Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.J. NEPŘIDĚLENO • BRNO • 27. BŘEZNA 2024

VERZE DOKUMENTU: 1.1

PRŮVODCE DOKLÁDÁNÍ POŽADAVKŮ PRO ZÁPIS SLUŽBY CLOUD COMPUTINGU PODLE PŘÍLOHY Č. 2 VYHLÁŠKY Č. 316/2021 SB.

PRO STŘEDNÍ, VYSOKOU A KRITICKOU BEZPEČNOSTNÍ ÚROVEŇ

Obsah

1 Úvod

Účelem tohoto dokumentu je nabídnout poskytovatelům služeb cloud computingu (dále jen „poskytovatelé“) metodickou pomůcku, která je provede základními pojmy, postupy a typickými problémy, s nimiž se mohou setkat při přípravě své žádosti o zápis nabídky cloud computingu do katalogu cloud computingu[1] (dále jen „žádost“).

Dosavadní zkušenosti se zápisy jednotlivých nabídek služeb totiž ukázaly, že se při přípravě svých žádostí mohou poskytovatelé potýkat s nepředpokládanými problémy ohledně určitých pojmů a jednotlivých způsobů doložení, se kterými operuje vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „vyhláška“), případně se objevují výkladové nejasnosti. Tento materiál si klade za cíl těmto opakujícím se problémům předcházet a snížit tak počet žádostí, které se vracejí k doplnění, případně k dalšímu vysvětlení, na nezbytné minimum, což povede zejména k úspoře času a nákladů na straně poskytovatelů.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31

616 00 Brno – Žabovřesky

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

[1] Dostupný na webových stránkách Digitální a informační agentury: Katalog cloud computingu – Digitální a informační agentura (gov.cz).

2 Právní rámec

Poskytování služeb cloud computingu veřejné správě je upraveno zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění účinném od 1. září 2021 (dále jen „ZoISVS“). Ten v § 6l ZoISVS stanovuje, že každý, kdo chce poskytovat služby cloud computingu, jimiž je zajištěn provoz informačních systémů veřejné správy (dále jen „ISVS“), musí být zapsán do katalogu cloud computingu, stejně tak jako každá služba cloud computingu, která je nabízena nebo poskytována pro zajištění provozu ISVS. Digitální a informační agentura (dále jen „DIA“) vede tento katalog a zároveň obecně koordinuje využívání cloud computingu orgány veřejné správy.

Zápis do katalogu je prováděn na žádost v rámci správního řízení a probíhá ve dvou fázích, kdy je nejprve zapsána osoba poskytovatele a následně až jím nabízené služby. Zároveň je dle § 6n písm. e) a f) ZoISVS podmínkou, že pokud je poskytování zapisované služby cloud computingu závislé na využití jiné služby nebo služeb cloud computingu, je třeba, aby tento cloud computing a jeho poskytovatel byli rovněž v katalogu zapsáni.

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) do řízení o zápisu do katalogu cloud computingu vstupuje v několika specifických situacích:

- při zápisu poskytovatele cloud computingu, kdy si dle § 6r odst. 1 ZoISVS DIA od NÚKIB vyžádá **závazné stanovisko** pro účely posouzení splnění požadavků dle § 6m odst. 1 písm. a) ZoISVS,
- při zápisu poskytovatele cloud computingu, kdy je dle § 6r odst. 5 ZoISVS DIA oprávněna vyžádat si od NÚKIB **informace** pro účely posouzení splnění požadavků dle § 6m odst. 1 písm. c) ZoISVS a
- při zápisu služby cloud computingu do bezpečnostní úrovně[2] střední, vysoká nebo kritická[3], kdy si dle § 6u odst. 1 ZoISVS DIA od NÚKIB vyžádá závazné stanovisko pro účely posouzení splnění požadavků dle § 6n písm. b) a e) ZoISVS.

Právě poslední z uvedených situací je věnován tento průvodce, přesněji tedy zápisu služeb cloud computingu, které jsou zařazené do bezpečnostní úrovně střední, vysoká a kritická. Vydání závazného stanoviska NÚKIB je podmíněno posouzením dané služby cloud computingu z hlediska

[2] Bezpečnostní úroveň pro využívání cloud computingu orgány veřejné moci vyjadřuje možné dopady kybernetického bezpečnostního incidentu na poptávaný cloud computing. Bezpečnostní úrovně jsou nízká, střední, vysoká nebo kritická. Dle vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, v návaznosti na § 4 odst. 5 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZKB“) musí orgán veřejné správy před uzavřením smlouvy o poskytování služeb cloud computingu zařadit poptávaný cloud computing, kterým se rozumí informační nebo komunikační systém jako celek nebo jeho část, které mohou být provozovány pomocí cloud computingu, do jedné z bezpečnostních úrovní dle této vyhlášky. Poté může dle § 6n písm. d) ZoISVS využívat pouze cloud computing, který je zařazen ve stejné nebo vyšší bezpečnostní úrovni jako jím poptávaný cloud computing.

[3] Dle § 6m odst. 2 ZoISVS může poskytovatelem cloud computingu poskytujícím orgánu veřejné správy cloud computing zařazený do nejvyšší bezpečnostní úrovně být pouze poskytovatel státního cloud computingu.

naplnění požadavků vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu, zejména přílohy č. 2.

3 Obecné požadavky při dokládání splnění požadavků

Obecnými požadavky a základními pojmy, které prostupují konkrétní požadavky v přílohách, se věnuje samotné paragrafové znění vyhlášky. Je třeba zohledňovat tyto požadavky při dokládání splnění jednotlivých konkrétních požadavků dle příloh a nevnímat přílohy jako stojící samy o sobě.

3.1 Požadavky na strukturu a náležitosti podkladů k ověření splnění požadavků

Struktura podkladů k ověření splnění požadavků podle § 3 a 4 vyhlášky musí být **přehledná** a **srozumitelná**. Splnění tohoto požadavku lze docílit tím, že poskytovatel ve formuláři[4] popíše každou jednotlivou službu cloud computingu, kterou žádá zapsat do katalogu cloud computingu, a pro každou z nich doloží splnění požadavků podle § 4 vyhlášky.

V případě, že více zapisovaných služeb spadajících do totožné bezpečnostní úrovně nabízeného cloud computingu a totožné třídy cloud computingu splňuje požadavek podle § 4 stejně, je možné doložit splnění takového požadavku pro všechny tyto služby dohromady pouze jednou a následně jednoznačně uvést všechny služby cloud computingu, na které se toto doložení vztahuje.[5]

Podklady pro ověření splnění požadavků podle § 3 a 4 vyhlášky musí obsahovat:

- identifikaci poskytovatele podle § 37 odst. 2 správního řádu (list „Identifikační údaje“ ve formuláři),
- popis splnění každého požadavku pro každou službu cloud computingu, kterou poskytovatel žádá zapsat do katalogu cloud computingu, popřípadě jasný popis skutečnosti, kterou poskytovatel dokládá splnění požadavku ve sloupci „Podklad, kterým poskytovatel doloží splnění požadavku“ přílohy č. 2 vyhlášky (list „Podklady k ověření IaaS-PaaS“ nebo „Podklady k ověření SaaS“ ve formuláři)[6] a
- podklady, kterými poskytovatel doloží splnění požadavku (tj. samostatné přílohy).[7]

V případě, že je pro doložení splnění požadavků podle § 3 a 4 vyhlášky nezbytné odkázat do jiného dokumentu, který je k formuláři připojen, učiní tak poskytovatel ve formuláři uvedením kapitoly, strany, odstavce a případně i konkrétní věty.[8] **Je potřeba důsledně odkazovat na konkrétní části dokládaných dokumentů**. Odkaz na webovou stránku není uznatelný, jelikož podoba webových stránek se mění v čase. Místo odkazu na webovou stránku lze doložit splnění požadavku například snímkem webové stránky nebo jiným dokumentem, který daný obsah webové stránky ukotví v čase.

