SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

NÁZEV MATERIÁLU	Připomínky Svazu průmyslu a dopravy České republiky k návrhu vyhlášky o některých požadavcích pro zápis do katalogu cloud computingu
Č. J.	78/2025
DATUM ZPRACOVÁNÍ	3. 7. 2025
KONTAKTNÍ OSOBA	Kristýna Zábojníková
E-MAIL	kzabojnikova@spcr.cz

Za Svaz průmyslu a dopravy ČR (SPČR) uplatňujeme tyto připomínky:

OBECNÉ PŘIPOMÍNKY

1. K terminologii vyhlášky

Navrhujeme v navrhovaném legislativním textu sjednotit terminologii se zákonem č. 365/2000 Sb., zákon o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (dále jen „**zákon o informačních systémech veřejné správy**“ nebo jen „**zákon**“). Zejména, kde je to relevantní, vypustit pojem „*služba cloud computingu*“ a nahradit jej pojmem „*nabídka cloud computingu*“, případně pojmem „*cloud computing*.

Odůvodnění:

Domníváme se, že terminologie navrhovaného legislativního textu není plně v souladu s terminologií, kterou užívá zákon o informačních systémech veřejné správy.

Návrh vyhlášky zejména v několika ustanoveních používá pojem „služba cloud computingu“, přestože v souladu s dikcí zákona by měl být užíván pojem „nabídka cloud computingu“ ve smyslu § 2 odst. 2 písm. d) zákona, případně pouze „cloud computing“ ve smyslu § 2 odst. 2 písm. b) zákona. Konkrétním příkladem je třeba ustanovení § 9 odst. 3, který uvádí: *„Struktura popisu splnění požadavků podle odst. 2 musí být přehledná a srozumitelná. Za tímto účelem poskytovatel popíše splnění každého z požadavků pro každou službu cloud computingu, kterou žádá zapsat do katalogu cloud computingu […]*“, ačkoliv formálně v terminologii zákona dochází vždy k zápisu *nabídky cloud computingu*, nikoliv *služby*.

Je nezbytné, aby návrh vyhlášky používal jednotnou terminologii s pojmoslovím zákona o informačních systémech veřejné správy. Navrhovaná vyhláška je pouze prováděcím právním předpisem k předmětnému zákonu. Z hlediska legislativní systematiky by měla sekundární legislativa co nejvíce respektovat terminologii právního předpisu, který provádí. Zavádění nebo používání odlišných pojmů by mělo být omezeno pouze na případy, kdy je to zcela nezbytné a odůvodněné (což se u předloženého návrhu většinově nezdá).

Užívání odlišné terminologie oslabuje srozumitelnost sekundární právní úpravy pro její adresáty a může vést ke zbytečné a vyhnutelné právní nejistotě. V případech, kdy stejný pojem není používán jednotně napříč

TELEFON (+420) 731 829 128 | E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADRESA FREYOVA 948/11, 190 00 PRAHA 9
ZAPSANÝ VE SPOLKOVÉM REJSTŘÍKU, VEDENÉM MĚSTSKÝM SOUDEM V PRAZE ODDÍL L, VLOŽKA 3148.
IČO: 00536211, DIČ: CZ00536211.

právními předpisy řešící stejnou problematiku, mohou mít povinné osoby obtíže s interpretací jednotlivých ustanovení.

Naopak průřezové terminologické sjednocení přispěje k vyšší jednoznačnosti ustanovení vyhlášky a jejích právních požadavků. Pro povinné subjekty pak bude snadnější porozumět konkrétním povinnostem, které jim vyhláška ukládá, a v důsledku toho je mohou efektivněji naplňovat.

Tato připomínka je doporučující.

2. **K zásahu do soukromého práva**

Navrhujeme podrobnou revizi jednotlivých požadavků pro zápis služeb do katalogu cloud computingu z hlediska přiměřenosti ve vztahu k zásadě smluvní svobody stran, která povede k odstranění nepřiměřených požadavků na smluvní vztahy mezi orgány veřejné správy a poskytovateli cloud computingu.

Odůvodnění:

Jednotlivé požadavky z vyhlášky (typicky z přílohy č. 3) lze rozdělit na požadavky technické a smluvní. Technické požadavky dokážou cíl vyhlášky, tedy primárně bezpečnost zákaznických dat orgánů veřejné správy patrně naplit. Smluvní požadavky však citelným způsobem zasahují do smluvní svobody stran, kdy vyhláška jako celek v podstatě supluje schopnost orgánů veřejné správy vyjednávat o smluvních podmínkách (tedy celkově vylučuje možnost smluvních stran nastavit si smluvní vztah dle vlastní vůle). Tento zásah do smluvní svobody stran zakotvené na zákonné úrovni (občanským zákoníkem) probíhá z úrovně podzákonné (vyhláškou). Dále jsou zcela vyloučená jakákoli alternativní ujednání smluvních stran, která by cíl vyhlášky mohla naplnit stejně účinně. Minimální změnou, která by měla být provedena, by mělo být zakotvení možnosti, aby si orgán veřejné správy mohl provést vlastní bezpečnostní posouzení (např. ve spolupráci s NÚKIB) na základě podkladů od poskytovatele, stejně jako činí v případě alternativních řešení oproti cloudu.

Uvedená připomínka má obecný charakter a vyžaduje komplexní zásah napříč právní úpravou. Proto není navrženo konkrétní znění.

Tato připomínka je doporučující.

3. **K nejasnosti odpovědnosti v případě přeprodeje**

Navrhujeme vyjasnění a nastavení odpovědností v případě přeprodeje registrované služby cloud computingu. Právní úprava odpovědnosti v případě přeprodeje zcela absentuje a není jasně stanoveno, kdo odpovídá za plnění materiálních požadavků registrace služby v případě přeprodeje. Navrhujeme zahrnutí takové úpravy do návrhu vyhlášky.

Odůvodnění:

Právní úprava nijak neřeší odpovědnost v případě tzv. přeprodeje služeb cloud computingu. V praxi se stává, že zejména globální poskytovatelé nemusí mít ve svém standardu nastaveny veškeré procesy a vlastnosti svých řešení tak, aby vyhovovaly požadavkům vyhlášky. V takovém případě často dochází k manuální úpravě

procesů a vlastností na míru individuálně konkrétnímu zákazníkovi z české veřejné správy. Takové manuální změny však nemusí a často nejsou zohledněny ve vztahu k partnerům (přeprodejcům).

Z důvodu rovného zacházení musí partnerský ekosystém dostávat rovné standardizované podmínky, a proto ve vztahu poskytovatel – přeprodejce není prostor pro individuální úpravy a ujednání. Tato situace není právní úpravou nijak zohledněna, naopak přeprodejci se nacházejí v šedé zóně, kdy jsou oprávněni přeprodávat, ale už nemají žádnou odpovědnost za naplnění materiálních požadavků. Uvedená situace může jednak působit problémy v případě odpovědnosti vůči zákazníkům, ale i vůči procesu zápisu a jednak může být ze strany přeprodejců zneužitelná, protože nemusí vlastní naplnění požadavků vůbec dokládat.

V tomto směru se tak jedná o legislativní mezeru, kterou je třeba právním předpisem odpovídajícím způsobem upravit. Uvedená připomínka má obecný charakter a vyžaduje komplexní zásah napříč právní úpravou. Proto není navrženo konkrétní znění.

Tato připomínka je doporučující.

4. **K nepřiměřenosti požadavků vůči alternativním řešením**

Navrhujeme rozšíření požadavků kladených na služby cloud computingu rovněž na alternativní ICT služby a produkty. Navrhnovaná úprava řeší výhradně služby cloud computingu, přičemž řada požadavků může být stejně tak aplikována na alternativní ICT služby a produkty. Z tohoto pohledu jsou služby cloud computingu znevýhodněny oproti jiným řešením.

Odůvodnění:

Právní úprava jako celek se vztahuje pouze na cloudové služby. Některé požadavky týkající se umístění a nakládání s daty jsou v tomto směru logické, protože oproti alternativním řešením nemají zákazníci svá data uložena na vlastní infrastruktuře, nýbrž na sdílené infrastruktuře poskytovatelů. Řada požadavků však s tímto specifikem cloudových služeb vůbec nesouvisí, respektive takové požadavky by mohly být stejně tak legitimně požadovány po poskytovatelích alternativních IT služeb, například softwaru nebo vlastního zákaznického vývoje. Právní úprava tak zásadním způsobem znevýhodňuje poskytovatele cloudových služeb, když na jejich služby klade nároky, které na alternativní řešení kladeny nejsou, ačkoli by stejně tak uplatňovány být mohly. V praxi je tak v otevřené soutěži zvýhodněn poskytovatel například vlastního zákaznického vývoje oproti poskytovateli cloudových služeb, protože požadavek registrace se uplatní pouze vůči druhému z nich, ačkoli jsou pro to pouze částečné důvody. Bylo by vhodné nastavit tržní prostředí tak, aby obecné požadavky byly vyžadovány pro všechna IT řešení.

Uvedená připomínka má obecný charakter a vyžaduje komplexní zásah napříč právní úpravou. Proto není navrženo konkrétní znění.

Tato připomínka je doporučující.

KONKRÉTNÍ PŘIPOMÍNKY

1. **K § 3 vyhlášky – způsobilost zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti (přestupky podle ZKB)**

Navrhujeme upravit znění ustanovení § 3 písm. b) a c) vyhlášky následujícím způsobem:

„§ 3

Požadavky na způsobilost zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy

Poskytovatelem způsobilým zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6m odst. 1 písm. a) zákona je poskytovatel za podmínek, že […]

b) poskytovatel ani jeho ovládající osoby[1] nebyli v posledních 5 letech pravomocně uznáni vinnými ze spáchání přestupku spočívajícího v neplnění některé z povinností uložené rozhodnutím o uložení nápravného opatření podle § 56 odst. 1 zákona o kybernetické bezpečnosti ***vydaného v důsledku porušení zákona o kybernetické bezpečnosti spočívajícím v jednání podle bodů 1 až 16 písm. c), pokud k jeho spáchání došlo v souvislosti s poskytováním regulované služby cloud computingu podle § 2 odst. 6 písm. c) ve spojení s § 3 zákona o kybernetické bezpečnosti****, a[2]*

c) poskytovatel ani jeho ovládající osoby nebyli v posledních 5 letech více než jednou pravomocně uznáni vinnými ze spáchání ***některého z přestupků spočívajících v jednání podle bodů 1 až 16, pokud k jejich spáchání došlo v souvislosti s poskytováním regulované služby cloud computingu podle § 2 odst. 6 písm. c) ve spojení s § 3 zákona o kybernetické bezpečnosti*** ~~*přestupku spočívajícího v*~~

~~*1. nesplnění povinnosti ohlásit změnu regulované služby podle § 9 odst. 1 zákona o kybernetické bezpečnosti,*~~

~~*2.*~~ ***1.*** *nesplnění povinnosti určit za účelem vymezení stanoveného rozsahu všechna primární aktiva podle § 12 odst. 2 písm. a) nebo podpůrná aktiva podle § 12 odst. 2 písm. c), nebo v nesplnění povinnosti jejich určení pravidelně přezkoumávat nebo aktualizovat podle § 12 odst. 5 zákona o kybernetické bezpečnosti,*

~~*3.*~~ ***2.*** *nesplnění povinnosti posoudit za účelem vymezení stanoveného rozsahu, zda primární aktiva určená podle § 12 odst. 2 písm. a) souvisí s poskytováním regulované služby nebo v nesplnění povinnosti toto posouzení pravidelně přezkoumávat nebo aktualizovat podle § 12 odst. 5 zákona o kybernetické bezpečnosti,*

[1] § 74 zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů.

