné moci průběžná kontrola platnosti certifikátů.

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

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

V případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě poskytovanou službu cloud computingu, musí poskytovaná služba cloud computingu spadat do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven.

K řádku 1.11

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 a vyšší požadována certifikace na ISO/IEC 27017.

K řádku 1.12

Certifikace ISO/IEC 27018 přináší specifikaci standardu ISO/IEC 27001 z hlediska ochrany osobních údajů a stanovuje dodatečná opatření pro poskytovatele. Orgány veřejné moci nemusí nezbytně nutně využívat služby cloud computingu ke zpracování osobních údajů, ale s ohledem na povahu činnosti orgánů veřejné moci lze zpracování osobních údajů spíše předpokládat, a proto je na místě zohlednění i výše zmíněných opatření směřujících na ochranu osobních údajů.

K řádku 1.13

Vzdálené přístupné prohlášení o aplikovatelnosti je dalším nástrojem umožňujícím orgánu veřejné moci soustavné ověřování souladu poskytované služby cloud computingu s deklarovanou úrovní zavedeného systému řízení bezpečnosti informací poskytovatele.

K řádku 1.14

Uložení sankcí, povinnost doplatit zbývající cenu plnění nebo propadnutí předplacené ceny v případě ukončení smlouvy, může negativně ovlivnit míru akceptace rizika orgánem veřejné moci pro bezpečnost informací (např. orgán veřejné moci si předplatí službu cloud computingu na 5 let a po prvním roce využívání služby cloud computingu se změní skutečný majitel poskytovatele za jiného, kterého by orgán veřejné moci považoval za rizikovějšího nebo by smlouvu na využívání služby cloud computingu ani neuzavřel z důvodu rizik pro bezpečnost informací plynoucích z osoby skutečného majitele). Z tohoto důvodu se definují situace související se schopností a možností poskytovatele poskytovat službu cloud computingu v parametrech umožňujících zajištění bezpečnosti informací, při kterých je možné odstoupit od smlouvy bez sankce. Každý z důvodů odstoupení od smlouvy je navíc podmíněn tím, že zároveň dojde ke zvýšení rizik z hlediska bezpečnosti informací u poskytovatele. Tuto podmínku je tak nezbytné splnit kumulativně vždy spolu s jednotlivým důvodem odstoupení pro odstoupení od smlouvy.

K jednotlivým důvodům pro odstoupení od smlouvy se uvádí:

a. Skutečný majitel jako osoba s rozhodujícím vlivem na fungování a provoz poskytovatele – jeho změna může zásadně ovlivnit přístup poskytovatele k bezpečnosti informací.

b. Změna sídla poskytovatele může vést ke změně jurisdikce, do které spadá poskytování služby cloud computingu a ke zvýšení rizik z toho vyplývajících.

c. Úřad může za určitých okolností stanovených zákonem omezit využívání dodávek či přímo konkrétního dodavatele. Za těchto okolností je pak nutné případně přistoupit i k odstoupení od smlouvy.

d. Důvod, pro který dojde k výmazu poskytovatele z katalogu cloud computingu, tedy ke ztrátě způsobilosti poskytovatele z hlediska zajištění důvěrnosti, dostupnosti nebo integrity informací, nebo z hlediska bezpečnosti, veřejného pořádku a dodržování práv třetích osob, bude zpravidla souviset s riziky pro bezpečnost informací.

e. Subdodavatel (dodavatel s vlivem na bezpečnost informací služby cloud computingu) může ovlivnit bezpečnost informací. Je na místě, aby orgán veřejné moci o této změně věděl a mohl využívání služby cloud computingu bez sankce ukončit. Konkrétní forma souhlasu může být upravená ve smlouvě o poskytování služby cloud computingu mezi orgánem veřejné moci a poskytovatelem.

f. Podobně jako změna subdodavatele může být negativně ovlivněna bezpečnost informací služby cloud computingu v případě, kdy klíčové prvky systému např. převede poskytovatel na jiného subdodavatele.

g. Přímo občanský zákoník uvádí možnost odstoupení od smlouvy poruší-li strana smlouvu podstatným způsobem.

h. Vedle změn subdodavatele a změn v kontrole nad technickým aktivem může dojít i k jiné změně, která může mít vliv na bezpečnost informací služby cloud computingu.

Smlouva je zcela zásadním a klíčovým nástrojem orgánu veřejné moci k prosazování bezpečnostních pravidel a jejich dodržování. Je nezbytné klást při její tvorbě a podpisu důraz na kvalitu, aby ve smlouvě byly zohledněny všechny relevantní požadavky vyplývající z bezpečnostních pravidel a dalších předpisů.

Služby cloud computingu a s nimi spojené smlouvy bývají často multi-tenantní, tj. jsou uzavírány ve stejném znění s velkým množstvím zákazníků. Ochota poskytovatelů smlouvy měnit nemusí být velká, je tedy nutné již při výběru poskytovatele dbát na to, aby jím předložená smlouva naplňovala výše řečené, či si vybrat poskytovatele, který je ochoten smlouvu měnit.

K řádku 2

Oblast „Organizace bezpečnosti informací“ stanovuje bezpečnostní pravidla, jejichž cílem je zajištění řádného plánování, implementace, údržby a neustálého zlepšování rámce bezpečnosti informací v rámci organizace poskytovatele služby cloud computingu.