[4] Žádost o zápis nabídky služeb cloud computingu je podávána na standardizovaném formuláři, který na svých webových stránkách, společně s metodickou podporou k jeho vyplnění, zveřejňuje DIA: Metodiky, návody, formuláře – Digitální a informační agentura (gov.cz).
[5] § 9 odst. 1 vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu
[6] § 9 odst. 2 vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu
[7] § 9 odst. 2 vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu
[8] § 9 odst. 4 vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu

3.1.1 Čestné prohlášení

V případě, že je splnění některého z požadavků podle § 3 a 4 vyhlášky dokládáno čestným prohlášením, musí z něho být patrné, kdo a kdy jej činí a co se jím dokládá. V případě, že čestné prohlášení činí osoba odlišná od poskytovatele, je přílohou žádosti o zápis nabídky cloud computingu do katalogu cloud computingu i doklad o zmocnění opravňující tuto osobu k tomuto čestnému prohlášení.[9]

3.1.2 Názvy služeb

Názvy služeb by neměly být zkracovány, překládány do českého jazyka a neměly by obsahovat překlepy. V opačném případě totiž mohou tyto nedostatky vyvolávat pochybnosti o určitosti vymezení zapisovaných služeb, komplikují vyhledávání a zároveň způsobují nepřehlednost žádosti. Takový nedostatek lze zhojit dokumentem, který účelově popisuje označení, zkratky, cizojazyčná znění služeb.

3.1.3 Balíčky služeb

Jestliže jsou nabízené služby rozděleny do jednotlivých balíčků služeb, je třeba tyto balíčky služeb jednoznačně definovat. Někteří poskytovatelé dokládají dokumenty, které se vztahují k celému balíčku služeb, ale nejsou v nich jmenovány služby jednotlivě. Pokud není jasné, jaké služby do daného balíčku služeb spadají, není možné určit, pro které nabízené služby je splnění požadavku daným dokumentem doloženo. Takový nedostatek lze zhojit přiložením samostatného dokumentu, kde bude deklarován rozsah služeb, pro který je podklad o splnění požadavku dokládán, nebo přímo ve formuláři *Žádosti o zápis nabídky cloud computingu* obdobnou deklarací. Obdobně to platí i u certifikátů, které nemají konkrétně určený rozsah obsažených služeb, např. ISO. I zde je nutné připojit samostatný dokument (např. čestné prohlášení), ze kterého bude jasně patrné, jakých služeb se taková certifikace týká.

3.1.4 Vazba prokazovaných skutečností pro zapisované služby

Při dokládání požadovaných dokumentů je nutné, aby vazba prokazovaných skutečností ke konkrétním nabízeným službám byla jasná. Popisované splnění požadavku v doložených dokumentech nesmí pokrývat jen část zapisovaných služeb.

3.1.5 Typy požadavků

Příloha č. 2 vyhlášky stanovuje dva typy požadavků na služby cloud computingu:

- Požadavek na zajištění: Poskytovatel musí prokázat, že zapisovaná služba automaticky (by default) zákazníkovi zajišťuje danou funkcionalitu.
    - Příklad požadavkem řádku 7.2
        - *„Poskytovatel **chrání** zákaznický obsah šifrováním při přenosu a v úložištích ve službě cloud computingu“*

[9] § 9 odst. 6 vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu

- Příklad požadavkem řádku 6.4
  - *„Poskytovatel **zajišťuje**, že […]“*

- Požadavek na dostupnost: Poskytovatel musí prokázat, že daná služba alespoň nabízí zákazníkovi danou funkcionalitu (umožňuje její využití).
  - Příklad požadavkem řádku 7.3
    - *„Poskytovatel **umožňuje** ochranu zákaznického obsahu šifrováním při přenosu a v úložištích ve službě cloud computingu pomocí některého z algoritmů uvedených v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost.“*
  - Příklad požadavkem řádku 4.1
    - *„Poskytovatel **je schopen** zajišťovat dostupnost služby cloud computingu s nepřetržitou provozní dobou […]“*

3.1.6 Odůvodněné neuplatnění požadavků vyhlášky

Pokud má poskytovatel za to, že se určitý požadavek na danou konkrétní službu neuplatní, je třeba toto explicitně uvést v dané kolonce formuláře, případně v samostatném dokumentu s uvedením názvu dané konkrétní služby, a zdůvodnit, proč tomu tak je, případně takové tvrzení prokázat dokumenty.[10]

3.2 Základní pojmy

Je nutné upozornit na skutečnost, že některé požadavky uvedené v příloze č. 2 této vyhlášky využívají specifické pojmy. Význam těchto pojmů je buď vysvětlen v samotném textu vyhlášky nebo v důvodové zprávě k této vyhlášce.[11] Při předkládání dokumentů k prokázání splnění požadavků uvedených v jednotlivých řádcích přílohy č. 2 je nezbytné, aby tyto dokumenty pracovaly s touto definovanou terminologií. Dokládané dokumenty mohou používat jiné pojmy, ale poskytovatel musí objasnit, že se obsahově shodují s pojmy užívanými ve vyhlášce.

Jako častý nedostatek lze uvést takový způsob doložení, kdy doložený podklad obsahuje pojem osobní údaj, ačkoliv požadavek vyžaduje splnění požadavku pro zákaznická data či specifické provozní údaje, což nejsou obsahově nutně překrývající se pojmy.

3.2.1 Obecné pojmy

Zákaznická data jsou všechna data, která jsou uživatelem poskytnuta poskytovateli v průběhu užívání služby cloud computingu.

[10] Jako příklad lze uvést požadavek v řádku 7.8 a 7.9. Jestliže poskytovatel nepřistupuje k nezašifrovaným zákaznickým datům, nemusí daný požadavek dokládat, musí nicméně tuto skutečnost uvést ve formulářové žádosti. Pokud však existuje dokument, který takové tvrzení poskytovatele osvědčuje, měl by na něj odkázat.

[11] Důvodová zpráva k vyhlášce je dostupná zde: 2021-08-31_oduvodneni_vyhlaska-vstupni-kriteria.pdf (gov.cz)

Pokud jsou některá zákaznická data obsažena v provozních údajích, neztrácejí tím povahu zákaznických dat. Stále se bude jednat o zákaznická data.