[2] Zákon č. X/X Sb., o kybernetické bezpečnosti.

*~~4.~~ **3.** nesplnění povinnosti evidovat aktiva podle § 12 odst. 3 zákona o kybernetické bezpečnosti,*

*~~5.~~ **4.** nesplnění povinnosti zavádět nebo provádět bezpečnostní opatření podle § 13 odst. 2 nebo § 18 odst. 1 zákona o kybernetické bezpečnosti,*

*~~6.~~ **5.** nesplnění povinnosti vybírat svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření nebo v nesplnění povinnosti zahrnovat požadavky vyplývající z bezpečnostního opatření do smlouvy s dodavatelem v rozporu s § 13 odst. 5 zákona o kybernetické bezpečnosti,*

*~~7.~~ **6.** nesplnění povinnosti předložit prvotní hlášení o incidentu podle § 16 odst. 1 nebo v nesplnění povinnosti doplnit některý z údajů o incidentu podle § 16 odst. 3 nebo v nesplnění povinnosti nahlásit kybernetický bezpečnostní incident podle § 18 odst. 2 zákona o kybernetické bezpečnosti,*

*~~8.~~ **7.** nesplnění povinnosti poskytnout informace nebo součinnost při zvládání incidentu podle § 17 odst. 3 zákona o kybernetické bezpečnosti,*

*~~9.~~ **8.** nesplnění rozhodnutím stanovené povinnosti nebo zákazu informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem podle § 19 odst. 1 zákona o kybernetické bezpečnosti,*

*~~10.~~ **9.** nesplnění povinnosti informovat uživatele regulované služby o významné hrozbě nebo krocích, které může uživatel služby učinit v reakci na ni, podle § 19 odst. 2 zákona o kybernetické bezpečnosti,*

*~~11.~~ **10.** nesplnění povinnosti uložené rozhodnutím o výstraze podle § 21 odst. 1 zákona o kybernetické bezpečnosti,*

*~~12.~~ **11.** nesplnění reaktivního protiopatření uloženého podle § 23 odst. 1 nebo § 23 odst. 4 zákona o kybernetické bezpečnosti,*

~~13. nesplnění povinnosti nahlásit změnu regulované služby podle § 26 odst. 1 zákona o kybernetické bezpečnosti,~~

*~~14.~~ **12.** porušení podmínky nebo zákazu uložených Národním úřadem pro kybernetickou a informační bezpečnost v opatření obecné povahy podle § 29 zákona o kybernetické bezpečnosti,*

*~~15.~~ **13.** nesplnění povinnosti zajišťovat dostupnost strategicky významné služby z území České republiky ve stanoveném čase nebo kvalitě podle § 33 odst. 1 zákona o kybernetické bezpečnosti,*

*~~16.~~ **14.** nesplnění povinnosti prověřit zajištění poskytování strategicky významné služby podle § 33 odst. 2 zákona o kybernetické bezpečnosti nebo v nesplnění povinnosti o tomto prověření vyhotovit záznam,*

~~*17. nesplnění povinnosti ohlásit službu Národnímu úřadu pro kybernetickou a informační bezpečnost podle § 6 odst. 1 zákona o kybernetické bezpečnosti,*~~

~~*18.*~~ ***15.*** *nesplnění povinnost uložené rozhodnutím podle § 24 odst. 1 zákona o kybernetické bezpečnosti,*

~~*19.*~~ ***16.*** *nesplnění povinnosti provést v souvislosti se stavem kybernetického nebezpečí opatření k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru uloženou rozhodnutím nebo opatřením obecné povahy podle § 39 zákona o kybernetické bezpečnosti~~*,*

~~*20. nesplnění některé z povinností podle § 10 odst. 2 kontrolního řádu[3] jako kontrolovaná osoba v souvislosti s kontrolou plnění povinností podle zákona o kybernetické bezpečnosti, nebo*~~

~~*21. nesplnění povinnosti podle § 10 odst. 3 kontrolního řádu[4] jako povinná osoba v souvislosti s kontrolou plnění povinností podle zákona o kybernetické bezpečnosti.“*~~

Odůvodnění:

K navrženému znění § 3 písm. b) a c) navrhujeme následující úpravy. Věříme, že tento rozsah požadavků v dostatečné míře zajistí posouzení způsobilosti poskytovatele cloud computingu zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správ, aniž by došlo k nežádoucímu vylučování a administrativní zátěže na soukromoprávní subjekty.

Materiální omezení na jednání související s poskytováním služby cloud computingu:

Navrhujeme výslovně omezit výčet přestupků pouze na přestupky, které byly spáchány **v souvislosti s poskytováním služby cloud computingu** ve smyslu nového zákona o kybernetické bezpečnosti.

Nový zákon o kybernetické bezpečnosti se oproti dosavadní úpravě výrazně rozšiřuje okruh regulovaných odvětví a služeb. Je tudíž pravděpodobnější, že poskytovatelé cloud computingu mohou současně poskytovat více regulovaných služeb – nikoliv jen jednu limitovanou službu cloud computingu.

Předmětem ustanovení § 3 vyhlášky mají být primárně požadavky na způsobilost zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy kladené na **poskytovatele cloud computingu**. Nicméně, z aktuálního návrhu legislativního textu vyplývá, že poskytovatel nesmí být vinen ze spáchání vybraných přestupků podle nového zákona o kybernetické bezpečnosti ve vztahu k *jakékoliv* regulované službě. Domníváme se, že takový požadavek není přiměřený a potenciální vyloučení z možnosti dodávat cloud computingu orgánům veřejné správy, by mělo být jen výsledek porušení při poskytování cloud computingu, nikoliv jiných služeb, které s cloud computingem nijak nesouvisejí. . Případné přestupky poskytovatele související s jinou regulovanou službou podle nového zákona o kybernetické bezpečnosti by neměly být pro posouzení způsobilosti relevantní.

[3] Zákon č. 255/2012 Sb., zákon o kontrole (kontrolní řád), ve znění pozdějších předpisů.

Vyloučení přestupků spočívajících v porušení administrativních povinností

Dále navrhujeme upravit zúžit výčet rozhodných přestupků v ustanovení § 3 písm. c). Navrhujeme vyloučit ty přestupky, které spočívají v nesplnění primárně administrativních povinností, tj. například povinnost ohlásit regulovanou službu Národnímu úřadu pro kybernetickou a informační bezpečnost nebo její změnu.

Domníváme se, že případné neplnění administrativních povinností, jako je například nesplnění oznamovacích či evidenčních povinností, samo o sobě nevypovídá o způsobilosti poskytovatele cloud computingu zajistit požadovanou úroveň důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy. Posouzení způsobilosti by mělo být založeno primárně na schopnosti poskytovatele naplnit věcný (materiální) rámec požadavků na kybernetickou bezpečnost, tj. zavedení bezpečnostních opatření, vymezení rozsahu aktiv nebo zavedení požadavků na dodavatelský řetězec. Proto navrhujeme vyjmout z návrhu legislativního textu ustanovení § 3 písm. c) body 1, 13, 17, 20 a 21.

S touto změnou souvisí rovněž další navržená úprava ustanovení § 3 písm. b) – poskytovatel cloud computingu by neměl být považován za nezpůsobilého v případě neplnění povinností uložených jakýmkoliv rozhodnutím o uložení nápravného opatření. Pro účely posouzení způsobilosti by mělo být relevantní pouze případné neplnění povinnosti dle rozhodnutí o uložení nápravného opatření vydaného z důvodu neplnění některé z povinností uvedených ve výčtu v § 3 písm. c), který navrhujeme omezit.

Tato připomínka je zásadní.

2. **K § 9 odst. 3 vyhlášky – doložení splnění požadavků pro nabídky cloud computingu**

Navrhujeme doplnit znění ustanovení § 9 odst. 3 následujícím způsobem:

„(3) Struktura popisu splnění požadavků podle odst. 2 musí být přehledná a srozumitelná. Za tímto účelem poskytovatel popíše splnění každého z požadavků pro každou službu cloud computingu, kterou žádá zapsat do katalogu cloud computingu. V případě, že poskytovatel v rámci jedné nabídky cloud computingu žádá zapsat více služeb cloud computingu spadajících do stejné bezpečností úrovně, je možné doložit splnění každého z požadavků pouze jednou a následně jednoznačně uvést všechny služby cloud computingu, na které se toto doložení vztahuje. ***V případě, že poskytovatel žádá zapsat nabídku cloud computingu, pro které je možné doložit splnění požadavků shodným podkladem, kterým byly prokázány již zapsané nabídky téhož poskytovatele, může se poskytovatel na tento podklad odkázat.***“

Odůvodnění:

Považujeme za vhodné doplnit navrhované znění ustanovení § 9 odst. 3 tak, aby poskytovateli cloud computingu bylo výslovně umožněno v žádosti o zápis nabídky do katalogu cloud computingu odkázat na podklady, které již v minulosti Digitální a informační agentuře (dále jen „Agentura“) předložil k prokázání splnění totožných požadavků v rámci jeho jiné, již zapsané nabídky.

V praxi poskytovatelé cloud computingu často aplikují jednotná bezpečnostní a organizační opatření napříč svými cloudovými službami, zejména pokud jde o opatření týkající se zajištění důvěrnosti, integrity a dostupnosti zpracovávaných informací. Tato opatření se pak typicky odrážejí v příslušné podkladové dokumentaci a smluvních podmínkách, které jsou z větší části shodné, a odlišuje se ve vztahu k dané službě

jen v míře, v jaké to povaha této konkrétní služby vyžaduje. Ilustrativním příkladem jsou typicky obchodní podmínky, které poskytovatelé používají jednotně pro všechny své cloudové služby.

Ze zkušenosti přitom víme, že Agentura v praxi již možnost odkazovat na dříve předložené podklady akceptuje. Nevidíme proto důvod, proč tento osvědčený a smysluplný přístup formálně nezakotvit do budoucna přímo ve vyhlášce. Takové zakotvení by vedlo ke zvýšení právní jistoty na straně poskytovatelů, kteří tento postup již praktikují, a zároveň by rozšířilo povědomí o tomto postupu i mezi těmi, kteří jej dosud nevyužívají a z opatrnosti dokládají identické podklady opakovaně.

Možnost odkazování na dříve doložené dokumenty přitom jednoznačně šetří administrativní náklady, jak na straně poskytovatelů, tak příslušných orgánů. Poskytovatelé nemusejí znovu shromažďovat a předkládat již jednou poskytnuté podklady, zatímco Agentura nebo Národní úřad pro kybernetickou a informační bezpečnost nejsou zase nuceny opakovaně přezkoumávat podkladovou dokumentaci, se kterou již v minulosti pracovaly. Takové opakované zkoumání totožných podkladů totiž nepřináší žádný přínos pro kvalitu přezkumu žádosti ani pro bezpečnost samotných cloudových služeb.

Je třeba taktéž zdůraznit, že z hlediska materiální stránky se možnost odkazování na již dokládané podklady významně neliší od případů, kdy poskytovatel zapisuje více nabídek cloud computingu hromadně v rámci jedné hromadné žádosti. V těchto případech se rovněž předkládají shodné podklady pro různé cloudové služby – rozdíl je pouze v tom, že k tomu dochází v rámci jednoho právního úkonu a v jiném časovém rámci.

Pro úplnost uvádíme, že navrhovaná změna se týká výhradně otázky administrativní formy prokazování splnění požadavků a nijak se nedotýká povinnosti tyto požadavky materiálně naplňovat. Na poskytovateli nadále zůstává odpovědnost zajistit, že odkazované podklady jsou aktuální a vztahují se k nově zapisované nabídce. Cílem je pouze umožnit zefektivnění procesu, aby zbytečně nekladl překážky poskytovatelům, kteří jinak plní všechny požadavky pro zápis.

