190

VYHLÁŠKA

ze dne 7. června 2023

o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Úřad“) stanoví podle § 28 odst. 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 205/2017 Sb., (dále jen „zákon“):

§ 1

Předmět úpravy

Tato vyhláška stanoví obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu podle § 6 písm. e) zákona, jejichž cílem je zajištění bezpečnosti informací při využívání služeb cloud computingu orgány veřejné moci.

§ 2

Základní pojmy

Pro účely této vyhlášky se rozumí

a) uživatelem služby cloud computingu (dále jen „uživatel“) ten, kdo služby cloud computingu prostřednictvím nebo jménem orgánu veřejné moci využívá,

b) zákaznickými daty všechna data, která jsou uživatelem nebo administrátorem[1]) na straně orgánu veřejné moci vložena do služby cloud computingu nebo jsou výsledkem využití služby cloud computingu uživatelem v průběhu využívání služby cloud computingu,

c) zákaznickým obsahem 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,

d) specifickými provozními údaji takové provozní údaje, které obsahují informace o identifikovaném nebo identifikovatelném uživateli nebo administrátorovi[1]) na straně orgánu veřejné moci,

e) zpracováním jakákoliv operace nebo soubor operací se zákaznickými daty nebo provozními údaji v elektronické podobě, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení,

f) subdodavatelem dodavatel poskytovatele s vlivem na bezpečnost informací služby cloud computingu,

g) technickým aktivem takové technické vybavení, komunikační prostředky a programové vybavení služby cloud computingu a objekty, které jsou využívány k poskytování služby cloud computingu a jejichž selhání může mít dopad na službu cloud computingu.

§ 3

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

(1) Bezpečnostní pravidla stanovují minimální požadavky pro využívání služby cloud computingu orgánem veřejné moci v příslušné bezpečnostní úrovni[2]) cloud computingu.

---

[1]) § 2 písm. a) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.

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

(2) Bezpečnostní pravidla pro orgány veřejné moci jsou stanovena v příloze k této vyhlášce.

§ 4

Přechodná ustanovení

Orgán veřejné moci, který využívá službu cloud computingu na základě smlouvy s poskytovatelem uzavřené přede dnem nabytí účinnosti této vyhlášky nebo smlouvy, která byla uzavřena na základě smlouvy uzavřené přede dnem nabytí účinnosti této vyhlášky, zajistí dodržování bezpečnostních pravidel pro poskytování služby cloud computingu stanovených touto vyhláškou od 1. ledna 2024.

§ 5

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. července 2023.

Ředitel:

Ing. **Kintr** v. r.

Řádek	Bezpečnostní pravidlo	Bezpečnostní úroveň
1. Obecné podmínky pro službu cloud computingu		
1.1	**Informace o poloze zpracování zákaznických dat** Orgán veřejné moci má k dispozici dostatek jasných a srozumitelných informací o provozu služby cloud computingu, poloze zpracování zákaznických dat a rizicích souvisejících se zpracováním zákaznických dat v dané poloze pro vyhodnocení rizik pro bezpečnost informací.	nízká střední vysoká kritická
1.2	**Posouzení rizika předání nebo zpřístupnění dat cizozemským orgánům** Orgán veřejné moci vyhodnocuje rizika pro bezpečnost informací vyplývající z polohy zpracování zákaznických dat a specifických provozních údajů, zejména z možných žádostí cizozemských orgánů o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, a s tím souvisejícím předáním, nebo zpřístupněním zákaznických dat nebo specifických provozních údajů (ustanovení Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) týkající se předávání osobních údajů do třetích zemí tímto nejsou dotčena). Orgán veřejné moci může využívat službu cloud computingu, u které vyhodnotil rizika pro bezpečnost informací jako přijatelná. Vyhodnocení rizik orgán veřejné moci písemně zaznamenává.	nízká střední vysoká kritická
1.3	**Trvalé uložení dat na území členských států Evropské unie a členských států Evropského sdružení volného obchodu** Zákaznická data ve stavu neaktivních dat jsou ukládána nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu (dále jen „EU/ESVO“). 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.	vysoká kritická
1.4	**Trvalé uložení specifických provozních údajů na území EU/ESVO** Specifické provozní údaje jsou ukládány nepřetržitě a výlučně na území členských států EU/ESVO. V případě, že služba cloud computingu daný požadavek nesplňuje, poskytovatel takovou službu jasně označuje a uvádí, zda taková služba cloud computingu ukládá specifické provozní údaje ve stavu neaktivních dat v pseudonymizované podobě nebo nepseudonymizované podobě. Poskytovatel uvádí místo uložení specifických provozních údajů ve stavu neaktivních dat.	vysoká kritická
1.5	**Omezení zpracování dat mimo území členských států EU/ESVO** Zákaznická data jsou zpracovávána pouze na území členských států EU/ESVO. Aniž jsou dotčeny požadavky stanovené pravidlem upraveným na řádku 1.3 této přílohy, v odůvodněných případech, po nezbytně nutnou dobu a v nezbytném rozsahu mohou být	vysoká kritická