Zákaznický obsah textová, zvuková, audiovizuální, obrazová nebo jiná data, která byla uživatelem do služby cloud computingu vložena, a to bez jejich metadat, a indexy k těmto datům.

Provozní údaje jsou data vygenerovaná nebo odvozená poskytovatelem v souvislosti s poskytováním služby cloud computingu.

Specifické provozní údaje jsou takové provozní údaje, které obsahují informace o identifikovaném nebo identifikovatelném uživateli. Jedná se o 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 vyhláška takovým údajům, které se svým významem blíží osobním údajům (a často jimi i jsou), poskytuje adekvátní ochranu a reflektuje tak požadavky vyplývající z práva na informační sebeurčení.

Zpracováním v širším smyslu se rozumí jakákoliv operace nebo soubor operací se zákaznickými daty a provozními údaji v elektronické podobě, prováděné pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, přenos či zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Neaktivní data (data at rest) jsou 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).

Ukládáním dat (údajů) ve stavu neaktivních dat se rozumí nepřetržité uložení dat v úložišti (v datovém centru), tj. neaktivními daty (data at rest) jsou data uložená a skladovaná v trvalém úložišti. Jde je dát do kontrastu s daty aktivními (data in use), která jsou v daném okamžiku zpracovávána (tj. zpracování dat v užším smyslu), a přenášenými daty (data in transit, in motion), tedy daty přenášenými po síti.

Bezpečnostní úrovní nabízeného cloud computingu se rozumí taková bezpečnostní úroveň, do které nabízený cloud computing řadí poskytovatel.

3.2.2 Pojmy související s pojmenováním forem dokládání splnění jednotlivých požadavků

Vedle výše uvedených pojmů dále vyhláška pracuje s pojmenováním forem dokládání splnění jednotlivých požadavků. Tyto můžeme rozdělit následovně:

Písemný popis, kterým se rozumí dokument, který poskytovatel typicky vyhotovuje jen pro účely žádosti o zapsání do katalogu. Je jím prohlašována skutečnost, u které není vyžadována žádná z ostatních forem, má typicky podobu samostatného dokumentu (na který je odkazováno ve formuláři) nebo prohlášení přímo v kolonce formuláře. Stále ovšem platí, že pokud je splnění

jakéhokoliv z požadavků prokazováno tímto způsobem, je třeba, aby z písemného popisu jasně vyplývalo, na které všechny služby se vztahuje a vůči kterému požadavku.

Čestné prohlášení je podobné písemnému popisu, rozdílem je, že je vždy nutná podoba samostatného dokumentu, na který je ve formuláři odkazováno. Mimo konkrétní rozsah služeb, ke kterým se čestné prohlášení vztahuje, a uvedení požadavku, jehož splnění je jím prokazováno, musí být zjevné, kdo konkrétně toto čestné prohlášení činí a jeho oprávnění jednat za poskytovatele. Čestné prohlášení stačí opatřit prostým podpisem.

Dokumentace (budoucího) smluvního závazku, do které spadají smluvní podmínky nebo jejich část, podmínky poskytování služby nebo jejich část, návrh smluvní dokumentace nebo jeho část, návrh smlouvy nebo jeho část, dokumenty oddělené od podmínek poskytování služby nebo smlouvy, produktová specifikace a jiné popisy služby cloud computingu; do této kategorie patří veškerá dokumentace, která bude v budoucnu zakládat nebo upravovat dvoustranný právní vztah mezi poskytovatelem služby a zákazníkem. Zejména v těchto dokumentech je třeba zajistit, že jejich pojmosloví odpovídá pojmům užívaným ve vyhlášce, jelikož je časté, že poskytovatel nepřipravuje smlouvy a smluvní podmínky pro účely žádosti o zápis služby do katalogu, ale již s nějakými návrhy smluvní dokumentace pracuje. V takových případech není potřeba přepisovat návrhy smluvní dokumentace tak, aby byla terminologicky v souladu s vyhláškou, postačí, pokud obsahově požadavky vyhlášky naplňuje. Poskytovatel zároveň připojí písemný popis, kde bude vztah mezi terminologií návrhu smluvní dokumentace a vyhlášky objasněn. Rovněž je u těchto podkladů zásadní, aby obsahovaly výčet služeb, ke kterým se vztahují.

Technická dokumentace je podkladem, který není součástí smluvní dokumentace, ale popisem určitých technických vlastností služby nebo vnitřních postupů a procesů, se kterými je v rámci ní operováno.

Auditní zprávou vydanou pro certifikaci/atestaci[12] a částí platné certifikace[13] se rozumí buď celá auditní zpráva, na jejímž základě byla poskytovateli daná certifikace či atestace udělena, nebo ta její část, ze které vyplývá splnění daného požadavku vyhlášky. Pokud je tento podklad vyžadován, nepostačí doložení certifikace či atestace jako takové, jelikož ta nemá ohledně splnění daného požadavku potřebnou výpovědní hodnotu. Zároveň je opět třeba ve formuláři odkazovat na konkrétní kapitolu, stranu, odstavec a případně i konkrétní větu, ze kterých splnění daného požadavku vyplývá. Oproti tomu pro doložení splnění požadavků řádků 6.1, 8.2, 8.3, 8.4, 8.5 a 8.6, jak ze samotného znění popisu požadovaných podkladů vyplývá, postačí **certifikace** jako taková. Výjimkou je dokládání splnění požadavku skrze auditní zprávu **SOC 2® Type 2** nebo auditní zprávou o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue **C5** ve formě Type 2 (např. v řádku 8.7), které jsou ze své podstaty vždy dokládány

[12] Jak je uvedeno např. v řádcích 2.1, 2.2, 2.3, 2.4, 2.6, 4.1, 4.2, 6.1, 6.2, 6.3, 6.4, 6.7, 7.2, 7.8, 7.9, 9.1, 9.2 a 10.1.
[13] Jak je uvedeno např. v řádcích 1.3, 1.4, 1.8, 6.4, 6.5 a 6.6.

v podobě kompletní auditní zprávy. Splnění některých požadavků je třeba zároveň doložit i **prohlášením o aplikovatelnosti**, jehož vzor je k nalezení na webových stránkách NÚKIB.[14]

Pokud jsou auditní zprávy, popřípadě certifikáty, vydány nikoli na poskytovatele, nýbrž na jeho organizační složku (odštěpný závod/divizi) odlišného názvu, která však nemá vlastní právní subjektivitu, lze je pro zápis služeb cloud computingu poskytovatele do katalogu použít, nicméně poskytovatel musí v takovém případě doložit čestné prohlášení, z něhož bude vyplývat,
že organizační složka je jeho přímou součástí a auditní zpráva, popřípadě certifikace, se tak vztahuje přímo na služby poskytovatele.