Tato připomínka je zásadní.

3. **<u>K § 9 odst. 6 písm. c) vyhlášky – právní závaznost návrhu smluvní dokumentace</u>**

Navrhujeme upravit znění ustanovení § 9 odst. 6 písm. c) vyhlášky následujícím způsobem:

„(6) Pro účely podkladů k ověření splnění požadavku na zajištění důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem podle § 4 se rozumí […]

*c) návrhem smluvní dokumentace návrh smlouvy, smluvních podmínek, podmínek poskytování služby či podobný podklad **<u>pro zapisovanou</u>**~~, sloužící jako právně závazná nabídka~~ **<u>nabídku</u>** ~~poskytování služby~~ cloud computingu, kterou poskytovatel žádá zapsat do katalogu cloud computingu,“*

<u>Odůvodnění:</u>

Navrhované ustanovení § 9 odst. 6 písm. c) vyhlášky definuje pojem *návrh smluvní dokumentace* jako takový návrh smlouvy, smluvních podmínek, podmínek poskytování služby či podobný podklad, který slouží jako <u>právně závazná</u> nabídka poskytování služby cloud computingu.

Předkládaná smluvní dokumentace musí být vzorová a nemůže být brána jako právně závazný návrh. V takovém případě by se smluvní dokumentace předkládaná pro účely zápisu do katalogu cloud computingu stala jako celek fixní, neměnná, a nebylo by ji možné jakkoliv měnit či aktualizovat. Smluvní dokumentace přitom často obsahuje rovněž komerční podmínky (ať už obecné nebo sjednávané individuálně pro každého zákazníka) anebo podmínky, které se neprokazují pro účely zápisu do katalogu cloud computingu a nejsou tak z regulatorního hlediska jakkoliv relevantní. Navrhovaný požadavek by fakticky znamenal „zafixování" smluvních podmínek jako celku k okamžiku podání nabídky, bez jakékoliv možnosti budoucích úprav.

Poskytovatelé cloud computingu v praxi své smluvní podmínky cloudových služeb pravidelně upravují a aktualizují, a to například i z důvodu vývoje technologií a bezpečnostních standardů. Odvětví, ve kterém působí poskytovatelé cloud computingu, je vysoce dynamické a standardy považované v daném okamžiku za *best practice* se mohou v řádu měsíců a let stát zastaralými.

Úprava smluvní dokumentace může být v některých případech i explicitně vyžadována, a to zejména za účelem přizpůsobení nově přijaté legislativě. Ostatně i samotný návrh této vyhlášky dle důvodové zprávy „*reaguje na chystanou novou legislativu v oblasti kybernetické bezpečnosti*" danou implementací směrnice NIS2[4] do českého právního řádu. Již nyní je zřejmé, že poskytovatelé cloud computingu budou muset výhledově revidovat své smluvní podmínky tak, aby reflektovaly nové požadavky na dodavatelské smlouvy dle této nové právní úpravy kybernetické bezpečnosti. Obdobně lze do budoucna očekávat dopady i dalších legislativních aktů, jako je nařízení o kybernetické odolnosti[5], akt o umělé inteligenci[6] nebo jiná relevantní právní úprava v oblasti digitální ekonomiky.

Z uvedených důvodů proto navrhujeme vypustit z definice pojmu *návrh smluvní dokumentace* požadavek na její „právní závaznost".

Současně v rámci této připomínky navrhujeme odstranit i slovní spojení *„poskytování služby"* a nahradit jej pojmoslovím odpovídajícím zákonu o informačních systémech veřejné správy. Tento zákon neužívá pojem „*služba cloud computingu*", nýbrž pojmy „*nabídka cloud computingu*" (ve smyslu § 2 odst. 2 písm. d)) či „*cloud computing*" (ve smyslu § 2 odst. 2 písm. b)). Z hlediska legislativní systematiky je žádoucí, aby prováděcí předpis nepoužíval odchylnou terminologii, pokud k tomu není věcný důvod (blíže viz obecná připomínka k terminologii vyhlášky).

Tato připomínka je zásadní.

[4] Celým názvem Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148

[5] Celým názvem Nařízení Evropského parlamentu a rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828

[6] Celý názvem Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828

4. **<u>K § 10 vyhlášky – přechodná ustanovení (splnění požadavků pro stávající zapsané poskytovatele a nabídky)</u>**

Navrhujeme zpřesnit přechodná ustanovení ve vztahu ke stávajícím registracím služeb, následujícím způsobem:

„(1) Žádosti o zápis poskytovatele do katalogu cloud computingu podle § 6q zákona a o zápis nabídky cloud computingu do katalogu cloud computingu podle § 6t zákona podané přede dnem účinnosti této vyhlášky se posuzují podle dosavadních právních předpisů.

<u>(2) Pro poskytovatele cloud computingu zapsané v katalogu cloud computingu přede dnem účinnosti této vyhlášky se splnění požadavku způsobilosti zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6m odst. 1 písm. a) zákona posuzuje podle dosavadních právních předpisů.</u>

<u>(3) Pro nabídky cloud computingu zapsané v katalogu cloud computingu přede dnem účinnosti této vyhlášky se plnění požadavku na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné moci podle § 6n písm. b) zákona posuzuje podle dosavadních právních předpisů.</u>

<u>(4)</u> *~~(2)~~ […]“*

<u>Odůvodnění:</u>

Předložený legislativní text výslovně neupravuje právní režim poskytovatelů a nabídek cloud computingu, kteří byli do katalogu cloud computingu již zapsáni. Jakékoliv existující zápisy by neměly být přijetím nové úpravy dotčeny a přijímaná vyhláška by se neměla na tyto existující zápisy uplatnit. Předložený návrh toto nereflektuje a nijak nezvažuje již existující zápisy.

Při absenci jakýchkoliv přechodných ustanovení by přitom bylo možné aplikovat požadavky podle navrhované vyhlášky i na existující zápisy – podle zákona Agentura průběžně posuzuje, zda již zapsaní poskytovatelé cloud computingu (srov. § 6s odst. 1 písm. b) zákona) i nabídky cloud computingu (§ 6w odst. 1 písm. b) zákona) i nadále splňují podmínky pro další vedení v katalogu. Absence výslovné přechodné úpravy by znamenala, že Agentura bude muset pro tyto účely automaticky aplikovat nové podmínky stanovené prováděcí vyhláškou. To by konkrétně znamenalo, že Agentura bude posuzovat:

- způsobilost poskytovatele zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy ve smyslu § 6m odst. 1 písm. a) zákona podle nového navrhovaného znění § 3 vyhlášky; a

- schopnost cloud computingu dosahovat alespoň základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné moci ve smyslu § 6n písm. b) zákona podle nových příloh č. 1 až 4 k vyhlášce.

V případě, že by Agentura zjistila, že stávající poskytovatelé a nabídky těmto novým podmínkám nevyhovují (a nedošlo by k odstranění zjištěných „nedostatků“ ve stanovené lhůtě), rozhodne o výmazu těchto poskytovatelů a nabídek z katalogu.

Absence výslovné přechodné úpravy může v praxi vyvolat nejistotu ohledně právního postavení poskytovatelů a jejich nabídek, kteří byli do katalogu zapsáni v souladu s předchozí právní úpravou, a současně navozuje riziko nepřípustné retroaktivity.

Nové podmínky stanovené prováděcí vyhláškou by se v souladu s principy právního státu měly vztahovat výhradně na nové zápisy, nikoliv na ty, které již v katalogu figurují. Rozšíření působnosti na dříve zapsané nabídky by mohlo být vnímáno jako zpětné působení právní normy, jež je v právním státě obecně zakázáno.

Jakýkoliv odlišný přístup by neúměrně zatížil poskytovatele, kteří své nabídky připravovali podle dosavadní platné právní úpravy a zajistili odpovídající bezpečnostní opatření a relevantní podkladovou dokumentaci podle podmínek účinných v době jejich zápisu. Tito poskytovatelé by tak byli nuceni v průběhu platnosti zápisu ad hoc plnit podmínky, se kterými nemohli fakticky počítat, což by mohlo vést nejen k organizačním a technickým obtížím, jakož i k nedůvodným ekonomickým a administrativním nákladům. Retroaktivní působení by rovněž bylo v rozporu s § 6w odst. 1 písm. c) zákona o informačních systémech veřejné správy, podle kterého zápis nabídky cloud computingu je časově omezen na tři roky, potažmo šest let[7]. Není tedy žádný legitimní důvod, aby se na poskytovatele a nabídky zapsané podle staré právní úpravy vztahovaly nové požadavky okamžitě, a ještě v průběhu platnosti původního zápisu, která je zákonem výslovně časově omezena.

Z těchto důvodů navrhujeme stanovit, že splnění příslušných požadavků se v případě poskytovatelů cloud computingu a nabídek cloud computingu již zapsaných v katalogu cloud computingu přede dnem nabytí účinnosti této vyhlášky posuzuje podle dosavadních právních předpisů. Pro úplnost uvádíme, že záměrem této připomínky je výhradně vyjasnit, jak se na legislativní úrovni uplatní nové materiální požadavky stanovené v § 3 (v případě poskytovatelů cloud computingu) a přílohách č. 1 až 4 vyhlášky (v případě nabídek cloud computingu) vůči již existujícím zápisům (potažmo, že se neuplatní). Není naopak cílem zpochybnit způsoby prokazování plnění požadavků, které stanoví například příloha č. 5 vyhlášky pro dokládání příslušných ISO certifikací.

Tato připomínka je zásadní.

5. **<u>K § 10 odst. 2 vyhlášky – přechodná ustanovení (požadavek na popis povinností vyplývajících z právních předpisů států mimo EU)</u>**

Navrhujeme upravit znění ustanovení § 10 odst. 2 vyhlášky následujícím způsobem v případě nevyhovění požadavku na úpravu řádku 2.2 přílohy č. 1, 2, 3 a 4 vyhlášky (viz připomínka č. 8):

*„(2) Splnění požadavků v řádcích **<u>2.2 přílohy č. 1 až 4 a v</u>** řádcích 8.1 a 8.2 přílohy č. 3 a 4 k této vyhlášce a požadavků na strukturu a náležitosti zprávy o provedení penetračního testu a intervaly pro její*

[7] Zákon konkrétně stanoví, že Agentura rozhodne o výmazu nabídky cloud computingu z katalogu cloud computingu *„uplyne-li doba 3 let ode dne, kdy byla nabídka cloud computingu do katalogu cloud computingu zapsána, pokud poskytovatel cloud computingu nepotvrdil Agentuře, že nabídka cloud computingu je stále platná, nebo uplyne-li doba <u>3 let ode dne, kdy poskytovatel cloud computingu naposledy potvrdil Agentuře, že nabídka cloud computingu je stále platná</u>*“.

předkládání podle § 6 se řídí dosavadními právními předpisy po dobu 18 měsíců ode dne nabytí účinnosti této vyhlášky.“

Odůvodnění:

V případě, že Národní úřad pro kybernetickou a informační bezpečnost nevyhoví ani jednomu z uvedených alternativních návrhů na úpravu řádku 2.2 přílohy č. 1, 2, 3 a 4 vyhlášky, navrhujeme na tento požadavek rozšířit odklad účinnosti formulovaný v § 10 odst. 2 vyhlášky.

Zejména pro globální poskytovatele cloud computingu bude vyhotovení tohoto posouzení dle požadavků na obsah posouzení, které mají být nově stanoveny jako závazné, velmi časově náročné, neboť bude vyžadovat hlubší analýzu právní úpravy v relevantních zemích. Je proto žádoucí, aby byl poskytovatelům poskytnut dostatečný časový prostor pro řádné splnění tohoto požadavku.