	zákaznická data zpracovávána i na území jiných států, pokud v popisu služby cloud computingu bude popsán způsob ochrany zákaznických dat před narušením bezpečnosti informací.	
1.6	**Omezení zpracování specifických provozních údajů mimo území členských států EU/ESVO** Specifické provozní údaje jsou zpracovávány na území členských států EU/ESVO. Aniž jsou dotčeny požadavky stanovené pravidlem upraveným na řádku 1.4 této přílohy, v odůvodněných případech, po nezbytně nutnou dobu a v nezbytném rozsahu mohou být specifické provozní údaje zpracovávány i na území jiných států, pokud v popisu služby cloud computingu bude popsán způsob ochrany specifických provozních údajů před narušením bezpečnosti informací.	vysoká kritická
1.7	**Omezení zpracování dat mimo území České republiky** Zákaznická data a specifické provozní údaje jsou zpracovávány na území České republiky. Mimo území České republiky mohou být zákaznická data a specifické provozní údaje zpracovávány pouze s výslovným písemným souhlasem orgánu veřejné moci.	kritická
1.8	**Smluvní ujednání o dostupnosti během běžného provozu** Smlouva o poskytování služby cloud computingu jasně a srozumitelně vymezuje rozsah dostupnosti služby cloud computingu, včetně právních následků porušení sjednaného rozsahu dostupnosti služby cloud computingu.	nízká střední vysoká kritická
1.9	**Soulad s certifikací systému řízení bezpečnosti** Služba cloud computingu je provozována v rozsahu systému řízení bezpečnosti informací, který je v souladu s požadavky vyhlášky o kybernetické bezpečnosti[3)] nebo s požadavky ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001.	nízká
1.10	**Certifikace systému řízení bezpečnosti informací** Služba cloud computingu je provozována v rozsahu systému řízení bezpečnosti informací, který byl certifikován podle ČSN EN ISO/IEC 27001, EN ISO/IEC 27001, nebo ISO/IEC 27001 certifikačním orgánem, který byl akreditován pro ověřování shody s normami ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 některým z členů Mezinárodního akreditačního fóra (IAF).	střední vysoká kritická
1.11	**Certifikace služby cloud computingu podle ISO/IEC 27017** Služba cloud computingu je provozovaná v souladu s normou ČSN ISO/IEC 27017 nebo ISO/IEC 27017, o čemž vystavil certifikát certifikační orgán, který byl akreditován pro ověřování shody s normami ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 některým z členů Mezinárodního akreditačního fóra (IAF). V případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě poskytovanou službu cloud computingu, poskytovaná služba cloud computingu musí spadat do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven.	střední vysoká kritická

[3)] Vyhláška č. 82/2018 Sb.