[14] Národní úřad pro kybernetickou a informační bezpečnost – Podpůrné materiály (gov.cz)

4 Časté nedostatky při dokládání splnění některých požadavků vyhlášky

Během posuzování splnění požadavků dle přílohy č. 2 vyhlášky poskytovateli jsme postupně shromáždili informace o požadavcích těch řádků, u kterých je v dokládání jejich splnění často chybováno. V této části budou tyto požadavky podrobněji rozebrány buď specificky pro daný konkrétní požadavek, nebo demonstrativně, kdy informace uvedené u daného požadavku lze použít obdobně u požadavků dalších.

V jednotlivých podkapitolách naleznete:

- **Popis požadavku**: obsahující požadavek pro popisovaný řádek,
- **Popis podkladu k doložení splnění požadavku**: obsahující podklad, kterým poskytovatel doloží splnění požadavku a
- **Komentář NÚKIB**: obsahující pomocné informace a doporučení poskytovatelům při procesu dokládání splnění požadavků

4.1 Řádek – 1. Místo zpracování a uložení dat

Podstatným prvkem a zároveň rizikem při využívání služeb cloud computingu je skutečnost, že zákazník předává svá data a informace poskytovateli cloud computingu. Poskytovatelem cloud computingu mnohdy může být zahraniční společnost, podléhající jurisdikci cizích států jak v Evropské unii a státech, které jsou členskými státy Evropského sdružení volného obchodu, tak ale i mimo Evropskou unie a Evropské sdružení volného obchodu. Zároveň jsou data při využívání služby cloud computingu ukládána na území států v Evropské unie a Evropského sdružení volného obchodu. Řádky 1 zavádí několik požadavků na poskytovatele cloud computingu, resp. na místo uložení a zpracování dat, které mají do této oblasti přinést více transparentnosti tak, aby si zákazníci byli uvedeného rizika vědomi a mohli ho zohlednit při rozhodování, zda služby cloud computingu využijí.

Poskytovatel cloud computingu doloží seznam všech lokalit, ve kterých bude docházet ke zpracovávání zákaznických dat a specifických provozních údajů. Lokalitu je nutné doložit minimálně na úroveň státu, ve kterém bude docházet k výše uvedenému zpracovávání. V souladu s výše uvedeným poskytovatel doloží také seznam všech lokalit, ve kterých je prováděn výkon správy a dohledu nad službou, zákaznickými daty a specifickými provozními údaji.

4.1.1 Řádek 1.3

Požadavek:

Zákaznická data ve stavu neaktivních dat jsou ukládána nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu.

V případě, že služba cloud computingu daný požadavek nesplňuje, poskytovatel takovou službu jasně označuje a uvádí, zda taková služba cloud computingu ukládá zákaznická data ve stavu neaktivních dat v pseudonymizované podobě nebo nepseudonymizované podobě.

Poskytovatel uvádí místo uložení zákaznických dat ve stavu neaktivních dat.

Na základě označení služby cloud computingu jako služby cloud computingu, která nesplňuje požadavek na uložení zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, bude tato služba cloud computingu uvedena na internetových stránkách Národního úřadu pro kybernetickou a informační bezpečnost a daný požadavek se na ni neuplatní. Taková služba cloud computingu bude rovněž označena v katalogu cloud computingu jako služba cloud computingu zapsaná na základě uvedené výjimky citací uvedené výjimky.

Podklad k doložení splnění požadavku:

Odkaz na část smluvních podmínek, kde je vymezen závazek uložení zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu,

nebo v případě, že se požadavek uložení zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu nevztahuje na danou službu, jasné označení takové služby a zároveň odkaz na část smluvních podmínek, kde je vymezen závazek uložení zákaznických dat ve stavu neaktivních dat v pseudonymizované podobě,

nebo v případě, že se požadavek uložení zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu neuplatní na danou službu

a zároveň taková služba ukládá zákaznická data ve stavu neaktivních dat v nepseudonymizované podobě, jasné označení takové služby.

Poskytovatel dále doloží odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF) nebo auditní zprávu SOC 2® Type 2, s odkazem na tu část, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ve kterých budou zákaznická data uložena ve stavu neaktivních dat s označením, zda jsou nebo nejsou v daném datovém centru uložena v pseudonymizované podobě.

Schéma doložení splnění požadavku viz příloha č. 1

Komentář NÚKIB:

Současné znění vyhlášky stanoví pro řádek 1.3 požadavek, aby zákaznická data ve stavu neaktivních dat byla ukládána výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu. Některé služby tyto požadavky (např. z technologických důvodů) nesplňují. Přesto bylo žádoucí, aby i tyto služby bylo možné zapsat do katalogu cloud computingu. Z tohoto důvodu existuje možnost zapsat tyto služby na základě výjimky, o kterou se poskytovatel přihlásí tím, že takové služby označí ve své žádosti jako nesplňující požadavky řádku 1.3. Po zápisu do katalogu cloud computingu jsou takové služby uvedeny na internetových stránkách Úřadu a taktéž budou označeny v katalogu cloud computingu. Cílem je, aby orgány veřejné správy mohly ve svých ISVS tyto služby využívat, ale zároveň byly informovány o tom, že jejich data mohou být ukládány v jiném režimu než u služeb ostatních.

Zápis na základě výjimky nemá vliv na bezpečnost služby a všechny služby zapsané v katalogu cloud computingu nabízejí takovou bezpečnost, jakou požaduje vyhláška. U těchto služeb je však nutné věnovat zvýšenou pozornost riziku vyplývajícímu z uchovávání dat ve třetích zemích.

Specifická situace nastává ve chvíli, kdy je poskytování poskytovatelem zapisované služby cloud computingu závislé na využití cloud computingu jiného poskytovatele (tj. jeho materiálního dodavatele), který je již zapsaný v katalogu cloud computingu. Typicky jde o zápis služby SaaS, která využívá již zapsané služby IaaS a PaaS. V takovém případě poskytovatel zapisované služby může namísto výše uvedených dokladů explicitně odkázat na doklady, které jeho materiální dodavatel předložil s jeho vlastní žádosti o zápis služeb do katalogu, a to buď v plném rozsahu, nebo s deklarací rozdílů v místech ukládání zákaznických dat mezi poskytovatelem a jeho materiálním dodavatelem (příkladně pokud má poskytovatel vlastní datové centrum nebo má v rámci datacenter materiálního dodavatele zvolenu konkrétní zónu). V případě, že je daná služba materiálního dodavatele poskytovatele zapsána do katalogu na základě výjimky dle řádku 1.3 přílohy, služby poskytovatele musí být rovněž automaticky zapisované na základě výjimky dle řádku 1.3 přílohy.

Pokud chce poskytovatel namísto dokládání splnění požadavku standardním způsobem využít odkazu na podklady přiložené k žádosti jeho materiálního dodavatele, je třeba ve formuláři tuto skutečnost explicitně uvést včetně výčtu služeb, pro které splnění požadavku takto dokládá.

4.1.2 Řádek 1.5

Požadavek:

Zákaznická data jsou zpracovávána na území členských států Evropské unie a členských států Evropského sdružení volného obchodu. Aniž jsou dotčeny požadavky stanovené na řádku 1.3 přílohy č. 2 k této vyhlášce, v odůvodněných případech, po nezbytně nutnou dobu a v nezbytném rozsahu mohou být zákaznická data zpracovávána i na území jiných států, pokud poskytovatel popíše, jak budou zákaznická data chráněna před narušením bezpečnosti informací.