Tato připomínka je zásadní.

6. **K § 10 odst. 2 vyhlášky – přechodná ustanovení (penetrační testování)**

Navrhujeme upravit znění ustanovení § 10 odst. 2 vyhlášky v kontextu připomínky č. 13 k řádku 8.2 přílohy č. 3 a 4 vyhlášky – metodika provádění penetračních testů následujícím způsobem:

„(2) Splnění požadavků v řádcích 8.1 a 8.2 přílohy č. 3 a 4 k této vyhlášce a požadavků na strukturu a náležitosti zprávy o provedení penetračního testu a intervaly pro její předkládání podle § 6 ***je možné doložit dle*** ~~*se řídí*~~ *dosavadní****ch*** ~~*mi*~~ *právní****ch*** ~~*mi*~~ *předpis****ů, a to*** *po dobu 18 měsíců ode dne nabytí účinnosti této vyhlášky.* ***Bez ohledu na přechodné ustanovení v odst. 1 se požadavky v řádcích 8.1 a 8.2 přílohy č. 3 a 4 k této vyhlášce uplatní i na žádosti o zápis nabídky cloud computingu do katalogu cloud computingu podle § 6t zákona podané přede dnem účinnosti této vyhlášky****."*

Odůvodnění:

Odůvodnění k této připomínce je uvedeno v připomínce č. 13 níže k řádku 8.2 přílohy č. 3 a 4 vyhlášky – metodika provádění penetračních testů následujícím způsobem, a to z důvodu propojení těchto dvou připomínek.

Tato připomínka je zásadní.

7. **K § 10 odst. 2 vyhlášky – přechodné období**

Navrhujeme prodloužit přechodné období uvedené v odst. 2 na dobu 24 měsíců.

Odůvodnění:

Delší přechodné období je nezbytné z následujících důvodů:

- komplexní procesy validace souladu vyžadují významný čas pro shromáždění potřebné dokumentace;

- kontinuita služeb je kritická - současné cloudové služby v katalogu by se staly neplatnými při změně požadavků;
- opětovná validace souladu vyžaduje značný čas;
- sběr a ověření důkazů je časově náročné.

Tato připomínka je zásadní.

8. **K řádku 2.2 přílohy č. 1, 2, 3 a 4 vyhlášky – žádost o zpřístupnění dat (požadavek na popis povinností vyplývajících z právních předpisů států mimo EU)“**

Navrhujeme upravit řádek 2.2. přílohy č. 1, 2, 3 a 4 vyhlášky dle návrhů níže.

Navrhované varianty se vztahují ke všem bezpečnostním úrovním, vybraná úroveň kritická je pouze demonstrativní, vzhledem k tomu, že se stejný text opakuje ve všech přílohách.

Varianta 1:

Úplně vypustit daný řádek:

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni kritická	Podklad, kterým poskytovatel doloží splnění požadavku
2. Žádosti o zpřístupnění a předání dat		
~~**2.2**~~	~~**Poskytovatel jasně a srozumitelně uvádí jeho povinnosti vyplývající z právních řádů států odlišných od členských států Evropské unie nebo odlišných od členských států Evropského hospodářského prostoru nebo u těch států, u kterých Evropská komise nerozhodla o udělení tzv. adequacy decision podle článku 45 obecného nařízení o ochraně osobních údajů1, na jejichž území se nalézá datacentrum nebo jiná infrastruktura, ve které dochází ke zpracování zákaznických dat nebo specifických provozních údajů podle řádků 1.1 této přílohy týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů.** **Tento popis musí být v takové kvalitě, aby z něj bylo možné zákazníkem posoudit vhodnost právního řádu s ohledem na zpracovávání zákaznických dat a specifických provozních údajů. Proto poskytovatel provede popis povinností obsahující informace o tom, který cizozemský orgán veřejné moci, jehož činnost spočívá v prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, zpravodajská služba, nebo jiný orgán s obdobným předmětem činnosti nebo obdobnými pravomocemi, může žádat o zpřístupnění a předání dat, za jakých podmínek může tento orgán žádat o zpřístupnění a předání dat a na jak dlouho, na jaká data se daná povinnost vztahuje (provozní, zákaznická) a zda je možné žádost o zpřístupnění nebo předání dat přezkoumat nezávislým soudem.**~~	~~**Písemný popis podle § 9 odst. 6 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku.**~~

Varianta 2:

Navrhujeme upravit znění řádku 2.2. přílohy č. 1 až 4 vyhlášky následovně[8]:

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni kritická	Podklad, kterým poskytovatel doloží splnění požadavku
2. Žádosti o zpřístupnění a předání dat		
2.2	~~Poskytovatel jasně a srozumitelně uvádí jeho~~ **Zákazník má k dispozici jasný a srozumitelný popis** povinnosti vyplývající z právních řádů států odlišných od členských států Evropské unie nebo odlišných od členských států Evropského hospodářského prostoru nebo u těch států, u kterých Evropská komise nerozhodla o udělení tzv. adequacy decision podle článku 45 obecného nařízení o ochraně osobních údajů[1], na jejichž území se nalézá datacentrum nebo jiná infrastruktura **poskytovatele**, ve které dochází ke zpracování zákaznických dat nebo specifických provozních údajů podle řádku 1.1 této přílohy týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů. Tento popis ~~musí být~~ **bude** v takové kvalitě, aby z něj bylo možné zákazníkem posoudit vhodnost právního řádu s ohledem na zpracovávání zákaznických dat a specifických provozních údajů. ~~Proto poskytovatel provede~~ **Popis** povinností ~~obsahující~~ **bude obsahovat** informace o tom, který cizozemský orgán veřejné moci, jehož činnost spočívá v prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, zpravodajská služba, nebo jiný orgán s obdobným předmětem činnosti nebo obdobnými pravomocemi, může žádat o zpřístupnění a předání dat, za jakých podmínek může tento orgán žádat o zpřístupnění a předání dat a na jak dlouho, na jaká data se daná povinnost vztahuje (provozní, zákaznická) a zda je možné žádost o zpřístupnění nebo předání dat přezkoumat nezávislým soudem.	**Žádný doklad se nevyžaduje**. Písemný popis podle § 9 odst. 6 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku, **vyhotoví Digitální a informační agentura nebo Národní úřad pro kybernetickou a informační bezpečnost**.

Varianta 3:

[8] Pozn.: V tabulce uvádíme znění příslušného požadavku obsaženého v řádku 2.2 přílohy č. 3 vyhlášky, nicméně znění tohoto požadavku v řádcích 2.2 příloh 1, 2 a 4 vyhlášky je materiálně stejné a námi navržené změny ve znění řádku 2.2 přílohy č. 3 lze implementovat rovněž v příslušných řádcích příloh 1,2 a 4 vyhlášky.

Navrhujeme upravit znění řádků 2.2. přílohy č. 1 až 4 vyhlášky následovně[9]:

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni kritická	Podklad, kterým poskytovatel doloží splnění požadavku
2. Žádosti o zpřístupnění a předání dat		
2.2	Poskytovatel jasně a srozumitelně uvádí jeho povinnosti vyplývající z právních řádů států odlišných od členských států Evropské unie nebo odlišných od členských států Evropského hospodářského prostoru nebo u těch států, u kterých Evropská komise nerozhodla o udělení tzv. adequacy decision podle článku 45 obecného nařízení o ochraně osobních údajů[1], na jejichž území se nalézá datacentrum nebo jiná infrastruktura, ve které dochází ke zpracování zákaznických dat nebo specifických provozních údajů podle řádků 1.1, 1.4 a 1.5 přílohy č. 2 k této vyhlášce týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů. Tento popis musí být v takové kvalitě, aby z něj bylo možné zákazníkem posoudit vhodnost právního řádu s ohledem na zpracovávání zákaznických dat a specifických provozních údajů. ~~Proto poskytovatel provede popis povinností obsahující informace o tom, který cizozemský orgán veřejné moci, jehož činnost spočívá v prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, zpravodajská služba, nebo jiný orgán s obdobným předmětem činnosti nebo obdobnými pravomocemi, může žádat o zpřístupnění a předání dat, za jakých podmínek může tento orgán žádat o zpřístupnění a předání dat a na jak dlouho, na jaká data se daná povinnost vztahuje (provozní, zákaznická) a zda je možné žádost o zpřístupnění nebo předání dat přezkoumat nezávislým soudem.~~	Písemný popis podle § 9 odst. 6 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku.

Odůvodnění:

K variantě 1:

Uvedený požadavek představuje zásadní administrativní zátěž pro poskytovatele a nepřispívá k vyšší úrovni kybernetické bezpečnosti (tj. k zajištění základní úrovně ochrany důvěrnosti, integrity a dostupnosti

[9] Pozn.: V tabulce uvádíme znění příslušného požadavku obsaženého v řádku 2.2 přílohy č. 3 vyhlášky, nicméně znění tohoto požadavku v řádcích 2.2 příloh 1, 2 a 4 vyhlášky je materiálně stejné.

informací), a nelze jej tedy z hlediska smyslu právní úpravy považovat za účelný. Jedná se o nepřiměřený požadavek. Nadto je problematická objektivita tohoto požadavku – není stanoveno a v podstatě prakticky ani nelze ověřit ze strany NUKIB/DIA správnost informací poskytnutých poskytovatelem. Současně není reflektována novelizace právních předpisů. Požadavek jako takový je tedy celkově nepřiměřený, nepřezkoumatelný a účinně nepřispívá k naplnění smyslu vyhlášky.

K variantě 2:

V rámci návrhu požadavku na vyhotovení popisu povinností vyplývajících z právních předpisů států odlišných od členských států EU/EHP došlo oproti stávajícímu požadavku dle řádku 2.5 přílohy č. 2 vyhlášky č. 316/2021 Sb. k významnému upřesnění rozsahu informací, které má posouzení obsahovat.

Již stávající požadavek na vyhotovení posouzení představuje pro poskytovatele cloud computingu nepřiměřenou administrativní zátěž, a to především pro globální poskytovatele cloud computingu, jež mohou teoreticky zpracovávat zákaznická data po celém světě. V praxi se tento požadavek ukázal jako zcela neproveditelný, nepřiměřený a nadměrně zatěžující pro poskytovatele cloud computingu. Popis povinností může u globálních poskytovatelů cloud computingu zahrnovat posouzení právních předpisů u více než sta zemí, což je pro poskytovatele jednak nepřiměřeně nákladné a jednak prakticky neproveditelné. Tento popis musí totiž vyhotovit každý poskytovatel cloud computingu samostatně, což vede k tomu, že zákazník má k dispozici popisy povinností plynoucích z právních předpisů třetích zemí od více poskytovatelů cloud computingu, které nebudou logicky konzistentní, budou v rozdílné kvalitě a mohou obsahovat rozdílné právní posouzení. Takový stav je přitom v rozporu s účelem celého požadavku.

Stávající požadavek na vyhotovení posouzení dává poskytovatelům cloud computingu alespoň jistou míru flexibility při zpracování posouzení. Nově navržené požadavky na obsah právního posouzení vycházejí ze vzorového zadání ke zpracování právního posouzení dle požadavku vyhlášky č. 316/2021 Sb., zveřejněného Digitální a informační agenturou[10]. Použití tohoto vzorového zadání však aktuálně není pro poskytovatele cloud computingu povinné. Nově však návrh vyhlášky stanoví tyto požadavky na obsah právního posouzení jako **závazné**, čímž se nároky na poskytovatele ještě dále zvýší.