1.12	**Certifikace služby cloud computingu podle ISO/IEC 27018** Služba cloud computingu je provozována v souladu s normou ČSN EN ISO/IEC 27018 nebo ISO/IEC 27018, o čemž vystavil certifikát certifikační orgán, který byl akreditován pro ověřování shody s normami ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 některým z členů Mezinárodního akreditačního fóra (IAF). V případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě poskytovanou službu cloud computingu, poskytovaná služba cloud computingu musí spadat do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven.	vysoká kritická
1.13	**Prohlášení o aplikovatelnosti** Orgán veřejné moci má vzdálený přístup k prohlášením o aplikovatelnosti, vydaným v souvislosti s certifikacemi podle ČSN ISO/IEC 27001 nebo ISO/IEC 27001, ČSN ISO/IEC 27017 nebo ISO/IEC 27017 a ČSN EN ISO/IEC 27018 nebo ISO/IEC 27018 podle pravidel upravených na řádcích 1.10 až 1.12 přílohy vyhlášky.	vysoká kritická
1.14	**Právo odstoupit od smlouvy** Orgán veřejné moci má právo bez sankcí odstoupit od smlouvy s poskytovatelem v případě, že dojde k podstatnému zvýšení rizika z hlediska bezpečnosti informací u poskytovatele: a) změnou skutečného majitele poskytovatele podle zákona o evidenci skutečných majitelů[4]; za změnu skutečného majitele se pro účely tohoto pravidla nepovažuje změna osoby ve vrcholovém vedení poskytovatele, b) změnou sídla poskytovatele do jiné země mimo území EU/EHP, c) vydáním opatření Úřadem podle zákona ve vztahu k poskytovateli nebo subdodavateli poskytovatele nebo dané služby cloud computingu, d) výmazem poskytovatele cloud computingu z katalogu cloud computingu z důvodu neplnění požadavků na poskytovatele cloud computingu podle zákona č. 365/2000 Sb.[5], e) změnou subdodavatele poskytovatele bez souhlasu orgánu veřejné moci, f) změnou kontroly nad zásadními podpůrnými aktivy[6] využívanými poskytovatelem k poskytování služby cloud computingu, g) hrubým porušením smluvních podmínek ze strany poskytovatele a h) významnou změnou[7] v poskytování služby cloud computingu.	vysoká kritická

[4] Zákon č. 37/2021 Sb., o evidenci skutečných majitelů, ve znění pozdějších předpisů.
[5] § 6m ve spojení s § 6s odst. 1 zákona č. 365/2000 Sb.
[6] § 2 písm. f) vyhlášky č. 82/2018 Sb.
[7] § 2 písm. o) vyhlášky č. 82/2018 Sb.

2. Organizace bezpečnosti informací		
2.1	**Systém řízení bezpečnosti informací** Poskytovatel má zaveden systém řízení bezpečnosti informací[8]. Rozsah systému řízení bezpečnosti informací zahrnuje organizační jednotky poskytovatele, lokality a procesy využívané k poskytování služby cloud computingu. Poskytovatel dokumentuje zavedená opatření pro nastavení, implementaci, údržbu a neustálé zlepšování systému řízení bezpečnosti informací. Dokumentace obsahuje rozsah systému řízení bezpečnosti informací a prohlášení o aplikovatelnosti[9], ve kterém je uvedeno, jaká bezpečnostní opatření byla vybrána pro potlačení rizik, a výsledky posledního auditu systému řízení bezpečnosti informací poskytovatele.	nízká střední vysoká kritická
2.2	**Politika bezpečnosti informací** Služba cloud computingu se řídí politikou bezpečnosti informací sdílenou a sdělovanou všem zaměstnancům, externím pracovníkům a subdodavatelům poskytovatele, dokumentovanou, verzovanou, kontrolovanou a schválenou vrcholovým vedením poskytovatele. Politika bezpečnosti informací popisuje význam bezpečnosti informací, bezpečnostní cíle, úroveň zabezpečení služby cloud computingu, nejvýznamnější aspekty bezpečnostní strategie k dosažení stanovených cílů a organizační strukturu poskytovatele služby cloud computingu v rozsahu systému řízení bezpečnosti informací.	nízká střední vysoká kritická
2.3	**Bezpečnostní opatření** Na základě politiky bezpečnosti informací podle pravidla upraveného na řádku 2.2 této přílohy jsou zavedena přiměřená bezpečnostní opatření.	nízká střední vysoká kritická
3. Politiky		
3.1	**Politika bezpečnosti informací** Politika bezpečnosti informací, kterou se řídí poskytování služby cloud computingu, je v souladu s požadavky orgánu veřejné moci na bezpečnost informací.	nízká střední vysoká kritická

[8] § 3 vyhlášky č. 82/2018 Sb.
[9] § 5 odst. 1 písm. f) vyhlášky č. 82/2018 Sb.