Podklad k doložení splnění požadavku:

1) *Poskytovatel uvede u služby cloud computingu,*

   a) *která zpracovává zákaznická data pouze na území členských států Evropské unie a členských států Evropského sdružení volného obchodu:*

      - *jasné označení takové služby cloud computingu a*
      - *deklaraci závazku zpracování zákaznických dat na území členských států Evropské unie a členských států Evropského sdružení volného obchodu,*

   b) *která zpracovává zákaznický obsah pouze na území členských států Evropské unie a členských států Evropského sdružení volného obchodu a která zpracovává nebo může zpracovávat zákaznická data bez zákaznického obsahu mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu:*

      - *jasné označení takové služby cloud computingu,*
      - *údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat bez zákaznického obsahu, a údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat bez zákaznického obsahu na příslušném předpokládaném území státu, a údaj o tom, zda jsou nebo nejsou zákaznická data bez zákaznického obsahu pseudonymizována v případě tohoto zpracování. U zákaznických dat bez zákaznického obsahu zpracovávaných mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu popis toho, jak budou chráněna ve smyslu kapitoly V. obecného nařízení o ochraně osobních údajů,*

   c) *která zpracovává nebo může zpracovávat zákaznická data mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu,*

      - *jasné označení takové služby cloud computingu,*
      - *údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat, a údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat na příslušném předpokládaném území státu a údaj o tom, zda jsou nebo nejsou zákaznická data pseudonymizována v případě tohoto zpracování. U zákaznických dat zpracovávaných mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu popis toho, jak budou chráněna alespoň ve smyslu kapitoly V. obecného nařízení o ochraně osobních údajů.*

2) *Má se za to, že předpokládanými územími států, na nichž dochází nebo může docházet ke zpracování zákaznických dat, nejsou:*

   - *území států, z nichž se mohou nepravidelně vzdáleně připojovat pracovníci technické podpory poskytovatele za účelem technické podpory služby cloud computingu, která se v čase mění a nemohou být specifikována předem;*

- *území států, do nichž poskytovatel může předávat zákaznická data za účelem poskytování volitelné doplňkové služby se zapojením třetích stran, která není sama o sobě službou cloud computingu, aktivované podle volby zákazníka, s tím, že poskytovatel jasně označí třetí stranu, jíž může předat zákaznická data, a je-li to možné, blíže specifikuje, jaká zákaznická data zpravidla předává a na jakou předpokládanou dobu zákaznická data předává.*

Schéma doložení splnění požadavku viz příloha č. 2

Komentář NÚKIB:

Požadavek tohoto řádku je podobný požadavku řádku 1.3, rozdílem je, že zde se hovoří o zpracování zákaznických dat v širším smyslu, nikoliv jen o jejich ukládání ve stavu neaktivních dat. Zpracování zákaznických dat v širším smyslu je možné i mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu bez nutnosti zapsání dané služby do katalogu na základě výjimky, jak je tomu v řádku 1.3, ovšem jen v odůvodněných případech a za předpokladu transparentnosti ze strany poskytovatele.

Podobně jako v požadavcích řádku 1.3 je třeba, aby poskytovatel rozřadil zapisované služby do kategorií, kdy je rozlišováno mezi nezpracováváním zákaznických dat mimo území Evropské unie a členských států Evropského sdružení volného obchodu [písm. a)], zpracováváním pouze zákaznických dat bez zákaznického obsahu mimo území Evropské unie a členských států Evropského sdružení volného obchodu [písm. b)] a zpracováváním jakýchkoliv zákaznických dat mimo území Evropské unie a členských států Evropského sdružení volného obchodu [písm. c)]. Na základě tohoto rozřazení je následně patrné, co je třeba pro každou z těchto služeb dokládat.

V případě zpracování zákaznických dat bez zákaznického obsahu a zákaznických dat mimo území států Evropské unie a Evropského hospodářského společenství je třeba popsat, případně odkázat na dokument, z nichž vyplývají tři základní okruhy informací ohledně zpracování zákaznických dat. Jsou jimi doba předpokládaná trvání, předpokládaný rozsah zpracování a předpokládaný účel zpracování. Tyto okruhy by měly být v žádosti jasně popsány, případně doplněny odkazy na relevantní dokumentaci, z níž tyto informace vyplývají.

Dále by v případě zpracování zákaznických dat bez zákaznického obsahu, popřípadě zákaznických dat obecně neměla chybět explicitně uvedená informace o tom, zda jsou nebo nejsou zpracovávaná data pseudonymizována.

4.1.3 Řádek 1.7

Požadavek:

Poskytovatel vyžaduje souhlas zákazníka pro případy zpracování zákaznických dat mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, který je vyjádřen v samostatném dokumentu, který obsahuje údaj o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat.

Poskytovatel informuje zákazníka o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat na příslušném předpokládaném území státu a o tom, zda jsou nebo nejsou zákaznická data pseudonymizována v případě tohoto zpracování.

Alternativně k vyžadování souhlasu a informování zákazníka poskytovatel v základním nastavení služby cloud computingu vyžaduje souhlas zákazníka pro případy zpracování zákaznických dat v každém jednotlivém případě zpracování zákaznických dat mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu.

Podklad k doložení splnění požadavku:

Dokument oddělený od podmínek poskytování služby či smlouvy, nebo odkaz na zřetelně uvedený text smluvní dokumentace, jimiž je vyžadován souhlas zákazníka pro případy zpracování zákaznických dat mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, které obsahují údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat,

nebo odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smluvní dokumentace nebo produktovou specifikaci, ze které bude patrné, že poskytovatel v základním nastavení služby vyžaduje souhlas zákazníka v každém jednotlivém případě zpracování zákaznických dat mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu.

Komentář NÚKIB:

Splnění tohoto požadavku je třeba dokládat pouze za situace, kdy poskytovatel zpracovává nebo může zpracovávat zákaznická data mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu dle požadavku řádku 1.5. Pokud poskytovatel takové zpracování zákaznických dat nepředpokládá, doložení souhlasu zákazníka s takovým zpracováním je matoucí. Je vhodné pouze ve formuláři nebo v samostatném dokumentu uvést, i za cenu opakování se vzhledem k požadavku řádku 1.5, že poskytovatel zpracování zákaznických dat mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu nepředpokládá, a tudíž je pro něj tento požadavek irelevantní.

4.2 Řádek - 2. Žádosti o zpřístupnění a předání dat

4.2.1 Řádek 2.5

Požadavek:

Poskytovatel jasně a srozumitelně uvádí jeho povinnosti vyplývající z právních předpisů států odlišných od členských států Evropské unie, v nichž poskytovatel předpokládá zpracování zákaznických dat dle řádků 1.1, 1.5 a 1.6 přílohy č. 2 k této vyhlášce týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů.