K řádku 2.1

Systém řízení bezpečnosti informací je základním požadavkem vycházejícím z bezpečnostních pravidel upravených na řádku 1.9 a 1.10 Přílohy. Rozsah systému řízení bezpečnosti informací pak musí orgán veřejné moci ověřit tak, aby odpovídal rozsahu poskytované služby cloud computingu zejména v oblasti organizačních jednotek, lokalit a procesů sloužících k zabezpečení jejího provozu.

K řádku 2.2

Politika bezpečnosti informací je nástrojem k prosazení bezpečnostního pravidla upraveného na řádku 2.1 Přílohy. Orgán veřejné moci by měl ověřit její aktuálnost a její reálnou implementaci v rámci systému řízení bezpečnosti informací poskytovatelem.

K řádku 2.3

Zavádění bezpečnostních opatření je logickým důsledkem aplikace bezpečnostních pravidel upravených na řádcích 2.1 a 2.2 Přílohy. Orgán veřejné moci si ověří (např. pomocí prohlášení o aplikovatelnosti – řádek 1.13 Přílohy), že poskytovatel zavádí s ohledem na svůj systém řízení bezpečnosti informací a svou politiku bezpečnosti informací bezpečnostní opatření sloužící k navýšení bezpečnosti informací.

K řádku 3

Oblast „Politiky“ stanovuje bezpečnostní pravidla, jejichž cílem je zajištění existence politik bezpečnosti informací u poskytovatele služby cloud computingu, jako jednoho z nástrojů systému řízení bezpečnosti informací, a zajištění souladu těchto politik s požadavky orgánu veřejné moci na bezpečnost informací.

K řádku 3.1

Orgán veřejné moci může využívat pouze takovou službu cloud computingu, jejíž poskytování se řídí politikou bezpečnosti informací, která je v souladu s požadavky orgánu veřejné moci na bezpečnost informací. Je málo pravděpodobné, že by poskytovatelé upravovali své politiky bezpečnosti informací podle požadavků jednotlivých orgánů veřejné moci. Dané ustanovení vyžaduje, aby orgán veřejné moci poptával a využíval pouze službu cloud computingu, jejíž politika je v souladu s jeho požadavky na bezpečnost informací.

K řádku 4

Oblast „Fyzická bezpečnost“ stanovuje bezpečnostní pravidla, která upravují zajištění fyzické bezpečnosti, ochranu před krádeží, poškozením, ztrátou a výpadkem provozu technických aktiv, případně zákaznických dat.

K řádku 4.1

Bezpečnost informací při poskytování služby cloud computingu je nutné zajistit i vhodnými bezpečnostními opatřeními sloužícími k fyzické ochraně datových center, tak, aby byla chráněna před vnějšími vlivy. Aplikovaná bezpečnostní opatření mají za cíl bránit především důsledkům přírodních katastrof, úmyslnému poškození lidskou činností, např. teroristickými útoky, a důsledkům havárií v prostorách datových center. Tento požadavek je zaměřen na spolehlivou ochranu samotných datacenter a všech jejích součástí obsahujících relevantní technická aktiva.

Zároveň pravidlo je třeba aplikovat přiměřeně s ohledem na to, co je v odpovědnosti a možnostech poskytovatele.

K řádku 4.2

Pro zachování kontinuity poskytování služby cloud computingu a zajištění její dostatečné dostupnosti je nezbytné, aby orgán veřejné moci využíval služeb poskytovatele schopného 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 musí mít alespoň dvě datacentra, kdy obě jsou dostatečně kapacitní k převzetí služeb druhého datacentra.

K řádku 4.3

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.

Za tím účelem je potřeba, aby orgán veřejné moci využíval služeb cloud computingu poskytovaných z datacenter, které jsou v dostatečné vzdálenosti od přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací, případně jsou přijata adekvátní bezpečnostní opatření, nebo alternativně využíval datacentra ve vzájemné vzdálenosti 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.

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

K řádku 4.4

Pro zajištění bezpečnosti informací je potřeba, aby orgán veřejné moci využíval služeb cloud computingu poskytovaných z budov a prostor (viz odůvodnění k řádku 4.1) u nichž je zajištěno adekvátními bezpečnostními opatřeními zabránění přístupům a zásahům, které by mohly vést ke snížení úrovně bezpečnosti informací.

K řádku 5

Oblast „Zajištění provozu služby cloud computingu“ stanovuje bezpečnostní pravidla, která upravují zajištění řádného provozu služeb. K naplnění tohoto cíle jsou stanovena vhodná opatření pro plánování a monitorování kapacit zdrojů na straně poskytovatele, ochrana před škodlivým kódem, zaznamenávání a monitorování událostí a řešení zranitelností, poruch a chyb.

K řádku 5.1

Smluvní zakotvení je zcela zásadní pro určení způsobu zpracování zákaznického obsahu. Případné změny ve způsobu zpracovávání je nutné smluvně ošetřit, případně je možné rovnou zakotvit do smlouvy proces, kterým bude možné způsoby zpracování zákaznického obsahu rozšiřovat či zužovat.