Z těchto důvodů považujeme za vhodné, aby popis povinností plynoucích z právních předpisů třetích zemí vytvořila Digitální a informační agentura nebo Národní úřad pro kybernetickou a informační bezpečnost. Popis povinností tak bude společný pro všechny poskytovatele služeb cloud computingu a bude pravidelně aktualizován. Zákazník poté bude mít možnost dohledat v tomto univerzálním popisu povinností právních předpisů třetích zemí popis právního řádu zemí, v nichž jeho poskytovatel služeb cloud computingu dokládá zpracování zákaznických dat dle požadavků vyhlášky. Tento návrh je o to více opodstatněný v situaci, kdy návrh vyhlášky nově stanoví závazné požadavky na obsah právního posouzení. V takové situaci je nejefektivnějším řešením vytvořit jednotné právní posouzení pro všechny poskytovatele cloud computingu,

[10] Vzorové zadání ke zpracování právního posouzení ve smyslu řádku 2.5 přílohy č. 2 vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu, dostupné na webové stránce https://www.dia.gov.cz/media/2481/download/Pokyny-k-pouz%CC%8Citi%CC%81-vzoru-pro-zpracova%CC%81ni%CC%81-pra%CC%81vni%CC%81ho-posouzeni%CC%81_ID_2.5.pdf?v=1

který bude odpovídat novým požadavkům na obsah a za jehož zpracování a aktualizaci budou odpovědná Digitální a informační agentura nebo Národní úřad pro kybernetickou a informační bezpečnost.

K variantě 3:

S ohledem na odůvodnění výše navrhujeme jako alternativní řešení vypustit z návrhu vyhlášky požadavky na obsah právního posouzení a zachovat tak z větší míry tento požadavek v jeho stávající podobě.

Důvodová zpráva k návrhu vyhlášky uvádí, že k rozvedení popisu relevantních povinností poskytovatele „*bylo přistoupeno na základě zpětné vazby poskytovatelů, pro které bylo toto ustanovení často nejasné, i na základě zkušeností správních orgánů, které pozorovaly obtíže poskytovatelů s doložením splnění tohoto požadavku, čemuž by lepší specifikace očekávané podoby doložení jeho splnění měla pomoci*“. Nová úprava tedy zjevně nemá za cíl rozšiřovat povinnosti poskytovatelů oproti původní úpravě, ale pouze srozumitelněji povinnosti vysvětlit a usnadnit jejich implementaci. Domníváme se však, že zakotvení konkrétních závazných požadavků na obsah posouzení není nezbytné, a naopak může vést k vyšším nárokům na poskytovatele cloud computingu, jak uvádíme výše.

Dle současného právního rámce jsou požadavky na obsah právního posouzení aktuálně obsaženy ve vzorovém zadání zveřejněném Digitální a informační agenturou[11], které však má doporučující, nikoliv závazný charakter. Tento přístup navrhujeme v rámci vyhlášky zachovat, aby byly požadavky na obsah předmětného posouzení stanoveny na úrovni nezávazného vzoru či metodického pokynu, a nikoliv formou závazných požadavků zakotvených ve vyhlášce.

Tato připomínka je zásadní.

9. **<u>K řádku 5.1 přílohy č. 1, 2, 3 a 4 vyhlášky – šifrování zákaznického obsahu</u>**

Navrhujeme upravit znění řádku 5.1. přílohy č. 1, 2, 3 a 4 dle návrhu níže.

Navrhovaná změna se vztahuje ke všem bezpečnostním úrovním, vybraná úroveň kritická je pouze demonstrativní, vzhledem k tomu, že se stejný text opakuje ve všech přílohách.

[11] Vzorové zadání ke zpracování právního posouzení ve smyslu řádku 2.5 přílohy č. 2 vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu, dostupné na webové stránce https://www.dia.gov.cz/media/2481/download/Pokyny-k-pouz%CC%8Citi%CC%81-vzoru-pro-zpracova%CC%81ni%CC%81-pra%CC%81vni%CC%81ho-posouzeni%CC%81_ID_2.5.pdf?v=1

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni kritická	Podklad, kterým poskytovatel doloží splnění požadavku
5. Nakládání s daty		
5.1	Poskytovatel vždy **<u>umožňuje ochranu zákaznického obsahu</u>** ~~**chrání zákaznický obsah**~~ šifrováním při všech síťových přenosech a v úložištích ve službě cloud computingu.	Část návrhu smluvní dokumentace podle § 9 odst. 6 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 6 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 6 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

<u>Odůvodnění:</u>

Navrhovaná úprava řádku 5.1. přílohy č. 1 až 4 reflektuje technicky specifická řešení, která dávají zákazníkům možnost aktivovat si popřípadě deaktivovat si šifrování zákaznického obsahu v rámci služby cloud computingu. Jedná se o situace, kdy si pouze sám zákazník (popř. prostřednictvím implementačního partnera) zvolí okamžik aktivace šifrování. Současně má zákazník možnost šifrování kdykoli deaktivovat. V takové situaci nemůže mít poskytovatel technicky žádnou kontrolu nad tím, jakým způsobem zákazník s aktivací/deaktivací šifrování nakládá. Současně však platí, že zákazník má možnost aktivovat si šifrování zákaznického obsahu po celou dobu využívání služby cloud computingu.

Požadavek, aby šifrování bylo aktivní vždy není u všech řešení technicky realizovatelný a současně odepírá zákazníkovi možnost aktivovat/deaktivovat si šifrování dle vlastního uvážení.

Příkladem může být třeba požadavek na šifrování zákaznického obsahu dle Cloud Computing Compliance Criteria Catalogue (C5), který stanoví povinnost pro poskytovatele vytvořit procesy a opatření, aby mohlo být šifrování zajištěno a ponechává odpovědnost za využívání šifrování na straně zákazníka.

Navrhujeme tedy úpravu v tomto smyslu, tedy aby požadavek směřoval k možnosti šifrování po celou dobu využívání služby cloud computingu.

Tato připomínka je zásadní.

10. <u>K řádku 5.2 přílohy č. 2, 3 a 4 vyhlášky – šifrování pomocí šifrovacích sad</u>

Navrhujeme znění řádku 5.2. přílohy č. 2, 3 a 4 dle návrhu níže.

Navrhovaná změna se vztahuje ke všem uvedeným bezpečnostním úrovním v příloze 2, 3 a 4, vybraná úroveň kritická je pouze demonstrativní, vzhledem k tomu, že se stejný text opakuje ve všech uvedených přílohách.

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni kritická	Podklad, kterým poskytovatel doloží splnění požadavku
5. Nakládání s daty		
5.2	Poskytovatel zákazníkovi umožňuje ochranu zákaznického obsahu šifrováním při všech síťových přenosech a v úložištích ve službě cloud computingu pomocí některého ze schválených algoritmů uvedených v aktuálně platném doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost, které je zveřejněno na jeho internetových stránkách, v rámci celé šifrovací sady. V případě že poskytovatel nabízí šifrovací sady, které obsahují takové algoritmy, které nejsou schválené v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost, poskytovatel umožní zákazníkovi výběr těch šifrovacích sad, které aplikují algoritmy **<u>materiálně srovnatelné a zabezpečující srovnatelnou úroveň ochrany jako algoritmy</u>** schválené v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost.	Část návrhu smluvní dokumentace podle § 9 odst. 6 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, nebo část další dokumentace podle § 9 odst. 6 písm. d) této vyhlášky, ze které vyplývá splnění požadavku

<u>Odůvodnění:</u>

Předložený legislativní text uvedený v řádku 5.2 přílohy č. 2 až 4 rozšiřuje stávající právní úpravu, podle níž jsou schválené šifrovací algoritmy stanoveny v aktuálně platném doporučení Národního úřadu pro kybernetickou a informační bezpečnost, zveřejněném na jeho internetových stránkách. Nově je v tomto ustanovení doplněna povinnost poskytovatele umožnit zákazníkovi v případě, že nabízí šifrovací sady obsahující algoritmy, které nejsou uvedeny v doporučení v oblasti kryptografických prostředků vydaném

Národním úřadem pro kybernetickou a informační bezpečnost, výběr výhradně těch šifrovacích sad, jež obsahují algoritmy schválené uvedeným doporučením.

Domníváme se, že předmětná právní úprava není předvídatelná a může narušovat právní jistotu povinných osob.

Metodika Národního úřadu pro kybernetickou a informační bezpečnost není obecně závazná a svou povahou podléhá jednostranným změnám, a to i bez veřejného konzultačního procesu. Takový stav může vést ke svévoli a povinné osoby se tak mohou ocitat v pozici, kdy nedokáží s jistotou předvídat obsah svých povinností.

Z hlediska legislativní systematiky není vůbec žádoucí, aby prováděcí právní předpis, jehož účelem je konkretizovat zákonem stanovené povinnosti, se dále ještě odkazoval na jiný podkladový dokument, který nemá povahu právního předpisu. Takový postup činí právní rámec méně přehledným a srozumitelným a komplikuje výklad práv a povinností povinných osob, které musí tedy nejen vykládat aplikovatelné právní předpisy, ale k tomu sledovat také průběžně aktualizované doporučení jednoho správního úřadu.

Zároveň kryptografické algoritmy podléhají rychlému vývoji, vylepšením a průběžným reakcím na nově objevené zranitelnosti, přičemž životní cyklus konkrétního algoritmu může být relativně krátký. Pokud by se poskytovatelé museli spoléhat výhradně na seznam algoritmů uvedených v doporučení Národního úřadu pro kybernetickou a informační bezpečnost platném v daném okamžiku, mohlo by to neúměrně omezovat technologickou flexibilitu, znemožňovat rychlou reakci na nová bezpečnostní rizika a narušovat dynamiku zavádění moderních, bezpečnějších kryptografických řešení.

Pro posílení právní jistoty proto navrhujeme výslovně stanovit, že pro splnění tohoto požadavku postačí umožnit zákazníkovi výběr těch šifrovacích sad, které využívají algoritmy materiálně srovnatelné a zajišťující obdobnou úroveň ochrany, jako je tomu u algoritmů uvedených v doporučení Národního úřadu pro kybernetickou a informační bezpečnost. Taková úprava je přiměřená, neboť zajišťuje předvídatelnost právního rámce, dává poskytovatelům vyšší míru jistoty pro přípravu a provoz jejich technických řešení a současně ponechává Národnímu úřadu pro kybernetickou a informační bezpečnost prostor nadále se odborně vyjadřovat ke kryptografickým algoritmům.

Tato připomínka je doporučující.

11. **<u>K řádku 7.1 přílohy č. 2, 3 a 4 vyhlášky – kybernetické bezpečnostní události</u>**

Navrhujeme upravit znění řádku 7.1. přílohy č. 2, 3 a 4 dle návrhu níže.

Navrhovaná změna se vztahuje ke všem uvedeným bezpečnostním úrovním v příloze 2, 3 a 4, vybraná úroveň kritická je pouze demonstrativní, vzhledem k tomu, že se stejný text opakuje ve všech uvedených přílohách.

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni kritická	Podklad, kterým poskytovatel doloží splnění požadavku
7. Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty		
7.1	Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí. ~~**Poskytovatel umožňuje zákazníkovi vzdálený přístup k informacím o všech událostech týkajících se daného zákazníka. Nové události zpřístupní poskytovatel zákazníkovi bez zbytečného odkladu, nejpozději však do 24 hodin.**~~	Část návrhu smluvní dokumentace podle § 9 odst. 6 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 6 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 6 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

Odůvodnění:

Uvedený požadavek se skládá ze tří dílčích požadavků – 1) povinnost sledovat kybernetické bezpečnostní události, 2) povinnost vyhodnocovat kybernetické bezpečnostní události a 3) informovat zákazníka o kybernetických bezpečnostních událostech. Dílčí požadavky 1 a 2 jsou tržním i legislativním standardem. Jedná se o technické opatření, jak uvádí i důvodová zpráva k tomuto bodu, a i v souvislosti s požadavky směrnice NIS2 se v evropském prostoru jedná o standardní technické opatření.