Podklad k doložení splnění požadavku:

Písemný popis povinností vyplývajících z právních předpisů států odlišných od členských států Evropské unie, v nichž poskytovatel předpokládá zpracování zákaznických dat dle řádků 1.1, 1.5 a 1.6 přílohy č. 2 k této vyhlášce týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů.

Písemný 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.

Komentář NÚKIB:

Zákazník by měl před využitím služeb cloud computingu vyhodnotit mj. i rizika spojená s využitím takových služeb, kdy podstatným rizikem je přístup cizích státních orgánů k datům vloženým do služby cloud computingu. Proto, aby měl zákazník pro své hodnocení maximum dostupných

informací o potenciálních právních závazcích a povinnostech poskytovatele cloud computingu, které se týkají zpřístupnění a předávání zákaznických dat a provozních údajů, je zaveden požadavek na poskytovatele cloud computingu tyto závazky a povinnosti jasně a srozumitelně popsat.

Z těchto důvodů uvádíme tyto minimální obsahové náležitosti, které při dokládání splnění požadavku Úřad požaduje:

1. Poskytovatel doloží právní posouzení jen u těch států, v nichž se nalézá datacentrum nebo jiná infrastruktura, ve které dochází ke zpracování zákaznických dat a specifických provozních údajů.
2. Poskytovatel doloží právní posouzení jen u států mimo EU a u těch států, u kterých Evropská komise nerozhodla o udělení tzv. adequacy decision podle článku 45 GDPR a které nejsou členskými zeměmi Evropského hospodářského prostoru. V případě, že se výjimka na základě tzv. adequacy decision aplikuje přímo na konkrétní společnost zajišťující infrastrukturu dle bodu 1., poskytovatel aplikaci této výjimky ve vztahu k dané společnosti vhodným způsobem doloží (například potvrzením o zápisu subjektu v Data Privacy Framework List v případě společnosti sídlící v USA, čestným prohlášením v případě kanadského subjektu podléhajícímu PIPEDA).
3. Poskytovatel doloží právní posouzení obsahující zejména informace o tom:
    a. 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,
    b. za jakých podmínek může tento orgán žádat o zpřístupnění a předání dat a na jak dlouho,
    c. na jaká data se daná povinnost vztahuje (provozní, zákaznická) a
    d. zda je možné žádost o zpřístupnění a předání dat přezkoumat nezávislým soudem.

4.3 Řádek - 4. Úrovně dostupnosti

Za podklad, kterým poskytovatel dokládá splnění požadavku tohoto řádku, je uznáván i podklad ve formě čestného prohlášení.

4.4 Řádek – 5. Připojení do výměnného uzlu internetu (IXP)

4.4.1 Řádek 5.1

Požadavek:

Poskytovatel má zajištěno připojení do výměnného uzlu internetu (IXP) v České republice.

Podklad k doložení splnění požadavku:

Výpis z veřejně dostupné databáze subjektů připojených do výměnného uzlu internetu, nebo platná smlouva s poskytovatelem služby výměnného uzlu internetu, nebo čestné prohlášení poskytovatele, že má zajištěno připojení do výměnného uzlu internetu (IXP) v České republice.

Komentář NÚKIB:

Poskytovatelé služeb SaaS, kteří sami nemají připojení do výměnného uzlu internetu v České republice, dokládají splnění požadavku tohoto řádku čestným prohlášením, že mají zajištěno připojení do výměnného uzlu internetu v České republice skrze své materiální dodavatele, a přikládají zachycení obrazovky některé z veřejně dostupných databází (příkladmo www.peeringdb.com nebo nix.cz) nebo dokument s obdobným obsahem, ze které plyne, že tento materiální dodavatel připojení do výměnného uzlu internetu v České republice zajištěno má. Poskytovatelé služeb IaaS a PaaS splnění požadavku dokládají zejména zachycením obrazovky některé z výše uvedených veřejně dostupných databází.

4.5 Řádek - 6. Zajištění poskytování služby cloud computingu

4.5.1 Řádek 6.4

Požadavek:

Poskytovatel zajišťuje, že primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, 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, nebo je přijato adekvátní bezpečnostní opatření, nebo se primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, nacházejí ve vzájemné vzdálenosti nejméně 50 km a u obou datových center je navržena a aplikována fyzická ochrana proti přírodním katastrofám, úmyslnému útoku nebo haváriím.

Podklad k doložení splnění požadavku:

Odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy nebo produktovou specifikaci nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo z auditní zprávy SOC 2® Type 2, s odkazem na tu část, ze které bude patrné zajištění alespoň jednoho záložního datového centra, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra,

a

pro doložení dostatečné vzdálenosti nebo přijetí adekvátního bezpečnostního opatření zpráva nebo jiný doklad o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka, které obsahuje náležitosti uvedené v příloze č. 5 k této vyhlášce,

nebo pro doložení vzájemné vzdálenosti nejméně 50 km a návrhu a aplikace fyzické ochrany proti přírodním katastrofám, úmyslnému útoku nebo haváriím odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávy SOC 2® Type 2, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ze kterých je služba cloud computingu poskytována a ze které bude patrné, že fyzická ochrana proti přírodním katastrofám, úmyslnému útoku nebo haváriím je navržena a aplikována.

Schéma doložení splnění požadavku viz příloha č. 3

Komentář NÚKIB:

Poskytovatel by při dokládání splnění požadavku neměl opomenout, že záložní datové centrum je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra. Rovněž dodávaná zpráva o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka musí obsahovat všechny náležitosti uvedené v příloze č. 5 vyhlášky.

4.6 Řádek - 7. Nakládání s daty

4.6.1 Řádek 7.2

Požadavek:

Poskytovatel chrání zákaznický obsah šifrováním při přenosu a v úložištích ve službě cloud computingu.

Podklad k doložení splnění požadavku:

Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrné, že poskytovatel chrání zákaznický obsah šifrováním při přenosu a v úložištích ve službě cloud computingu,

nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel chrání zákaznický obsah šifrováním při přenosu a v úložištích ve službě cloud computingu.

Komentář NÚKIB:

Poskytovatel musí prokázat, že zapisovaná služba *automaticky (by default)* zákaznický obsah šifrováním při přenosu a v úložištích ve službě cloud computingu. Nestačí tedy, že by poskytovatel pouze *umožňoval* ochranu dat šifrováním (viz kapitola 3.1.5)

Pokud by tedy poskytovatel doložil, že šifrování dat je podmíněno předchozí aktivací ze strany zákazníka, nebylo by možné tento požadavek považovat za splněný.

4.6.2 Řádek 7.3

Požadavek:

Poskytovatel umožňuje ochranu zákaznického obsahu šifrováním při přenosu a v úložištích ve službě cloud computingu pomocí některého z algoritmů uvedených v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost, které je zveřejněno na jeho internetových stránkách.[15]

Podklad k doložení splnění požadavku:

Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrný způsob šifrování při přenosu a v úložištích ve službě cloud computingu.

Komentář NÚKIB:

Požadavek lze považovat za splněný i v případě, pokud poskytovatel v dodaném dokumentu uvádí, že šifrování při přenosu a v úložištích ve službě cloud computingu provádí pomocí některého z algoritmů uvedených v aktuálním doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost.