4. Fyzická bezpečnost		
4.1	**Fyzická bezpečnost budov a prostor** V datových centrech, ve kterých dochází k poskytování služby cloud computingu je navržena a aplikována fyzická ochrana proti přírodním katastrofám, úmyslnému útoku nebo haváriím.	nízká střední vysoká kritická
4.2	**Modely redundance** Služba cloud computingu je poskytována alespoň ze dvou datových center, která jsou od sebe oddělena dostatečnou vzdáleností k zajištění vzájemné provozní zastupitelnosti a odolnosti v poskytování služby cloud computingu.	nízká střední vysoká kritická
4.3	**Vzdálenost datových center od zdrojů rizik** Primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby cloud computingu 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 cloud computingu poskytované z primárního datového centra, nacházejí ve vzájemné vzdálenosti nejméně 50 km.	vysoká kritická
4.4	**Opatření k detekci a zabránění neoprávněného přístupu** U budov a prostor vztahujících se k poskytování služby cloud computingu, včetně vstupu to těchto budov a prostor, jsou prokazatelně zavedena bezpečnostní opatření vhodná k včasné detekci a zabránění neoprávněnému či neautorizovanému přístupu k technickým aktivům, nebo k zákaznickým datům a provozním údajům, nebo poškození a neoprávněným zásahům do technických aktiv, zákaznických dat nebo provozních údajů.	střední vysoká kritická
5. Zajištění provozu služby cloud computingu		
5.1	**Bezpečné nakládání se zákaznickým obsahem** Zákaznický obsah je zpracováván pouze způsobem sjednaným ve smlouvě o poskytování služby cloud computingu.	nízká střední vysoká kritická
5.2	**Hodnocení informací o zranitelnostech a hrozbách** Orgán veřejné moci vyhodnocuje informace a podklady týkající se zranitelností a hrozeb využívané služby cloud computingu a přijímá odpovídající opatření.	vysoká kritická

5.3	**Rozdělení prostředí v cloudu** Zákaznická data jsou bezpečně a striktně oddělována od jiných dat, která jsou uložená a zpracovávaná na sdílených virtuálních a fyzických zdrojích využívaných k poskytování služby cloud computingu tak, aby byla zajištěna důvěrnost a integrita zákaznických dat.	střední vysoká kritická
5.4	**Přenos a zálohování dat** Zákaznická data a data nezbytná pro poskytování služby cloud computingu jsou zálohována do lokality v dostatečné vzdálenosti. Při přenosu do této lokality i při uložení v této lokalitě jsou zákaznická data a data nezbytná pro poskytování služby cloud computingu šifrována v souladu s uznávanými nejmodernějšími požadavky v oblasti kryptografických prostředků nebo alespoň v souladu s doporučením Úřadu v oblasti kryptografických prostředků zveřejněným na internetových stránkách Úřadu.	vysoká kritická
5.5	**Shromažďování provozních údajů a jejich náležitosti** Provozní údaje se vztahem ke službě cloud computingu se shromažďují zejména o událostech: a) přihlašování a odhlašování u všech účtů, a to včetně neúspěšných pokusů, b) činnosti provedené administrátory[1)] na straně poskytovatele zejména pokud zaměstnanci nebo externí pracovníci poskytovatele čtou nebo zapisují nešifrovaná zákaznická data nebo specifické provozní údaje zpracovávané ve službě cloud computingu nebo k nim přistupují bez předchozího souhlasu orgánu veřejné moci, c) úspěšné i neúspěšné manipulace s účty, oprávněními a přístupovými právy, d) neprovedení činností v důsledku nedostatku přístupových práv a oprávnění, e) činnosti uživatelů a administrátorů[1)] na straně orgánu veřejné moci, které mohou mít vliv na bezpečnost informací ve službě cloud computingu, f) zahájení a ukončení činností technických aktiv, g) kritická i chybová hlášení technických aktiv a h) pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí. Provozní údaje zaznamenané podle tohoto pravidla obsahují zejména: a) datum a čas, včetně specifikace časového pásma, b) typ činnosti, c) identifikaci technického aktiva, které činnost zaznamenalo, d) jednoznačnou identifikaci účtu, pod kterým byla činnost provedena, e) jednoznačnou síťovou identifikaci zařízení původce a f) úspěšnost nebo neúspěšnost činnosti.	střední vysoká kritická
5.6	**Monitorování a zaznamenávání událostí** Služba cloud computingu zahrnuje nástroj pro monitorování a zaznamenávání událostí. Orgán veřejné moci má přístup k informacím o stavu zabezpečení, zejména k informacím vyplývajícím z provozních údajů shromážděných podle pravidla upraveného na řádku 5.5 této přílohy.	střední vysoká kritická