Nad rámec dílčích bodů 1 a 2 obsahuje tento bod i dílčí bod 3, tedy povinnost ujednat si se zákazníkem, aby poskytovatel informoval zákazníka o kybernetických bezpečnostních událostech. Tento dílčí bod 3 představuje nepřiměřený zásah do smluvní svobody smluvních stran a současně se jedná o požadavek, který jde nad rámec tržního i legislativního standardu. Pro srovnání, například certifikace Cloud Computing Compliance Criteria Catalogue (C5) požaduje první dva dílčí body, ovšem třetí dílčí bod nikoli. Jedná se tedy o unikátní požadavek, který například globální poskytovatelé cloudových služeb běžně nezohledňují. Proto navrhujeme úpravu tohoto bodu tak, že se dílčí bod 3 vypustí.

Tato připomínka je zásadní.

12. <u>K řádku 8.1 přílohy č. 1, 2, 3 a 4 vyhlášky – kybernetické bezpečnostní události</u>

Navrhujeme upravit znění řádku 8.1. přílohy č. 1, 2, 3 a 4 dle návrhu níže.

Navrhovaná změna se vztahuje ke všem bezpečnostním úrovním, vybraná úroveň kritická je pouze demonstrativní, vzhledem k tomu, že se stejný text opakuje ve všech přílohách.

Řádek	**Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni kritická**	**Podklad, kterým poskytovatel doloží splnění požadavku**
8. Testování služby cloud computingu		
8.1	Poskytovatel pravidelně provádí skeny zranitelností služby cloud computingu v intervalu alespoň jeden sken zranitelností každé 3 měsíce a v případě zjištění zranitelností zavádí nápravná opatření.	Tři záznamy o provedení skenů zranitelností ~~**provedených v souladu s platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách,**~~ provedených maximálně 12 měsíců před podáním žádosti o zápis zapisované služby do katalogu cloud computingu, ~~**kdy alespoň jeden z těchto záznamů nebude starší než 3 měsíce před podáním žádosti o zápis zapisované služby do katalogu cloud computingu**~~, ze kterých vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 6 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

Odůvodnění:

Za prvé, uvedená metodika nebyla ze strany NUKIB v okamžiku průběhu připomínkového řízení zveřejněna, a proto není možné posoudit její požadavky. Dále je taková metodika problematická z hlediska aktualizací, kdy není vyjasněno, jak má poskytovatel postupovat v případě aktualizace této metodiky, případně v jakých lhůtách musí poskytovatelé danou aktualizaci reflektovat. Současně je zde riziko, že by metodika nebyla pro poskytovatele zcela vůbec proveditelná, což by mohlo vést k nemožnosti registrovat cloudové služby, resp. k vyškrtnutí stávajících registrací. Proto navrhujeme vyškrtnutí odkazu na uvedenou metodiku NUKIB.

Za druhé dáváme na zvážení, zda-li je relevantní perioda 3 měsíců. Pokud je v SOC reportu uvedeno, že cloud poskytovatel provádí periodické skeny zranitelnosti, je na zvážení, zda-li je tento údaj pro cloudového poskytovatele povinný i s ohledem na časovou náročnost zápisu do katalogu služeb a reakční dobou příslušných institucí.

Tato připomínka je doporučující.

13. **K řádku 8.2 přílohy č. 3 a 4 vyhlášky – metodika provádění penetračních testů**

Navrhujeme upravit znění řádku 8.2. přílohy č. 3 a 4 vyhlášky dle návrhu níže.

Navrhované varianty se vztahují ke všem uvedeným bezpečnostním úrovním v příloze 3 a 4, vybraná úroveň kritická je pouze demonstrativní, vzhledem k tomu, že se stejný text opakuje ve všech uvedených přílohách.

Navrhujeme znění řádku 8.2 přílohy č. 3 a č. 4 upravit následujícím způsobem:

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni kritická	Podklad, kterým poskytovatel doloží splnění požadavku
8. Testování služby cloud computingu		
8.2	Poskytovatel zajišťuje provádění penetračních testů podle standardu NIST 800-115, metodiky OSSTMM, **aktuálně platného standardu OWASP Top 10** nebo standardu OWASP ASVS Level 1 odpovídající charakteru zapisované služby cloud computingu, ~~a~~**anebo** v souladu s aktuálně platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, **nebo v souladu s metodikou FedRAMP**.	Zpráva z provedení penetračního testu, ze které vyplývá splnění požadavku.

A také navrhujeme upravit znění ustanovení § 10 odst. 2 vyhlášky, jak je zároveň uvedeno i v připomínce č. 6 výše, následovně:

„(2) Splnění požadavků v řádcích 8.1 a 8.2 přílohy č. 3 a 4 k této vyhlášce a požadavků na strukturu a náležitosti zprávy o provedení penetračního testu a intervaly pro její předkládání podle § 6 ***je možné doložit dle*** *~~se řídí~~ dosavadní**ch**~~mi~~ právní**ch**~~mi~~ předpis**ů**~~y~~**, a to** po dobu 18 měsíců ode dne nabytí účinnosti této vyhlášky.* ***Bez ohledu na přechodné ustanovení v odst. 1 se požadavky v řádcích 8.1 a 8.2 přílohy č. 3 a 4***

***k této vyhlášce uplatní i na žádosti o zápis nabídky cloud computingu do katalogu cloud computingu podle § 6t zákona podané přede dnem účinnosti této vyhlášky**."*

Odůvodnění:

Předložený legislativní text přináší oproti stávající úpravě požadavků na provádění penetračních testů významné změny. Navrhované znění řádku 8.2 přílohy č. 3 vyhlášky nově stanoví, že mezi přípustné mezinárodní standardy, podle nichž má poskytovatel provádět penetrační testování, již nepatří standard OWASP Top 10. Soulad navíc musí být navíc zajištěn s aktuálně platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost uveřejněnou na jeho internetových stránkách.

Považujeme za nežádoucí, aby požadavky byly stanoveny takto kumulativně – tj. zajišťovat penetrační testy zároveň podle mezinárodně uznávaných standardů a k tomu i podle metodiky Národního úřadu pro kybernetickou a informační bezpečnost. Domníváme se, že takový postup je v rozporu s principem právní jistoty a předvídatelnosti. Metodika Národního úřadu pro kybernetickou a informační bezpečnost nemá charakter právního předpisu a může být jednostranně měněna bez veřejné konzultace. Tento stav vytváří prostor pro svévoli a zvyšuje právní nejistotu, protože poskytovatelé nejsou schopni s dostatečnou mírou předvídatelnosti posoudit, jakým konkrétním způsobem mají být penetrační testy prováděny v daném okamžiku. I z hlediska legislativní systematiky je nežádoucí, aby prováděcí právní předpis, jehož účelem je konkretizace zákonem stanovených povinností, odkazoval na jiný podkladový dokument bez právní závaznosti. To činí právní rámec méně přehledným a komplikuje výklad práv a povinností poskytovatelů, kteří by museli soustavně sledovat rovněž vývoj doporučení, jež nemají charakter právního předpisu. Zároveň takový přístup může významně zvyšovat náklady na straně poskytovatelů, kteří mohou být nuceni neustále obměňovat používané standardy.

Penetrační testování je vysoce specializovaná a technicky sofistikovaná oblast, v níž je již běžnou praxí postupovat podle zavedených a mezinárodně uznávaných standardů. Tyto standardy jsou osvědčené a poskytují dostatečnou míru jistoty i bezpečnosti. Domníváme se proto, že požadavek na souběžné dodržování metodiky Národního úřadu pro kybernetickou a informační bezpečnost představuje v praxi nadbytečnou zátěž, aniž by přinášel reálné bezpečnostní výhody nad rámec toho, co je zajištěno samotným uplatněním příslušných mezinárodních standardů.

Pokud předkladatel trvá na povinnosti zajistit provádění penetračních testů v souladu s metodikou Národního úřadu pro kybernetickou a informační bezpečnost, navrhujeme alespoň, aby její použití nebylo povinné souběžně s mezinárodními standardy, **ale aby bylo možné ji uplatnit alternativně** – tj. že poskytovatel musí předkládat penetrační testy, které jsou v souladu se stanovenými standardy nebo metodikou. Připuštění alternativního způsobu naplnění požadavku by podle našeho názoru nijak nenarušilo jeho účel ani smysl, a zároveň by ponechalo Národnímu úřadu pro kybernetickou a informační bezpečnost prostor k odbornému vyjádření a metodickému vedení v oblasti penetračního testování, pokud si tak přeje.

Dále navrhujeme mezi jednotlivé alternativy doplnit rovněž **mezinárodní metodiku FedRAMP**. Metodika FedRAMP má univerzální strukturu a je plně použitelná pro všechny jakýkoliv typ cloudových služeb (IaaS, PaaS i SaaS). Ač předložený návrh vyhlášky oproti dosavadní právní úpravě vyhlášky č. 316/2021 Sb. odstranil formální rozlišení cloudových služeb na třídy IaaS, PaaS a SaaS. Tento krok vítáme, neboť rigidní kategorizace

způsobovala v praxi poskytovatelům obtíže. U požadavků na penetrační testování však toto rozdělení zůstává fakticky zachováno – poskytovatel je podle návrhu vyhlášky povinen aplikovat takový standard, který odpovídá „*charakteru zapisované služby cloud computingu*“. Poskytovatel musí tak implicitně i nadále zohlednit, zda se jedná o službu typu IaaS, PaaS nebo SaaS. S ohledem na novou systematiku návrhu vyhlášky, která formálně opouští dosavadní kategorizaci, považujeme za vhodné výslovně umožnit využití takové metodiky, která všechny tři třídy cloudových služeb jednotně pokrývá.

Metodika FedRAMP zároveň zajišťuje vysokou úroveň bezpečnosti plně srovnatelnou s požadavky české legislativy. Jedná se o dlouhodobě zavedenou metodiku uznávanou širokou odbornou komunitou, která je pravidelně aktualizovaná s ohledem na aktuální hrozby a technologický vývoj. Metodiku FedRAMP běžně využívají globální poskytovatelé cloudových služeb jako součást svých interních bezpečnostních rámců. Vzhledem k tomu, že se požadavky vyhlášky budou vztahovat i na subjekty s globálním působením a jednotnou standardizací procesů napříč jurisdikcemi, považujeme za žádoucí výslovně umožnit, aby penetrační testování mohlo být prováděno i v souladu s touto mezinárodně uznávanou metodikou.

Doplnění metodiky FedRAMP mezi uznávané metodiky by tedy přispělo k vyšší právní jistotě a předvídatelnosti, aniž by snižovalo úroveň bezpečnosti. Naopak by umožnilo efektivnější a flexibilnější naplňování požadavků vyhlášky, zejména u poskytovatelů, kteří již mají tento rámec implementovaný.

Současně navrhujeme zpětné doplnění **standardu OWASP Top 10** mezi přípustné mezinárodní standardy pro penetrační testování. Neexistuje žádný věcně relevantní důvod pro jeho vyloučení. Standard OWASP Top 10 je mezinárodně uznávaný a široce využívaný rámec, který byl dosud považován za plně vyhovující účelu předmětného požadavku (tj. zajištění odpovídající úrovně penetračního testování). Jeho dosavadní uplatňování se v praxi osvědčilo jako funkční a efektivní a nevykazovalo známky systémového selhání či nedostatků, které by odůvodňovaly jeho náhlé vypuštění.