Jestliže poskytovatel při dokládání splnění požadavku pro šifrování zákaznického obsahu při přenosu pouze uvede, že u zapisovaných služeb je používán protokol TLS v1.2, nelze bez dalšího považovat požadavek vyhlášky za splněný. Součástí TLS v1.2 jsou i algoritmy, které jsou zastaralé a které nejsou součástí doporučení NÚKIB. Je tedy nutné specifikovat, jaké šifrovací algoritmy má poskytovatel v rámci tohoto protokolu zvoleny.

4.6.3 Řádek 7.4

Požadavek:

Poskytovatel umožňuje zákazníkovi využití vlastního šifrovacího klíče (BYOK).

Podklad pro splnění tohoto požadavku:

Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrné, že poskytovatel umožňuje zákazníkovi využití vlastních šifrovacích klíčů, a to buď jejich vygenerováním v certifikovaném hardware security modulu (dále jen "HSM modulu") umístěném u poskytovatele pod vzdálenou správou zákazníka, nebo importem těchto klíčů z jiných prostředků pod správou zákazníka.

Komentář NÚKIB:

Poskytovatel může splnit uvedený požadavek tak, že součástí jeho služby bude možnost zákazníka vytvořit vlastní šifrovacího klíče pomocí HSM modulu, který je součástí služby poskytovatele. Není přitom podstatné, zda je tento HSM modul dodáván přímo poskytovatelem či jeho subdodavatelem. Druhou variantou splnění požadavku je, že poskytovatel umožní zákazníkovi import klíčů za použití prostředků pod správou zákazníka. Podstatou požadavku zůstává zajištění možnosti využití šifrovacích klíčů zákazníkem z prostoru pod správou zákazníka.

[15] Doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost je dostupné zde: https://nukib.gov.cz/cs/infoservis/aktuality/1984-nukib-pripravil-podpurne-materialy-pro-ochranu-pred-hrozbou-v-podobe-kvantovych-pocitacu/

4.6.4 Řádek 8.4

Požadavek:

Poskytovatel je držitelem platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), do jejíhož rozsahu certifikace náleží posuzovaná služba cloud computingu provozovaná v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017.

Podklad k doložení splnění požadavku:

Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu a provozovanou v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017,

nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven.

Komentář NÚKIB:

Verze ČSN "EN" ISO/IEC 27017 i přesto, že není uvedená ve vyhlášce v podkladě pro doložení, je uznatelným podkladem pro doložení splnění požadavku.

4.7 Řádek 9. Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty

4.7.1 Řádek 9.2

Požadavek:

Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí. Poskytovatel umožní zpřístupnění vzdáleně všech událostí tykajících se konkrétního zákazníka zákazníkovi. Nové události zpřístupní zákazníkovi bez zbytečného odkladu po vzniku události, nejpozději však do 24 hodin.

Podklad k doložení splnění požadavku:

Odkaz na konkrétní část podmínek poskytování služby cloud computingu, část návrhu smlouvy nebo jiný popis služby cloud computingu, ze kterých bude patrné, že poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí a umožní zpřístupnění vzdáleně všech událostí tykajících se konkrétního zákazníka zákazníkovi a nové události zpřístupní zákazníkovi bez zbytečného odkladu, nejpozději však do 24 hodin po vzniku události,

nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí, umožní zpřístupnění vzdáleně všech událostí tykajících se konkrétního zákazníka zákazníkovi a nové události zpřístupní zákazníkovi bez zbytečného odkladu po vzniku události, nejpozději však do 24 hodin.

Komentář NÚKIB:

Událostmi dle věty druhé požadavku řádku 9.2 přílohy č. 2 vyhlášky jsou míněny, s ohledem na systematiku ustanovení a odůvodnění vyhlášky, kybernetické bezpečnostní události.

Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[16].

Vytvořit v rámci vyhlášky konkrétní výčet událostí není možné, protože závisí na specificích zapisované služby. Obecně lze říci, že půjde o události ve vztahu k dané konkrétní službě a konkrétnímu tenantovi (například pokus o opakovanou neúspěšnou změnu hesla, pokus o připojení z neobvyklé lokality). Zároveň omezení na události konkrétního zákazníka míří na to, aby zákazníci nepožadovali více informací, než kolik se jich přímo týká. Z doložené dokumentace musí konkrétně vyplývat, jaké události mohou být zákazníkovi zpřístupněny. Zákazník má mít přístup se ke všem bezpečnostním událostem, které se jej týkají a mohou jej ovlivnit.

4.7.2 Řádek 9.3

Požadavek:

Poskytovatel informuje zákazníka v případě narušení bezpečnosti informací zákaznických dat a specifických provozních údajů bez zbytečného odkladu, ale nejpozději do 72 hodin od okamžiku, kdy se o narušení bezpečnosti zákaznických dat dozvěděl. Jakmile je řešení incidentu uzavřeno, informuje poskytovatel zákazníka o přijatých opatřeních.

Podklad k doložení splnění požadavku:

Odkaz na konkrétní část podmínek poskytování služby cloud computingu, část návrhu smlouvy nebo jiný popis služby cloud computingu, ze které bude patrné, že poskytovatel informuje zákazníka v případě narušení bezpečnosti informací zákaznických dat a specifických provozních údajů bez zbytečného odkladu, ale nejpozději do 72 hodin od okamžiku, kdy se o narušení bezpečnosti zákaznických dat dozvěděl.

Komentář NÚKIB:

Z dodaného podkladu rovněž musí vyplývat, že jakmile je řešení incidentu uzavřeno, informuje poskytovatel zákazníka o přijatých opatřeních.

4.8 Řádek 10. Testování služby cloud computingu

4.8.1 Řádek 10.1 Skeny zranitelnosti

Požadavek:

Poskytovatel provádí pravidelně skeny zranitelností. Služba cloud computingu zapisovaná do katalogu cloud computingu musí být zahrnuta do rozsahu skenu zranitelností.

Podklad k doložení splnění požadavku:

Tři záznamy o provedení skenů zranitelností provedených maximálně 3 měsíce před podáním žádosti o zápis služby cloud computingu do katalogu cloud computingu,

[16] § 7 odst. 1 ZKB

nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávu SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že skeny zranitelností jsou prováděny pravidelně v takovém intervalu, ze kterého bude vyplývat, že byly provedeny alespoň 3 skeny zranitelností maximálně 3 měsíce před podáním žádosti o zápis služby cloud computingu do katalogu cloud computingu.

Komentář NÚKIB:

Z pohledu Národního úřadu pro kybernetickou a informační bezpečnost je klíčové, zda poskytovatel cloud computingu pravidelně testuje zranitelnosti nabízeného cloud computingu.

Vyžadujeme dokládat splnění požadavku i pro služby, které nemají vnější rozhraní, pokud poskytovatel neprokáže, že vzhledem k vlastnostem zapisované služby není sken zranitelnosti aplikovatelný nebo že jeho provedení není pro vlastnosti zapisované služby nutný.