5.7	**Doba uchování provozních údajů** Provozní údaje shromážděné podle pravidla upraveného na řádku 5.5 této přílohy jsou uchovány po dobu alespoň 12 měsíců od jejich vytvoření.	vysoká
5.8	**Doba uchování provozních údajů** Provozní údaje shromážděné podle pravidla upraveného na řádku 5.5 této přílohy jsou uchovány po dobu alespoň 18 měsíců od jejich vytvoření.	kritická
5.9	**Ukládání provozních údajů** Vygenerované provozní údaje jsou uchovávány ve vhodné, neměnné a sdružené formě bez ohledu na jejich zdroj tak, aby bylo možné centrální autorizované vyhodnocení dat. Mezi technickým aktivem shromažďujícím provozní údaje podle pravidla upraveného na řádku 5.5 této přílohy a technickým aktivem, na němž jsou provozní údaje vytvářeny, je prováděno ověřování identity. Přenos mezi technickým aktivem shromažďujícím provozní údaje podle pravidla upraveného na řádku 5.5 této přílohy a technickými aktivy, na nichž jsou provozní údaje vytvářeny, probíhá zabezpečeným aktuálně odolným šifrováním nebo po sítích pod kontrolou poskytovatele.	střední vysoká kritická
5.10	**Poskytnutí provozních údajů orgánu veřejné moci** Orgán veřejné moci má na žádost k dispozici provozní údaje o činnostech uživatelů, ve vhodné formě a v přiměřeném čase tak, aby mohl provést analýzu jakéhokoliv kybernetického bezpečnostního incidentu, který se ho týká.	střední vysoká kritická
6. Správa identit a řízení přístupu		
6.1	**Vícefaktorová autentizace pro přístup** Přístup orgánu veřejné moci do správy služby cloud computingu je zabezpečen vícefaktorovou autentizací.	střední vysoká kritická
6.2	**Řízení přístupu orgánu veřejné moci** Orgán veřejné moci řídí přístupy uživatelů a administrátorů[1)] na straně orgánu veřejné moci do služby cloud computingu, zejména: a) přiřazuje jedinečná uživatelská jména, b) uděluje a upravuje uživatelské účty a účty administrátorů[1)] na straně orgánu veřejné moci a přístupová oprávnění na základě principu nejnižšího oprávnění (least-privilege principle) a principu nutnosti vědět (need-to-know principle), c) pravidelně alespoň jednou ročně kontroluje přidělené uživatelské účty a účty administrátorů[1)] na straně orgánu veřejné moci a přístupová oprávnění, d) blokuje a odebírá přístupové účty v případě nečinnosti a e) odebírá nebo mění přístupová oprávnění při ukončení nebo změně smluvního vztahu.	nízká střední vysoká kritická