K řádku 5.2

Orgán veřejné moci průběžně vyhodnocuje informace a podklady týkající se zranitelností a hrozeb využívané služby cloud computingu. U přijatých bezpečnostních opatření ověřuje a vyhodnocuje jejich účinnost.

K řádku 5.3

Sdílené fyzické a virtuální zdroje zahrnují operační paměti, výpočetní jádra a sítě sloužící pro připojení externích zařízení k serverům (storage area network). K oddělení zákaznických dat je možné využít například firewally, seznamy pro řízení přístupů (accsses control lists), štítkování (tagging), zřízení virtuálních lokálních sítí (VLAN), virtualizace či opatření v sítích sloužících pro připojení externích zařízení k serverům (storage area network, SAN).

K řádku 5.4

Orgán veřejné moci musí využívat takovou službu cloud computingu, která umožňuje ochranu dat zálohováním. K určení dostatečné vzdálenosti lze obdobně využít bezpečnostní pravidlo upravené na řádku 4.3 Přílohy.

Šifrování je jedním z nástrojů zvýšení ochrany důvěrnosti dat, který omezuje neoprávněný přístup k zákaznickým datům jak ze strany administrátorů poskytovatele, uživatelů s nedostatečným oprávněním, tak osob s nekalými úmysly. Proto se stanovuje povinnost zákaznická data 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. Vedle doporučených algoritmů však mohou existovat i jiné, novější, účinnější, které nebyly zahrnuty do doporučení. Konečné řešení o využití konkrétního algoritmu je pak volbou orgánu veřejné moci.

K řádku 5.5

Shromažďování provozních údajů a jejich náležitosti je nezbytné pro zaznamenávání událostí, které se v informačních a komunikačních systémech udály, stejně tak je to důležité i při využití služby cloud computingu k provozu informačního systému. Bezpečnostní pravidlo v tomto směru předepisuje minimální rozsah těchto záznamů, a to jak z pohledu událostí, které je nutné zaznamenat (např. činnosti vyžadující privilegovaná oprávnění, kritická chybová hlášení atd.), tak i s ohledem na to, jaké podrobnosti musí být zaznamenány (např. datum a čas, typ činnosti, identifikace účtů a původců atp.).

Požadavek na zaznamenávání provozních údajů a jejich náležitostí je zde uveden z důvodu, že událost může být důležitá například při vyhodnocování nebo vyšetřování útoku či kybernetického bezpečnostního incidentu. Neobvyklé provozní události jsou pak indiciemi toho, že se systém nebo služba cloud computingu nechová standardním způsobem.

K řádku 5.6

Monitoring událostí, jejich zaznamenávání, vyhodnocování a následné zpřístupňování jsou pro orgán veřejné moci nezbytné s ohledem na přijímání rozhodnutí týkajících se jeho dat vložených do služby cloud computingu. Orgán veřejné moci si s poskytovatelem dohodne, které monitorované informace jej zajímají a jakým způsobem mu budou zpřístupněny. Nástrojem pro sledování a vyhodnocování kybernetických bezpečnostních událostí se rozumí např. Security Information and Event Management (SIEM).

K řádku 5.7

Všechny zaznamenané provozní údaje je nutné po určitou dobu uchovávat (některé kybernetické bezpečnostní incidenty jsou detekovány až v korelaci určitých událostí v čase). Doba, po kterou je nutné mít záznamy uchované, je pro bezpečnostní úroveň „vysoká“ 12 měsíců.

Důvod, proč je doba nastavena takto, je zejména zkušenost předkladatele a také skutečnost, že střední doba detekce incidentu v regionu EMEA (Europe Middle East And Africa) je 24 měsíců. To znamená, že v případěkybernetického bezpečnostního incidentu, trvá organizaci 24 měsíců, než zjistí, že se u ní vůbec incident stal. Při vyšetřování takového incidentu je pak zcela klíčové, zda jsou tyto záznamy k dispozici či nikoliv. Hodnotou 12 měsíců se zvyšuje šance na zajištění potřebných důkazů k případnému šetření a analyzování incidentů. Stanovené období, po které mají být logy uchovávány, se ale vztahuje pouze na logy týkající se bezpečnosti informací, tedy logy související s důvěrností, dostupností a integritou informací.

K řádku 5.8

Všechny zaznamenané provozní údaje je nutné po určitou dobu uchovávat (některé kybernetické bezpečnostní incidenty jsou detekovány až v korelaci určitých událostí v čase). Doba, po kterou je nutné mít záznamy uchované, je pro bezpečnostní úroveň „kritická“ 18 měsíců.

Důvod, proč je doba nastavena takto, je zejména zkušenost předkladatele a také skutečnost, že střední doba detekce incidentu v regionu EMEA (Europe Middle East And Africa) je 24 měsíců. To znamená, že v případě kybernetického bezpečnostního incidentu, trvá organizaci 24 měsíců, než zjistí, že se u ní vůbec incident stal. Při vyšetřování takového incidentu je pak zcela klíčové, zda jsou tyto záznamy k dispozici či nikoliv. Hodnotou 18 měsíců se zvyšuje šance na zajištění potřebných důkazů k případnému šetření a analyzování incidentů. Stanovené období, po které mají být logy uchovávány, se ale vztahuje pouze na logy týkající se bezpečnosti informací, tedy logy související s důvěrností, dostupností a integritou informací.