Není zřejmé, na základě jakých konkrétních skutečností předkladatel dospěl k závěru, že je vhodné tento osvědčený a mezinárodně aprobovaný rámec opustit. Jeho vyloučení by znamenalo neodůvodněné omezení poskytovatelů, kteří mají své interní procesy nastaveny právě v souladu s tímto standardem. Takový krok by pro ně představoval neúměrnou administrativní a technickou zátěž, aniž by přinesl reálný přínos z hlediska zvýšení bezpečnosti.

Navrhujeme, aby se všechny navrhované varianty promítly do praxe okamžitě, a to i pro již probíhající řízení. Není žádný důvod odkládat možnost využití nových standardů, pokud jsou již nyní běžně používané a mezinárodně uznávané.

Všechny navrhované standardy (včetně FedRAMP a OWASP Top 10) by měly být akceptovány bezodkladně, i pro žádosti podané před účinností nové vyhlášky. Neexistuje důvod, proč by nové rámce nebyly uznávány již nyní – jejich praktická využitelnost i mezinárodní validita je zřejmá. Vzhledem k tomu, že jednotlivé standardy budou fungovat alternativně, poskytovatelé si tak mohou vybrat, který rámec zvolí – tím se podporuje flexibilita a nedochází k dodatečnému zatěžování trhu.

Z těchto důvodů by mělo dojít rovněž k úpravě přechodného ustanovení § 10 odst. 2 návrhu vyhlášky, které odkládá účinnost požadavků dle řádků 8.1 a 8.2 přílohy č. 3 a č. 4 o 18 měsíců, a to s cílem poskytnout

poskytovatelům cloudových služeb dostatečný čas na přípravu a implementaci těchto novelizovaných požadavků.

Nicméně přijetím našich návrhů – včetně zpětného zakotvení OWASP Top 10 a výslovného uznání FedRAMP – se značně rozšiřují možnosti, jak lze požadavky na penetrační testování naplnit. Oba standardy jsou již v praxi široce využívány, a proto by poskytovatelé nemuseli nijak zásadně měnit své dosavadní interní postupy. Za této situace se plošný odklad účinnosti jeví jako nadbytečný.

Zvláště upozorňujeme, že metodika FedRAMP je navržena jako univerzálně použitelná napříč typy cloudových služeb (IaaS, PaaS, SaaS) a je mezinárodně respektovaným nástrojem pro prokazování bezpečnosti. Její použití by proto mělo být umožněno i pro řízení, která byla zahájena ještě před účinností nové vyhlášky. Jinak by mohlo docházet k neefektivnímu zamítání žádostí z čistě formálních důvodů – tedy kvůli nesouladu se stávající vyhláškou č. 316/2021 Sb. – přestože tyto žádosti de facto splňují požadavky nové právní úpravy. Takový postup by byl zbytečně zatěžující jak pro poskytovatele, tak pro samotný Úřad, který by tytéž žádosti musel po několika měsících znovu posuzovat a schvalovat.

Pro úplnost navrhujeme alternativní úpravu i pro případ, že nebude akceptováno zpětné doplnění OWASP Top 10. V takové situaci doporučujeme změnit první větu § 10 odst. 2, aby poskytovatelé, kteří tento rámec dosud využívají, mohli jeho použití doložit podle dosavadních předpisů. Zároveň by mělo být výslovně umožněno využití metodiky FedRAMP i bez 18měsíčního odkladu. V případě, že by však ke zpětnému zakotvení standardu OWASP Top 10 došlo, uvedené úpravy v první větě § 10 odst. 2 již nebudou potřeba.

Nad rámec výše uvedeného dále apelujeme na Národní úřad pro kybernetickou a informační bezpečnost, aby v zájmu transparentnosti a právní jistoty zveřejnil příslušnou metodiku, na kterou návrh vyhlášky odkazuje. Povinnost dodržovat „*aktuálně platnou metodiku*“ bez toho, aby tato metodika byla veřejně dostupná, zcela oslabuje právní jistotu regulovaných subjektů a znemožňuje jim odpovědně vůbec posoudit dopad navrhované právní úpravy. To je pochopitelně zcela v rozporu se zásadami transparentního a předvídatelného legislativního procesu.

Tato připomínka je zásadní.

14. K řádku 5.2 přílohy č. 1 vyhlášky – záznam o přístupu k nezašifrovaným zákaznickým datům

Navrhujeme upravit znění řádku 5.2 přílohy č. 1 vyhlášky následujícím způsobem:

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni nízká	Podklad, kterým poskytovatel doloží splnění požadavku
5. Nakládání s daty		
5.2	Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo v daném případě bez přechozího svolení zákazníka. Tento záznam musí obsahovat alespoň důvod, čas, trvání, typ a rozsah přístupu a dostatek dalších údajů potřebných k tomu, aby mohl zákazník vyhodnotit rizikovost tohoto přístupu. Poskytovatel umožňuje zákazníkovi přístup k tomuto záznamu, a za tím účelem jej uchovává alespoň po dobu 7 dní. Poskytovatel nemusí umožňovat přístup k záznamu v případě, že interní a externí pracovníci přistupují k nezašifrovanému zákaznickému obsahu na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat a vyrozumění zákazníka o této žádosti není možné v souladu s bodem 2.1 této přílohy. **V případě, že poskytovatel nemá přístup k nezašifrovaným zákaznickým datům bez svolení zákazníka, pak se tento bod 5.2 neuplatní. Tento bod 5.2 se neuplatní rovněž v případě, že se jedná o veřejně přístupná zákaznická data.**	Část návrhu smluvní dokumentace podle § 9 odst. 6 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 6 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 6 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

Odůvodnění:

V praxi jsou běžná také řešení, v rámci kterých nemůže nastat situace, že by poskytovatel mohl přistoupit k nezašifrovaným zákaznickým datům bez svolení (autorizace) ze strany zákazníka (např. řešení, kde není tzv. „super-admin“). V takovém případě navrhujeme, uvést tuto situaci přímo v rámci požadavku. Doložení by pak mohlo proběhnout formou např. čestného prohlášení. Uvedené reflektuje rovněž metodiku NUKIB k požadavkům pro zápis do katalogu cloud computingu, v rámci něhož uvádí NUKIB následující komentář: „*Toto nemusí splnit v případě, kdy je vyloučeno, že by jeho zaměstnanci nebo zaměstnanci externího subjektu mohli přistoupit k nezašifrovaným datům zákazníka.*“ Aby se předešlo výkladovým problémům, je vhodné toto uvést přímo na úrovni vyhlášky (resp. požadavku).

V praxi dále může nastat situace, kdy zákazník data účelově nešifruje za účelem jejich plošné distribuce a sdílení. Příkladem mohou být obecné webové stránky, veřejně dostupné dokumenty, případně materiály, které vlastník dat (zákazník) určí jako veřejné.

Navrhujeme, aby ustanovení zohlednilo například možnost toho, že vlastník dat (zákazník) stanoví klasifikaci dat a určí, zda-li jsou nešifrovaná data veřejná/neveřejná a zajistí odpovídající dostupnost nešifrovaných zákaznických dat. Zákazník rovněž zajistí. že takto veřejně přístupná nešifrovaná data budou ve stavu read-only, aby nedošlo k jejich nežádoucí modifikaci.

Pokud jsou nezašifrovaná zákaznická data veřejně přístupná, poskytovatel nemusí vyhotovovat záznam o přístupu jeho interních a externích pracovníků. Cílem je zbytečně nezvyšovat administrativní náročnost poskytovatele.

Tato připomínka je zásadní.

15. K řádku 5.3 přílohy č. 2 vyhlášky – záznam o přístupu k nezašifrovaným zákaznickým datům

Navrhujeme upravit znění řádku 5.3 přílohy č. 2 vyhlášky následujícím způsobem:

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni střední	Podklad, kterým poskytovatel doloží splnění požadavku
5. Nakládání s daty		
5.3	Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo v daném případě bez přechozího svolení zákazníka. Tento záznam musí obsahovat alespoň důvod, čas, trvání, typ a rozsah přístupu a dostatek dalších údajů potřebných k tomu, aby mohl zákazník vyhodnotit rizikovost tohoto přístupu. Poskytovatel umožňuje zákazníkovi přístup k tomuto záznamu, a za tím účelem jej uchovává alespoň po dobu 7 dní. Poskytovatel nemusí umožňovat přístup k záznamu v případě, že interní a externí pracovníci přistupují k nezašifrovanému zákaznickému obsahu na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat a vyrozumění zákazníka o této žádosti není možné v souladu s bodem 2.1 této přílohy. **V případě, že poskytovatel nemá přístup k nezašifrovaným zákaznickým datům bez svolení zákazníka nebo se jedná o veřejně přístupná data, pak se tento bod 5.3 neuplatní. Tento bod 5.3 se neuplatní rovněž v případě, že se jedná o veřejně přístupná zákaznická data.**	Část návrhu smluvní dokumentace podle § 9 odst. 6 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 6 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 6 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

Odůvodnění:

V praxi jsou běžná také řešení, v rámci kterých nemůže nastat situace, že by poskytovatel mohl přistoupit k nezašifrovaným zákaznickým datům bez svolení (autorizace) ze strany zákazníka (např. řešení, kde není tzv. „super-admin“). V takovém případě navrhujeme, uvést tuto situaci přímo v rámci požadavku. Doložení by pak

mohlo proběhnout formou např. čestného prohlášení. Uvedené reflektuje rovněž metodiku NUKIB k požadavkům pro zápis do katalogu cloud computingu, v rámci něhož uvádí NUKIB následující komentář: *„Toto nemusí splnit v případě, kdy je vyloučeno, že by jeho zaměstnanci nebo zaměstnanci externího subjektu mohli přistoupit k nezašifrovaným datům zákazníka.*“ Aby se předešlo výkladovým problémům, je vhodné toto uvést přímo na úrovni vyhlášky (resp. požadavku).

V praxi dale může nastat situace, kdy zákazník data účelově nešifruje za účelem jejich plošné distribuce a sdílení. Příkladem mohou být obecné webové stránky, veřejně dostupné dokumenty, případně materiály, které vlastník dat (zákazník) určí jako veřejné.

Navrhujeme, aby ustanovení zohlednilo například možnost toho, že vlastník dat (zákazník) stanoví klasifikaci dat a určí zda-li jsou nešifrovaná data veřejná/neveřejná a zajistí odpovídající dostupnost nešifrovaných zákaznických dat. Zákazník rovněž zajistí. že takto veřejně přístupná nešifrovaná data budou ve stavu read-only, aby nedošlo k jejich nežádoucí modifikaci.

Pokud jsou nezašifrovaná zákaznická data veřejně přístupná, poskytovatel nemusí vyhotovovat záznam o přístupu jeho interních a externích pracovníků. Cílem je zbytečně nezvyšovat administrativní náročnost poskytovatele.

Tato připomínka je zásadní.

16. **K řádku 5.3 přílohy č. 3 vyhlášky – BYOK**

Navrhujeme upravit znění řádku 5.3. přílohy č. 3 následujícím způsobem, tak aby došlo k zajištění zásady přiměřenosti ve vztahu k požadavku na možnost využití vlastního šifrovacího klíče ze strany zákazníka. Níže předkládáme dva alternativní návrhy na změnu tohoto požadavku.