6.3	**Řízení přístupu poskytovatele** Poskytovatel v rámci své organizace řídí přístupy k informačnímu systému využívanému k poskytování služby cloud computingu orgánu veřejné moci.	nízká střední vysoká kritická
6.4	**Dohody o mlčenlivosti a důvěrnosti** Dohody o mlčenlivosti a důvěrnosti mezi poskytovatelem a jeho zaměstnanci, externími pracovníky a subdodavateli jsou uzavřeny předtím, než je zaměstnancům, externím pracovníkům a subdodavatelům udělen přístup k zákaznickým datům a specifickým provozním údajům.	nízká střední vysoká kritická
6.5	**Přístupová práva administrátorů[1)] na straně poskytovatele** Přístupová práva jsou přidělována konkrétním administrátorům[1)] na straně poskytovatele podle principu nutnosti vědět (need-to-know principle) a časově omezena na základě hodnocení rizik poskytovatele.	nízká střední vysoká kritická
6.6	**Souhlas pro přístup k zákaznickým datům nebo specifickým provozním údajům** Přístup zaměstnanců nebo externích pracovníků poskytovatele k zákaznickým datům nebo specifickým provozním údajům, které nejsou šifrovány nebo byly dešifrovány, je možný pouze po předchozím souhlasu orgánu veřejné moci. Pro potřeby udělení tohoto souhlasu je orgán veřejné moci informován o důvodu, době trvání, času, typu a rozsahu přístupu tak, aby byl schopen vyhodnotit rizika spojená s tímto přístupem.	kritická
7. Správa klíčů a šifrování		
7.1	**Šifrování zákaznického obsahu při přenosu** Poskytovatel má zavedené procesy a technická opatření s aktuálně odolným šifrováním a ověřením identity pro zabezpečení přenosu zákaznického obsahu po sítích mimo kontrolu poskytovatele.	nízká střední vysoká kritická
7.2	**Šifrování zákaznického obsahu při uchovávání** Poskytovatel má zavedené procesy a technická opatření pro aktuálně odolné šifrování zákaznického obsahu během uchovávání.	nízká střední vysoká kritická

7.3	**Úroveň šifrování zákaznického obsahu** Zákaznický obsah je při přenosu a v úložištích ve službě cloud computingu šifrován v souladu s uznávanými nejmodernějšími požadavky v oblasti kryptografických prostředků nebo alespoň pomocí některého z algoritmů uvedeného v doporučení Úřadu v oblasti kryptografických prostředků zveřejněném na internetových stránkách Úřadu.	vysoká kritická
8. Zabezpečení komunikace		
8.1	**Technické prostředky** Orgán veřejné moci využívá nástroje nebo služby pro zvýšení odolnosti vůči útokům typu odepření služby (DoS/DDoS).	vysoká kritická
8.2	**Ochrana datových přenosů do služby cloud computingu** Zákaznická data přenášená do služby cloud computingu jsou chráněna proti neoprávněnému zásahu, kopírování, úpravě, přesměrování nebo vymazání v souladu s požadavky orgánu veřejné moci na zajištění bezpečnosti informací.	nízká střední vysoká kritická
8.3	**Ochrana datových přenosů ze služby cloud computingu** Zákaznická data přenášená ze služby cloud computingu jsou chráněna proti neoprávněnému zásahu, kopírování, úpravě, přesměrování nebo vymazání v souladu se zavedenou politikou bezpečnosti informací poskytovatele.	nízká střední vysoká kritická
8.4	**Připojení do výměnného uzlu internetu** Poskytovatel má zajištěno připojení do výměnného uzlu internetu (IXP) v České republice.	vysoká kritická
9. Přenositelnost, propojení a exit strategie		
9.1	**Zajištění kontinuity informačního systému orgánu veřejné moci** Orgán veřejné moci má při ukončení využívání služby zákaznická data a provozní údaje ve formátu a rozsahu nezbytném pro zajištění kontinuity informačního sytému, pro jehož provoz službu cloud computingu využíval. V případě, že pro zajištění kontinuity informačního systému je nezbytné vydání dat poskytovatelem služby, formát a rozsah zákaznických dat a provozních údajů je předem sjednán.	nízká střední vysoká kritická
9.2	**Plán pro ukončení využívání služby cloud computingu** Orgán veřejné moci vytvoří plán pro ukončení využívání služby cloud computingu (dále jen „exit strategie“), který zahrnuje zejména: a) cíle, kterých má exit strategie dosáhnout,	nízká střední vysoká