K řádku 5.9

Orgán veřejné moci využije takovou službu cloud computingu, která mu umožní zajistit splnění bezpečnostních pravidel. Správná forma ukládání a ochrana uložených provozních údajů je nezbytná k umožnění naplnění bezpečnostního pravidla upraveného na řádku 5.10 Přílohy. Vhodnou formu ukládání si dohodne orgán veřejné moci s poskytovatelem. Zajištění neměnnosti provozních údajů je pro případné vyšetřování kybernetických bezpečnostních incidentů klíčové, aby bylo možné zjistit přesně průběh událostí a bylo zabráněno jejich změně za účelem zahlazení stop.

K řádku 5.10

Monitoring provozních údajů, jejich zaznamenávání, vyhodnocování a následné zpřístupňování, je pro orgán veřejné moci nezbytné s ohledem na přijímání rozhodnutí týkajících se jeho dat vložených do služby cloud computingu. Orgán veřejné moci si s poskytovatelem dohodne, které provozní údaje jej zajímají, jakým způsobem, v jakém formátu a v jakém časovém horizontu či intervalu mu budou zpřístupněny.

K řádku 6

Oblast „Správa identit a řízení přístupu“ stanovuje bezpečnostní pravidla, která upravují zavedení a dodržování vhodných postupů v oblasti autorizace a autentizace přístupů uživatelů ke službě cloud computingu jak na straně poskytovatele, tak na straně orgánu veřejné moci tak, aby se zabránilo neoprávněným přístupům ke službě cloud computingu. Důraz je pak kladen především na účty uživatelů s privilegovanými přístupovými oprávněními, u kterých je v případě neoprávněného přístupu ke službě cloud computingu větší riziko narušení bezpečnosti informací orgánu veřejné moci.

K řádku 6.1

Orgán veřejné moci musí využívat pro přístup do správy služby cloud computingu vícefaktorovou autentizaci s nejméně dvěma různými typy faktorů. Tento způsob je z pohledu bezpečnosti v současné době nejvhodnější. V případě dvou faktorů funguje tak, že daná entita, která se autentizuje do systému, musí znát např. heslo a dále musí pro úspěšnou autentizaci mít k dispozici i druhý faktor, např. token.

K řádku 6.2

Za účelem řízení přístupu k službě cloud computingu a jednoznačnému určení vykonavatele operace v této službě, je požadavkem této regulace správa životního cyklu identit a přístupových oprávnění uživatelů a administrátorů.

V souladu s nejlepšími praktikami (ISO/IEC 27002) musí být přístupová práva a oprávnění uživatelům a administrátorům služby cloud computingu přidělována pouze v rozsahu nezbytném pro výkon činností vyplývajících z popisu pracovního místa či smluvního ujednání. Důležité je z tohoto pravidla neudělovat žádné výjimky. Nezbytná je i pravidelná kontrola přidělených identit a přístupových oprávnění a odebírání nebo změna přístupových oprávnění při změně pracovní pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role. Stejný požadavek je i v případě ukončení nebo změny smluvního vztahu. Důvodem je ochrana zákaznických dat a specifických provozních údajů před jejich kompromitací a zneužitím.

Orgán veřejné moci musí pro řízení přístupu k informačnímu a komunikačnímu systému všem přidělit jedinečné identifikátory z důvodu jednoznačného stanovení vykonavatele události.

K řádku 6.3

Orgán veřejné moci využívá pouze takovou službu cloud computingu, jejíž poskytovatel řídí přístupy k informačnímu systému využívanému k jejímu poskytování. Odůvodnění k pravidlu upravenému na řádku 6.2 Přílohy se využije obdobně.

K řádku 6.4

Dohody o mlčenlivosti a důvěrnosti mezi poskytovatelem a jeho zaměstnanci, externími pracovníky a subdodavateli by měly obsahovat zejména ustanovení o tom:

- které informace jsou důvěrné;
- na jakou dobu se dohoda uzavírá;
- jak postupovat po skončení trvání dohody;
- jak je řízen pohyb a oběh důvěrné informace;
- jak postupovat v případě sdílení důvěrné informace s dalšími stranami, pokud je to nezbytné;
- jaké jsou důsledky porušení dohody.

K řádku 6.5

Orgán veřejné moci využívá pouze takovou službu cloud computingu, jejíž poskytovatel řídí přístupy k informačnímu systému využívanému k jejímu poskytování. Odůvodnění k pravidlu upravenému na řádku 6.2 Přílohy se využije obdobně.

Poskytovatel musí při řízení přístupu k informačnímu a komunikačnímu systému všem přidělit jedinečné identifikátory z důvodu jednoznačného stanovení vykonavatele události.

Princip nutnosti vědět (need-to-know principle) zdůrazňuje striktní přidělování přístupových oprávnění pouze těm administrátorům na straně poskytovatele, kteří skutečně potřebují mít k výkonu správy služby cloud computingu přístup zřízen, a to pouze na dobu, kdy tato potřeba trvá.

K řádku 6.6

V případě úrovně „kritická“ je nutné posílit kontrolu nad přístupem zaměstnanců nebo externích pracovníků poskytovatele k zákaznickým datům nebo specifickým provozním údajům, které nejsou šifrovány nebo byly dešifrovány nad rámec běžného řízení přístupu.