Varianta 1:

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni vysoká	Podklad, kterým poskytovatel doloží splnění požadavku
5. Nakládání s daty		
~~**5.3**~~	~~**Poskytovatel umožňuje zákazníkovi využití vlastních šifrovacích klíčů (BYOK), a to buď jejich vygenerováním v certifikovaném hardware security modulu (HSM modulu) umístěném u poskytovatele pod vzdálenou správou zákazníka, nebo importem těchto klíčů z jiných prostředků pod správou zákazníka.**~~	~~**Část návrhu smluvní dokumentace podle § 9 odst. 6 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, nebo**~~ ~~**část další dokumentace podle § 9 odst. 6 písm. d) této vyhlášky, ze které vyplývá splnění požadavku.**~~

Varianta 2:

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni vysoká	Podklad, kterým poskytovatel doloží splnění požadavku
5. Nakládání s daty		
5.3	Poskytovatel umožňuje zákazníkovi využití vlastních šifrovacích klíčů (BYOK**, HYOK**), a to buď jejich vygenerováním v certifikovaném hardware security modulu (HSM modulu) umístěném u poskytovatele pod vzdálenou správou zákazníka, nebo importem těchto klíčů z jiných prostředků pod správou zákazníka.	Část návrhu smluvní dokumentace podle § 9 odst. 6 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, nebo část další dokumentace podle § 9 odst. 6 písm. d) této vyhlášky, ze které vyplývá splnění požadavku.

Odůvodnění:

K variantě 1:

V prvé řadě navrhujeme vypuštění tohoto požadavku s ohledem na to, že se nejedná o standardní tržní požadavek a není proto běžnou součástí řešení poskytovatelů. V porovnání například se srovnatelnými požadavky Cloud Computing Compliance Criteria Catalogue (C5) se jedná o značně nepřiměřený požadavek, kdy na rozdíl od této certifikace není v rámci vyhlášky přípustná žádná alternativa, co se šifrovacích klíčů týče.

K variantě 2:

Pokud by návrhu na vypuštění tohoto požadavku nebylo vyhověno, pak navrhujeme alespoň rozšíření požadavku o variantu Hold your own key (HYOK). HYOK stejně jako BYOK umožňuje zákazníkovi využití vlastních šifrovacích klíčů. Šifrovací klíče jsou i v případě HYOK pod správou zákazníka. Z hlediska znění požadavku tak lze naplnit požadavek stejně tak prostřednictvím BYOK jako HYOK. Lze rovněž tvrdit, že HYOK může pro zákazníka představovat vyšší míru zabezpečení.

Tato připomínka je zásadní.

17. K řádku 5.5 přílohy č. 3 vyhlášky – záznam o přístupu k nezašifrovaným zákaznickým datům

Navrhujeme upravit znění řádku 5.5 přílohy č. 3 vyhlášky následujícím způsobem:

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni vysoká	Podklad, kterým poskytovatel doloží splnění požadavku
5. Nakládání s daty		
5.5	Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo v daném případě bez přechozího svolení zákazníka. Tento záznam musí obsahovat alespoň důvod, čas, trvání, typ a rozsah přístupu a dostatek dalších údajů potřebných k tomu, aby mohl zákazník vyhodnotit rizikovost tohoto přístupu. Poskytovatel umožňuje zákazníkovi přístup k tomuto záznamu, a za tím účelem jej uchovává alespoň po dobu 7 dní. Poskytovatel nemusí umožňovat přístup k záznamu v případě, že interní a externí pracovníci přistupují k nezašifrovanému zákaznickému obsahu na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat a vyrozumění zákazníka o této žádosti není možné v souladu s bodem 2.1 této přílohy. **V případě, že poskytovatel nemá přístup k nezašifrovaným zákaznickým datům bez svolení zákazníka nebo se jedná o veřejně přístupná data, pak se tento bod 5.5 neuplatní. Tento bod 5.5 se neuplatní rovněž v případě, že se jedná o veřejně přístupná zákaznická data.**	Část návrhu smluvní dokumentace podle § 9 odst. 6 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 6 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 6 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

Odůvodnění:

V praxi jsou běžná také řešení, v rámci kterých nemůže nastat situace, že by poskytovatel mohl přistoupit k nezašifrovaným zákaznickým datům bez svolení (autorizace) ze strany zákazníka (např. řešení, kde není tzv. „super-admin“). V takovém případě navrhujeme, uvést tuto situaci přímo v rámci požadavku. Doložení by pak mohlo proběhnout formou např. čestného prohlášení. Uvedené reflektuje rovněž metodiku NUKIB k požadavkům pro zápis do katalogu cloud computingu, v rámci něhož uvádí NUKIB následující komentář: „*Toto nemusí splnit v případě, kdy je vyloučeno, že by jeho zaměstnanci nebo zaměstnanci externího subjektu mohli přistoupit k nezašifrovaným datům zákazníka.*“ Aby se předešlo výkladovým problémům, je vhodné toto uvést přímo na úrovni vyhlášky (resp. požadavku).

V praxi dále může nastat situace, kdy zákazník data účelově nešifruje za účelem jejich plošné distribuce a sdílení. Příkladem mohou být obecné webové stránky, veřejně dostupné dokumenty, případně materiály, které vlastník dat (zákazník) určí jako veřejné.

Navrhujeme, aby ustanovení zohlednilo například možnost toho, že vlastník dat (zákazník) stanoví klasifikaci dat a určí, zda-li jsou nešifrovaná data veřejná/neveřejná a zajistí odpovídající dostupnost nešifrovaných zákaznických dat. Zákazník rovněž zajistí. že takto veřejně přístupná nešifrovaná data budou ve stavu read-only, aby nedošlo k jejich nežádoucí modifikaci.

Pokud jsou nezašifrovaná zákaznická data veřejně přístupná, poskytovatel nemusí vyhotovovat záznam o přístupu jeho interních a externích pracovníků. Cílem je zbytečně nezvyšovat administrativní náročnost poskytovatele.

Tato připomínka je zásadní.

18. K řádku 5.4 přílohy č. 4 vyhlášky – záznam o přístupu k nezašifrovaným zákaznickým datům

Navrhujeme upravit znění řádku 5.4 přílohy č. 4 vyhlášky následujícím způsobem:

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni kritická	Podklad, kterým poskytovatel doloží splnění požadavku
5. Nakládání s daty		
5.4	Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo v daném případě bez přechozího svolení zákazníka. Tento záznam musí obsahovat alespoň důvod, čas, trvání, typ a rozsah přístupu a dostatek dalších údajů potřebných k tomu, aby mohl zákazník vyhodnotit rizikovost tohoto přístupu. Poskytovatel umožňuje zákazníkovi přístup k tomuto záznamu, a za tím účelem jej uchovává alespoň po dobu 7 dní. Poskytovatel nemusí umožňovat přístup k záznamu v případě, že interní a externí pracovníci přistupují k nezašifrovanému zákaznickému obsahu na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat a vyrozumění zákazníka o této žádosti není možné v souladu s bodem 2.1 této přílohy. **V případě, že poskytovatel nemá přístup k nezašifrovaným zákaznickým datům bez svolení zákazníka nebo se jedná o veřejně přístupná data, pak se tento bod 5.4 neuplatní. Tento bod 5.4 se neuplatní rovněž v případě, že se jedná o veřejně přístupná zákaznická data.**	Část návrhu smluvní dokumentace podle § 9 odst. 6 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 6 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 6 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

Odůvodnění:

V praxi jsou běžná také řešení, v rámci kterých nemůže nastat situace, že by poskytovatel mohl přistoupit k nezašifrovaným zákaznickým datům bez svolení (autorizace) ze strany zákazníka (např. řešení, kde není tzv. „super-admin“). V takovém případě navrhujeme, uvést tuto situaci přímo v rámci požadavku. Doložení by pak

mohlo proběhnout formou např. čestného prohlášení. Uvedené reflektuje rovněž metodiku NUKIB k požadavkům pro zápis do katalogu cloud computingu, v rámci něhož uvádí NUKIB následující komentář: *„Toto nemusí splnit v případě, kdy je vyloučeno, že by jeho zaměstnanci nebo zaměstnanci externího subjektu mohli přistoupit k nezašifrovaným datům zákazníka.*“ Aby se předešlo výkladovým problémům, je vhodné toto uvést přímo na úrovni vyhlášky (resp. požadavku).

V praxi dale může nastat situace, kdy zákazník data účelově nešifruje za účelem jejich plošné distribuce a sdílení. Příkladem mohou být obecné webové stránky, veřejně dostupné dokumenty, případně materiály, které vlastník dat (zákazník) určí jako veřejné.

Navrhujeme, aby ustanovení zohlednilo například možnost toho, že vlastník dat (zákazník) stanoví klasifikaci dat a určí zda-li jsou nešifrovaná data veřejná/neveřejná a zajistí odpovídající dostupnost nešifrovaných zákaznických dat. Zákazník rovněž zajistí. že takto veřejně přístupná nešifrovaná data budou ve stavu read-only, aby nedošlo k jejich nežádoucí modifikaci.

Pokud jsou nezašifrovaná zákaznická data veřejně přístupná, poskytovatel nemusí vyhotovovat záznam o přístupu jeho interních a externích pracovníků. Cílem je zbytečně nezvyšovat administrativní náročnost poskytovatele.

Tato připomínka je zásadní.

19. **K řádkům s názvem *„Pro řádek 8.2 přílohy č. 3 a 4 k této vyhlášce*“ přílohy č. 6 vyhlášky – způsob doložení provádění penetračních testů**

Navrhujeme řádky s názvem *„Pro řádek 8.2 přílohy č. 3 a 4 k této vyhlášce*“ přílohy č. 6 vyhlášky upravit následujícím způsobem:

Požadavky na strukturu a náležitosti zprávy o provedení penetračního testu	
Pro řádek 8.2 přílohy č. 3 a 4 k této vyhlášce	Zprávu z provedení penetračního testu provedeného podle **standardu NIST 800-115, metodiky OSSTMM, aktuálně platného standardu OWASP Top 10 nebo standardu OWASP ASVS Level 1 odpovídající charakteru zapisované služby cloud computingu, anebo podle** platné metodiky vydané Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách**, nebo podle metodiky FedRAMP.**
Poskytovatel dodá každých 24 měsíců evidence služby cloud computingu v katalogu cloud computingu Digitální a informační agenturou	
Pro řádek 8.2 přílohy č. 3 a 4 k této vyhlášce	Zprávu z provedení penetračního testu provedeného podle **standardu NIST 800-115, metodiky OSSTMM, aktuálně platného standardu OWASP Top 10 nebo standardu OWASP ASVS Level 1 odpovídající charakteru zapisované služby cloud computingu, anebo podle** platné metodiky vydané Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách**, nebo podle metodiky FedRAMP.** Zpráva z provedení penetračního testu nesmí být starší než 24 měsíců od data vyhotovení předchozí předložené zprávy o provedení penetračního testu. Z předložené zprávy o provedení penetračního testu nebo z auditní zprávy podle § 9 odst. 6 písm. e) této vyhlášky nebo prohlášení o

	aplikovatelnosti dokládaných podle přílohy č. 5 musí vyplývat, že poskytovatel zavádí nápravná opatření vzhledem k nálezům předchozích penetračních testů.

Odůvodnění:

V návaznosti na náš připomínkovací návrh k řádku 8.2 přílohy č. 3 a č. 4 navrhujeme provést odpovídající změnu rovněž v navrhované příloze č. 6 vyhlášky, která na tento požadavek přímo navazuje. V rámci připomínkovacího návrhu navrhujeme provést odpovídající úpravy přílohy č. 6 vyhlášky, tj. (1) doplnění možnosti dokládání provádění penetračních testů rovněž podle metodiky FedRAMP; (2) zpětné doplnění mezinárodních standardů a metodik, včetně standardu OWASP Top 10; a (3) umožnění poskytovateli zvolit si příslušnou metodiku, tedy aby nebyl povinen postupovat výlučně podle metodiky vydané Národním úřadem pro kybernetickou a informační bezpečnost, pokud využívá jiný mezinárodně uznávaný rámec, který zajišťuje srovnatelnou úroveň bezpečnosti.

Pokud jde o podrobnější odůvodnění, plně odkazujeme na náš připomínkovací návrh k řádku 8.2 přílohy č. 3 a č. 4.

Tato připomínka je zásadní.