	b) definici kritérií pro spuštění exit strategie, c) definici situací pro spuštění exit strategie, například: 1. insolvence, rozpad nebo ukončení činnosti poskytovatele, 2. výmaz poskytovatele nebo výmaz poskytované služby cloud computingu z katalogu cloud computingu, 3. nesoulad smlouvy s právními či regulatorními požadavky, 4. uplynutí doby, na kterou byla smlouva uzavřena, 5. hrubé porušení smluvních podmínek o úrovni služby cloud computingu ze strany poskytovatele, 6. neshoda s poskytovatelem při jednáních o změně smlouvy, 7. významná změna[7)] kontroly nad poskytovatelem, 8. významná změna[7)] kontroly nad technickými aktivy využívanými poskytovatelem k poskytování služby cloud computingu, 9. významná změna[7)] u subdodavatelů, 10. jiná významná změna[7)] na straně poskytovatele relevantní pro poskytování služby cloud computingu, 11. podstatná nemožnost orgánu veřejné moci využívat službu cloud computingu, d) definici možných variant řešení migrace, e) analýzu dopadů zaměřenou na náklady a lidské zdroje nutné k úspěšnému provedení exit strategie, f) rozdělení rolí a zodpovědností v průběhu exit strategie a transferu systémů k jiným poskytovatelům, g) určení dat nutných pro úspěšné zvládnutí exit strategie včetně určení formátu těchto dat, h) definici opatření k zajištění součinnosti poskytovatele při předání dat, i) určení doby pro provedení exit strategie, j) definici parametrů úspěchu při provádění exit strategie a k) opatření pro zajištění úspěšného provedení exit strategie.	kritická
9.3	**Zajištění požadavků na exit strategii** Smlouva o poskytování služby cloud computingu zohledňuje požadavky orgánu veřejné moci na exit strategii podle pravidla upraveného na řádku 9.2 této přílohy.	nízká střední vysoká kritická
9.4	**Dokumentace bezpečnosti vstupů a výstupů** Služba cloud computingu je přístupná pro jiné služby cloud computingu nebo IT systémy orgánu veřejné moci skrze zdokumentované rozhraní příchozích a odchozích zákaznických dat tak, aby z nich orgán veřejné moci mohl v případě potřeby získat zákaznická data, a to pokud se jedná o služby cloud computingu, které zákaznická data ukládají ve stavu neaktivních dat. Poskytovatel na vyžádání orgánu veřejné moci zpřístupní příslušnou dokumentaci.	střední vysoká kritická
9.5	**Smluvní podmínky o poskytování zákaznických dat** Smlouva o poskytování služby cloud computingu ve vztahu k jejímu ukončení upravuje zejména: a) typ, rozsah, strukturu a formát dat, které poskytovatel předá orgánu veřejné moci; nedohodne-li se orgán veřejné moci s poskytovatelem jinak, zajistí orgán veřejné moci, že zákaznická data budou poskytovatelem předána ve strukturovaném, běžně používaném, strojově čitelném a interoperabilním formátu,	nízká střední vysoká kritická