Je vyžadován informovaný souhlas orgánu veřejné moci s každým jednotlivým přístupem. Lze doporučit, aby byl tento souhlas udělován v auditovatelné formě.

K řádku 7

Oblast „Správa klíčů a šifrování“ stanovuje bezpečnostní pravidla, která upravují vhodné a efektivní využívání šifrovacích metod a postupů k zajištění důvěrnosti a integrity a dostupnosti informací vložených do služby cloud computingu.

K řádku 7.1

Šifrování je jedním z nástrojů zvýšení ochrany důvěrnosti dat k omezení neoprávněného přístupu k těmto datům jak ze strany administrátorů poskytovatele cloud computingu, uživatelů s nedostatečným oprávněním, tak osob s nekalými úmysly. Proto se stanovuje povinnost data orgánů veřejné moci šifrovat. Obzvláště kritický je pak přenos dat po sítích mimo prostory datacenter, kdy k jednotlivým síťovým prvkům, ať už na trase do jiného datacentra nebo k orgánu veřejné moci, mohou přistupovat osoby nepověřené poskytovatelem nebo orgánem veřejné moci.

K řádku 7.2

Šifrování je jedním z nástrojů zvýšení ochrany důvěrnosti dat k omezení neoprávněného přístupu k těmto datům jak ze strany administrátorů poskytovatele cloud computingu, uživatelů s nedostatečným oprávněním, tak osob s nekalými úmysly. Proto se stanovuje povinnost data orgánů veřejné moci šifrovat.

Místo, kde jsou trvale uložena zákaznická data je rizikové vzhledem k tomu, že se data na daném místě koncentrují a mohou se uchovávat trvale i po odpojení napájení a jsou tedy vystavena riziku případného fyzického transportu neoprávněnými osobami.

K řádku 7.3

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. Vedle doporučených algoritmů však mohou existovat i jiné, novější, účinnější, které nebyly zahrnuty do doporučení. Konečné řešení o využití konkrétního algoritmu je pak volbou orgánu veřejné moci učiněnou zpravidla výběrem konkrétního poskytovatele.

K řádku 8

Oblast „Zabezpečení komunikace“ stanovuje bezpečnostní pravidla, jejichž cílem je zajištění bezpečnosti informací orgánu veřejné moci při jejich přenosu přes komunikační sítě a zajištění odolnosti těchto sítí.

K řádku 8.1

Vzhledem k tomu, že služby cloud computingu jsou poskytovány vzdáleně, mohou být obzvláště citlivé na útoky typu DoS/DDoS. Orgán veřejné moci musí proto využívat při využití služby cloud computingu nástroje nebo služby pro zvýšení odolnosti vůči útokům typu odepření služby (DoS/DDoS).

K řádku 8.2

Ochrana datových přenosů do a ze služby cloud computingu proti neoprávněnému zásahu, kopírování, úpravě, přesměrování nebo vymazání může být zajištěna například šifrováním v souladu s pravidlem upraveným na řádku 7.3 Přílohy.

K řádku 8.3

Ochrana datových přenosů do a ze služby cloud computingu proti neoprávněnému zásahu, kopírování, úpravě, přesměrování nebo vymazání může být zajištěna například šifrováním v souladu s pravidly upravenými na řádcích 7.1 a 7.3 Přílohy.

K řádku 8.4

Dalším z opatření pro zajištění vyšší dostupnosti služby cloud computingu je požadavek na to, aby orgán veřejné moci využil takovou službu cloud computingu, jejíž poskytovatel má zajištěno připojení 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 orgán veřejné moci.

K řádku 9

Oblast „Přenositelnost, propojení a exit strategie“ stanovuje bezpečnostní pravidla pro několik situací, které v životním cyklu služby cloud computingu mohou zpravidla nastat. Zejména je nutné, aby byl umožněn přístup ke službám cloud computingu skrze jiné cloudové služby či jiné IT systémy orgánu veřejné moci.

Orgán veřejné moci má povinnost vytvořit plán pro ukončení využívání služby (exit strategii), který následně musí zohlednit ve smluvních vztazích o poskytování služeb cloud computingu. Dále také bezpečnostní pravidla cílí na to, aby měl orgán veřejné moci možnost získat data vložená do služby cloud computingu po skončení smluvního vztahu s poskytovatelem a aby došlo k výmazu zákaznických dat po ukončení smluvního vztahu.

K řádku 9.1

Držení dat a schopnost s nimi nakládat bude zpravidla klíčová pro zajištění kontinuity služby poskytované informačním systémem, pro který je služba cloud computingu využívána.

Je proto vhodné si formát a rozsah zákaznických dat a provozních údajů, které se mají předávat vždy sjednat.

K řádku 9.2

Při využívání služby cloud computingu je orgán veřejné moci do veliké míry závislý na poskytovateli. Plán pro ukončení využívání služby je nástrojem, který má zajistit, aby při ukončení využívání služby nedošlo k diskontinuitě jejího provozu.

Propracovanost exit strategie by měla být úměrná k bezpečnostní úrovni (nízká, středná, vysoká, kritická), pro kterou je služba cloud computingu vytvořena.