Jako podklad k prokázání splnění požadavku uznáváme i jiné dokumenty, které spolehlivě prokazují, že poskytovatel pravidelně skeny zranitelnosti pro zapisované služby provádí. Jako příklad lze uvést auditní zprávy FedRamp nebo auditní zpráva SOC 2 Type 2®.

Některé záznamy o provedení skenování zranitelností mohou obsahovat pouze IP adresy bez bližšího určení názvů služeb, na které se skenování zaměřilo. V takovém případě je nutné, aby poskytovatel k doloženým skenům zranitelností přiložil alespoň čestné prohlášení, kde poskytovatel detailně popíše, ke kterým konkrétním IP adresám se zapisované služby, podléhající skenům zranitelnosti, vztahují.

V případě, že dodané dokumenty obsahují citlivé informace, lze takové informace ve zprávě neuvést/zakrýt (začernit). I v tomto případě musí být nicméně patrné, že skeny zranitelnosti byly provedeny.

4.9 Řádek 10.2 a 10.3 Penetrační testování

Požadavek:

Poskytovatel zajišťuje provádění penetračních testů subjektem, který je nezávislý na poskytovateli. Služba cloud computingu zapisovaná do katalogu cloud computingu musí být zahrnuta do rozsahu penetračního testu.

Podklad k doložení splnění požadavku řádku 10.2:

Zpráva z provedení penetračního testu provedeného podle standardu NIST 800-115 nebo v souladu s metodikou OSSTMM. Penetrační test provede subjekt, který je nezávislý na poskytovateli. Zpráva z provedení penetračního testu nesmí být starší než 24 měsíců před podáním žádosti o zápis služby cloud computingu do katalogu cloud computingu.

Podklad k doložení splnění požadavku řádku 10.3:

Zpráva z provedení penetračního testu, při kterém budou ověřena rizika alespoň podle standardu OWASP Top 10 Web Application Security Risks. Penetrační test provede subjekt, který je nezávislý na poskytovateli. Zpráva z provedení penetračního testu nesmí být starší než 24 měsíců před podáním žádosti o zápis služby cloud computingu do katalogu cloud computingu.

Komentář NÚKIB:

Jedním z požadavků stanovených na řádcích 10.2 a 10.3 přílohy č. 2 vyhlášky pro vysokou a kritickou bezpečnostní úroveň je i provádění penetračních testů na poskytovateli nezávislým subjektem, které mají prověřit zabezpečení poskytované služby cloud computingu. Cílem tohoto požadavku je zajistit, že poskytovatel bude pravidelně ověřovat podle uznávaných standardů, že nabízená služba cloud computingu nemá bezpečnostní nedostatky, které by znamenaly případné bezpečnostní riziko pro orgány veřejné správy.

Splnění tohoto požadavku má poskytovatel služby cloud computingu doložit zprávou z provedení penetračního testu. Není však nezbytné poskytovat konkrétní nálezy ve zprávě z provedení penetračního testu a odhalovat případné zranitelnosti. Není ani záměrem poskytovatele služby cloud computingu jakkoliv trestat, pokud byly zranitelnosti v rámci penetračního testování odhaleny a ve zprávě identifikovány. Klíčové je, že poskytovatel bezpečnost svých služeb pravidelně ověřuje a zjištěné chyby v zabezpečení je schopen reflektovat.

Ze samotného znění požadavku uvedeného na řádcích 10.2 a 10.3 přílohy č. 2 vyhlášky a způsobu doložení jeho splnění vyplývá, že je třeba, aby předkládaná zpráva z penetračního testu splňovala následující požadavky:

- **NEZÁVISLOST** – Zpráva byla vyhotovena třetím subjektem, který je nezávislý na poskytovateli.
- **DATUM** – Stáří zprávy z penetračním testu je maximálně 24 měsíců k datu podání žádosti o zápis do katalogu.
- **OBSAH** – Z obsahu zprávy z penetračního testu je patrné, že penetrační test proběhl v souladu s předepsanou metodikou OSSTMM nebo standardy NIST 800-115, OWASP Top 10 a tudíž:
    - zpráva obsahuje jednotlivé oblasti testování stanovené v metodice/standardech a ve zprávě je uveden explicitní odkaz na metodiku/standardy, podle kterých byl penetrační test proveden nebo
    - je provedení dle dané metodiky/standardu deklarováno alespoň v doložených dokumentech (např. čestné prohlášení subjektu provádějícího penetrační test).
- **ROZSAH** – Zpráva z penetračního testu zahrnuje výčet služeb cloud computingu, které byly:
    - zahrnuty do rozsahu penetračního testu nebo
    - zahrnuje takový popis rozsahu penetračního testu, ze kterého bude jednoznačně patrné, že služba cloud computingu, kterou poskytovatel žádá zapsat do katalogu cloud computingu, náleží do daného rozsahu penetračního testu cloud computingu nebo
    - poskytovatel služby cloud computingu připojuje čestné prohlášení s výčtem služeb, které byly v rozsahu daného penetračního testu.

V případě, že zpráva z penetračního testu neobsahuje konkrétní výčet testovaných služeb, pak je nezbytné doložit alespoň formou čestného prohlášení, jaké služby byly do rozsahu penetračního testu zahrnuty. Pokud tedy není prokázáno, zda nabízená služba byla v rozsahu

penetračního testu dle specifikovaných kritérií, pak nejsou splněny podmínky vyhlášky, a tedy nelze takovou službu do katalogu zapsat.

V případě, že z doložené zprávy o provedení penetračního testu vyplývá, že penetrační test byl proveden podle jiné metodiky/standardu, než požaduje vyhláška, pak musí poskytovatel doložit, že tato jiná metodika/standard je v souladu s vyhláškou vyžadovanou metodikou/standardem. Poskytovatel může tuto skutečnost prokázat čestným prohlášením subjektu provádějícího penetrační test nebo doložením této jiné metodiky/standardu, ze které bude patrné, že aplikuje vyhláškou požadovanou metodiku/standard. Upozorňujeme nicméně na to, že z čestného prohlášení musí jednoznačně vyplývat, že se vztahuje na poskytovatelem doloženou zprávu z provedení penetračního testu.

Doložení splnění požadavku je možné provést i skrze souhrnnou zprávu o provedení penetračního testování. Takový dokument musí nadále splňovat požadavky popsané v předchozích odstavcích.

V případě, že dodané dokumenty obsahují citlivé informace, lze takové informace ve zprávě neuvést/zakrýt (začernit). I v tomto případě musí být nicméně patrné, že penetrační testování bylo provedeno.

5 Seznam příloh

1. schéma-řádek13.pdf
2. schéma-řádek15.pdf
3. schéma-řádek64.pdf

6 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP: RED**	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová **TLP: AMBER**	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta.
Oranžová **TLP: AMBER+STRICT**	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
Zelená **TLP: GREEN**	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP: CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
29. února 2024	1.0	OREG – ORDIT	Vytvoření dokumentu
27. března 2024	1.1	OREG - ORDIT	Doplnění definic k pojmům a oprava překlepů