Jedním z nejčastějších cílů exit strategie bude co nejmenší omezení dostupnosti, zachování kontinuity a kvality služby cloud computingu.

K řádku 9.3

Orgán veřejné moci má povinnost vytvořit plán pro ukončení využívání služby (exit strategii), který následně musí zohlednit ve smlouvě o poskytování služby cloud computingu. Viz také odůvodnění k pravidlu upravenému na řádku 1.14 Přílohy. Smlouva zohlední takové požadavky orgánu veřejné moci na exit strategii, které lze specifikovat v době uzavření smlouvy.

K řádku 9.4

V rámci zajištění kontinuity a s ohledem na rozsah dat zpracovávaných za využití služby cloud computingu je třeba, aby bylo možné vkládat a zejména vyjmout všechna vložená zákaznická data standardizovaným způsobem přes definovaná a dokumentovaná rozhraní, na která se může orgán veřejné moci nebo jiný poskytovatel určený orgánem veřejné moci napojit. Takové napojení umožnuje automatizovaný a rychlý přenos dat a podporuje kontinuitu služby cloud computingu poskytovanou k zajištění provozu informačního systému orgánu veřejné moci.

K řádku 9.5

Typ a rozsah dat a podmínek jejich předávání závisí mimo jiné na třídě cloud computingu.

V případě třídy cloud computingu IaaS a PaaS je orgán veřejné moci zpravidla zodpovědný za zálohování a vynětí dat, která jsou vložena do služby cloud computingu, před ukončením smluvního vztahu.

Odpovědnost poskytovatele je limitována poskytnutím dat nutných k nastavení (např. konfiguraci sítí, obrazů či virtuálních zařízení) infrastruktury nebo platformy, kterou orgán veřejné moci využívá v rámci prostředí poskytovatele.

V případě třídy cloud computingu SaaS orgán veřejné moci bude zpravidla spoléhat na funkce exportu zákaznických dat, který mu poskytne poskytovatel. Zákaznická data vytvořená orgánem veřejné moci by měla být dostupná ve stejném formátu v jakém jsou uložena ve službě cloud computingu. Specifická provozní data by měla být dostupná v aplikovatelných standardních formátech (např. CSV, JSON, XML).

K řádku 9.6

Využívání služby cloud computingu nesmí vést ke ztrátě vlastnických práv k zákaznickým datům. Nejsou tím vyloučeny případy využívání zákaznických dat ze strany poskytovatele na základě smluvního ujednání s orgánem veřejné moci.

K řádku 9.7

Relevantním regulatorním požadavkem je pro povinné osoby podle zákona o kybernetické bezpečnosti Příloha č. 4 vyhlášky o kybernetické bezpečnosti.

Za relevantní právní požadavek lze považovat pro ostatní případy ustanovení smlouvy o poskytování služby cloud computingu.

K řádku 10

Oblast „Nákup, vývoj a úprava informačních systémů“ stanovuje bezpečnostní pravidla, jejichž cílem je nastavení vhodných postupů a procesů k zajištění bezpečnosti informací ve vývojovém cyklu služeb cloud computingu. Jde zejména o opatření zajišťující proces řízení změn a oddělení testovacího a vývojového prostředí od produkčního prostředí tak, aby se zachovala bezpečnost informací orgánu veřejné moci a aby bylo zajištěno plynulé poskytování služby cloud computingu.

K řádku 10.1

Za účelem ochrany provozního prostředí, a v něm umístěných dat před ohrožením vývojovými a testovacími činnostmi, se stanoví povinnost oddělení provozního prostředí od testovacího a vývojového prostředí. Omezení stanovené pravidlem míří na činnosti prováděné poskytovatele, nikterak však neomezuje činnosti vykonávané zákazníkem. To nijak neomezuje povinnost uvedenou v § 10 odst. 3 vyhlášky o kybernetické bezpečnosti.

K řádku 10.2

Dostatečným předstihem se rozumí takový předstih, který orgánu veřejné moci umožní provést zhodnocení rizik spojených se změnou a případně zavést opatření vedoucí ke snížení rizik předtím, než je změna zavedena.

Způsob informování by měl být upravený ve smlouvě o poskytování cloud computingu.

K řádku 11

Oblast „Řízení dodavatelů“ stanovuje bezpečnostní pravidla, jejichž cílem je nastavení vhodných postupů a procesů k zajištění bezpečnosti informací orgánu veřejné moci při řetězení dodavatelů služby cloud computingu. Jedná se o opatření zajišťující funkční procesy řízení subdodavatelů a opatření zajišťující přijatelnou míru kontroly orgánu veřejné moci nad tím, jací subdodavatelé poskytovatele budou zpracovávat jeho data.

K řádku 11.1

Dostatečným předstihem se rozumí takový předstih, který orgánu veřejné moci umožní provést zhodnocení rizik spojených se změnou subdodavatele a případně zavést opatření vedoucí ke snížení rizik předtím, než je změna provedena.

K řádků 12

Oblast „Správa kybernetických bezpečnostních událostí a incidentů“ stanovuje bezpečnostní pravidla, jejichž cílem je nastavení vhodných opatření k zajištění konzistentního a komplexního přístupu k zaznamenávání, hodnocení, komunikaci a řešení kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů ve službě cloud computingu. Důraz je kladen zejména na zajištění informování orgánu veřejné moci o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech tak, aby mohl včas přijmout potřebná opatření.

K řádku 12.1

Narušení bezpečnosti informací zákaznických dat a specifických provozních údajů je závažným bezpečnostním incidentem, o kterém musí být orgán veřejné moci informován bez zbytečného odkladu tak, aby mohl přijmout adekvátní opatření. Pro zhodnocení účinnosti přijatého opatření má být orgán veřejné moci informován.

Čas 72 hodin byl zvolen s ohledem na článek 33 GDPR, který stanoví lhůtu pro hlášení incidentů dozorovému úřadu.

K řádku 12.2

Monitoring bezpečnostních událostí, jejich vyhodnocování a následné předávání informací o nich je pro orgán veřejné moci nezbytné s ohledem na přijímání rozhodnutí týkajících se jeho dat vložených do služby cloud computingu. Orgán veřejné moci si s poskytovatelem 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).

K řádku 13

Oblast „Řízení kontinuity činností“ stanovuje bezpečnostní pravidla, jejichž cílem je nastavení vhodných opatření k zajištění kontinuity poskytování služby cloud computingu a zajištění kontinuity činností orgánu veřejné moci závislých na poskytovaných službách cloud computingu.

K řádku 13.1

Plán kontinuity činností je klíčovým dokumentem pro zachování kontinuity služby. Propracovanost plánu kontinuity činností by měla být úměrná k bezpečnostní úrovni (nízká, středná, vysoká, kritická) služby cloud computingu, pro kterou je plán vytvořen.

Současně s tím by měl plán kontinuity činností zohlednit povinnosti vyplývající z bezpečnostních pravidel upravených v oddílu 9 Přílohy.

K řádku 14

Oblast „Soulad s předpisy a audit“ stanovuje bezpečnostní pravidla, jejichž cílem je zajištění souladu činností poskytovatele s regulatorními a smluvními požadavky dopadajícími na činnosti spjaté s poskytováním služeb cloud computingu.

K řádku 14.1

Orgán veřejné moci využije takovou službu cloud computingu, jejíž poskytovatel k zajištění souladu s požadavky vyplývajícími z právních předpisů a smluv jednoznačně identifikuje, dokumentuje a udržuje aktuální veškeré relevantní povinnosti vyplývající pro něj z právních předpisů a smluvních požadavků.

Porušování právních předpisů poskytovatelem lze označit za bezpečnostní riziko pro orgán veřejné moci.

Za relevantní právní předpisy lze například považovat GDPR, zákon o kybernetické bezpečnosti, vyhlášku o kybernetické bezpečnosti, zákon o informačních systémech veřejné správy a jiné.

Za relevantní smluvní požadavky lze označit například soulad s požadovanými certifikacemi.

K řádku 14.2

Požadavek slouží k ověření dodržování bezpečnostních pravidel, jejichž plnění je přeneseno na poskytovatele.

Zároveň je záměrem uvedeného ustanovení vyjádřit obecně platnou zásadu, že kontrolní oprávnění nelze zneužívat a aplikovat šikanózně.

Předkladatel a poskytovatel se vzájemně předem dohodnou na rozsahu, datu, době trvání, požadavcích na kontrolu a požadovaných podkladech, ledaže by tento požadavek na vzájemnou dohodu umožňoval poskytovateli bezdůvodně zdržovat průběh šetření. Kontrola na místě nebo na 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.

Kontrolní práva poskytované předkladateli 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, předložením dokumentace či jiných podkladů připravených orgánem veřejné moci či poskytovatelem předem pro kontrolní účely, včetně kontroly ze strany předkladatele, 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, která je pověřena vedením šetřených prostor poskytovatele.

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

- Předkladatel nebude oprávněn přistupovat k jakýmkoliv datům patřícím orgánu veřejné moci nebo poskytovateli bez souhlasu daného orgánu veřejné moci, včetně orgánu veřejné moci, který je kontrolovanou osobou.

K řádku 14.3

Za účelem plnění povinnostní přenesených na poskytovatele si orgán veřejné moci zajistí oprávnění k provedení auditu obdobně jako podle článku 28 GDPR, odstavec 3 písm. h).

K řádku 15

Oblast „Žádosti cizozemských orgánů o zpřístupnění nebo předání dat“ stanovuje bezpečnostní pravidla, jejichž cílem je zajistit, aby poskytovatel nezpřístupňoval zákaznická data třetím stranám především z řad zpravodajských služeb a orgánů cizích států činných v trestním řízení. Pokud již má ke zpřístupnění dojít, je nezbytné, aby se tak stalo v souladu s mezinárodními smlouvami (na základě justiční spolupráce), legislativními požadavky a popsaným procesem. Pokud je to možné, orgán veřejné moci by se měl vždy o takové žádosti dozvědět a podílet se na jejím vyřízení. Cizozemským orgánem se rozumí státní orgán odlišný od státního orgánu České republiky. Právním předpisem třetí země se rozumí právní řád státu, podle kterého byla žádost o informace podána a také právní řád státu, jemuž poskytovatel podléhá.

K tomu lze ještě uvést, že prodejce nesmí nikdy nakládat se zákaznickými daty. Pokud se stane, že by s nimi nakládal, je třeba ho považovat za poskytovatele a vztáhnout na něj všechny povinnosti z toho vyplývající.

K řádku 15.1

Orgán veřejné moci 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 orgán veřejné moci pro své hodnocení maximum dostupných informací o potenciálních právních závazcích a povinnostech poskytovatele, které se týkají zpřístupnění a předávání zákaznických dat a provozních údajů, se zavádí toto bezpečnostní pravidlo.

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

Požadavek je v souladu s ustanovením Annex A, kapitoly DOC-03.1 a DOC-03.2 EUCS. 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 15.2

V souladu s pravidlem upraveným na řádku 15.1 Přílohy je orgán veřejné moci povinen se v maximální možné míře seznámit s povinnostmi poskytovatele vyplývajícími z právních předpisů států odlišných od členských států EU/ESVO, týkajících se zpřístupnění a předávání zákaznických dat a specifických provozních údajů cizozemským orgánům.

S ohledem na povinnosti orgánu veřejné moci podle pravidla upraveného na řádku 1.2 Přílohy spočívající v posouzení rizika předání nebo zpřístupnění dat cizozemským orgánům, může orgán veřejné moci pro tyto účely využít informace získané podle pravidla upraveného na řádku 15.1 Přílohy.

K řádku 15.3

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

Cizozemským orgánem se rozumí státní orgán odlišný od státního orgánu České republiky (viz zákon č. 269/2021 Sb., o občanských průkazech, ve znění pozdějších předpisů).

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 řádku 15.4

Bezpečnostní pravidlo upřesňuje, jak má poskytovatel postupovat v případě obdržení žádosti o zpřístupnění nebo předání dat, zejména 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, podle něhož byla žádost podána a jemuž poskytovatel podléhá. Nejčastěji se bude jednat o uplatňování adekvátních právních prostředků ke zneplatnění nebo zrušení příkazu data orgánu veřejné moci vydat nebo zpřístupnit. Uvedené má za cíl omezit zpřístupnění dat, případně omezit rozsah zpřístupňovaných zákaznických dat třetím stranám, především zpravodajským službám. Pokud již má ke zpřístupnění dojít, je nezbytné, aby se to nestalo jinak, než jak je předvídáno mezinárodními smlouvami (na základě justiční spolupráce) nebo právním řádem státu, podle něhož byla žádost podána a jemuž poskytovatel podléhá a v návrhu vyhlášky popsaným procesem, především tedy po právním posouzení žádosti provedeném poskytovatelem. Pokud je to možné, orgán veřejné moci by se měl vždy o takové žádosti dozvědět a podílet se na jejím vyřízení.

Postup uvedený v bezpečnostním pravidle 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 zákon č. 269/2021 Sb., o občanských průkazech, ve znění pozdějších předpisů).

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

K řádku 15.5

Požadavek rozvádí povinnost poskytovatele upravenou v pravidle upraveném na řádku 15.3 Přílohy tak, že v případě obdržení žádosti cizozemského orgánu o zpřístupnění či vydání dat orgánu veřejné moci, musí poskytovatel tuto žádost přezkoumat všemi vhodnými způsoby. Pouze v případě, že z posouzení poskytovatele vyplyne, že je taková žádost proveditelná, aplikovatelná, je právně závazná a rozsah, v jakém je požadován přístup k datům orgánu veřejné moci 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 orgánu veřejné moci.

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

K řádku 15.6

Požadavek rozvádí povinnost poskytovatele stanovenou v pravidle upraveném na řádku 15.4 Přílohy tak, že v případě obdržení žádosti cizozemského orgánu o zpřístupnění či vydání dat orgánu veřejné moci přezkoumá všemi vhodnými způsoby tuto žádost. I v případě, že z posouzení poskytovatele vyplyne, že je taková žádost proveditelná, aplikovatelná, je právně závazná a rozsah, v jakém je požadován přístup k datům či jejich vydání, odpovídá účelu, za jakým byla žádost podána, je poskytovatel povinen vyvinout veškeré možné úsilí v mezích zákona (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 orgánu veřejné moci.

Pouze pro úplnost se uvádí, že v případě, že poskytovatel 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 povinen provést záznam, ze kterého bude patrné zejména to, proč shledal či neshledal předmětnou žádost proveditelnou, aplikovatelnou, právně závaznou a rozsahem odpovídající jejímu účelu. Tento záznam musí poskytovatel uchovat alespoň 10 let, případně jej prokazatelně předat orgánu veřejné moci.

K řádku 15.7

V případě, že z posouzení poskytovatele vyplyne, že je taková žádost proveditelná, aplikovatelná, je právně závazná a rozsah, v jakém je požadován přístup k datům či jejich vydání, odpovídá účelu, za jakým byla žádost podána, je poskytovatel povinen vyvinout veškeré možné úsilí v mezích zákona (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 orgánu veřejné moci.

Pouze pro úplnost se uvádí, že v případě, že poskytovatel 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.

K řádku 15.8

Poskytovatel v případě, že nedosáhne zrušení povinnosti zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, 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.

K řádku 15.9

V případě služeb poskytovaných systémům zařazeným do kritické bezpečnostní úrovně je s ohledem na skutečnost, že data budou trvale umístěna na území České republiky, poskytovatel povinen žádosti třetích stran, především 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.