	b) určení lhůty k předání nebo zpřístupnění zákaznických dat ze strany poskytovatele orgánu veřejné moci, c) určení doby, po kterou budou data uchované poskytovatelem po ukončení smlouvy o poskytování služby cloud computingu a d) určení lhůty k vymazání zákaznických dat poskytovatelem.	
9.6	**Vlastnictví zákaznických dat** Orgán veřejné moci má v plném rozsahu po celou dobu využívání služby cloud computingu zachována vlastnická práva k zákaznickým datům. Přípustné případy využití zákaznických dat poskytovatelem jsou definovány ve smlouvě s poskytovatelem.	nízká střední vysoká kritická
9.7	**Bezpečný výmaz dat** Zákaznická data jsou po ukončení smluvního vztahu vymazána způsobem, který je v souladu s relevantními právními a regulatorními požadavky.	nízká střední vysoká kritická
10. Nákup, vývoj a úprava informačních systémů		
10.1	**Oddělení prostředí** Provozní prostředí služby cloud computingu je poskytovatelem fyzicky nebo logicky odděleno od testovacího nebo vývojového prostředí služby cloud computingu, aby se zabránilo neautorizovanému přístupu k zákaznickým datům, šíření škodlivého kódu nebo změnám technických aktiv. Z důvodu ochrany důvěrnosti dat data obsažená v provozním prostředí nejsou používaná v testovacím ani v jakémkoliv jiném prostředí.	střední vysoká kritická
10.2	**Informování o významných změnách**[7)] Orgán veřejné moci je s dostatečným předstihem předem definovaným způsobem informován o plánované významné změně[7)] v poskytování služby cloud computingu a jejích dopadech.	vysoká kritická
11. Řízení dodavatelů		
11.1	**Informování o subdodavatelích** Orgán veřejné moci je informován o subdodavatelích poskytovatele, a to jak před uzavřením smlouvy o poskytování služby cloud computingu, tak vždy s dostatečným předstihem před změnou subdodavatele.	střední vysoká kritická

12. Správa kybernetických bezpečnostních událostí a incidentů		
12.1	**Informování o kybernetickém bezpečnostním incidentu** Poskytovatel informuje orgán veřejné moci 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 kybernetického bezpečnostního incidentu uzavřeno, informuje poskytovatel orgán veřejné moci o přijatých opatřeních.	nízká střední vysoká kritická
12.2	**Vyhodnocování kybernetických bezpečnostních událostí** Poskytovatel má zavedeny a využívá nástroje pro detekci, sběr a vyhodnocování kybernetických bezpečnostních událostí.	nízká střední vysoká kritická
13. Řízení kontinuity činností		
13.1	**Plán kontinuity činností** Orgán veřejné moci má zdokumentované postupy pro případ neočekávaného ukončení činnosti poskytovatele, případ omezení přístupu k zákaznickým datům a přesun zákaznických dat (včetně nezbytných provozních údajů) zpět nebo k jinému poskytovateli.	nízká střední vysoká kritická
14. Soulad s předpisy a audit		
14.1	**Identifikace požadavků** Poskytovatel jednoznačně identifikuje, dokumentuje a udržuje aktuální veškeré relevantní povinnosti vyplývající z právních předpisů a smluvní požadavky kladené na poskytovatele a týkající se bezpečnosti informací služby cloud computingu. Poskytovatel dokumentuje způsob, jakým tyto povinnosti dodržuje.	střední vysoká kritická
14.2	**Právo auditu Úřadem** Ve vztahu k dané službě cloud computingu je poskytovatelem jednou ročně nebo na základě opakujících se kybernetických bezpečnostních incidentů nebo v případě rozporu vůči deklarovaným parametrům umožněno Úřadu zdarma provedení kontroly	nízká střední vysoká

	splnění požadavků podle kontrolního řádu[10)] na všech místech a zařízeních souvisejících s poskytováním služby cloud computingu. Poskytovatel zároveň poskytne Úřadu veškerou potřebnou součinnost, vyjma zpřístupnění či předání zákaznických dat bez souhlasu dotčeného orgánu veřejné moci.	kritická
14.3	**Zákaznický audit** Orgán veřejné moci je oprávněn provést audit souladu systému řízení bezpečnosti informací poskytovatele s právem České republiky nebo smluvními podmínkami a dodržování politik poskytovatele.	vysoká kritická
15. Žádosti cizozemských orgánů o zpřístupnění nebo předání dat		
15.1	**Popis povinností poskytovatele předávat a zpřístupňovat informace** Poskytovatel jasně a srozumitelně uvádí své povinnosti vyplývající z právních předpisů států odlišných od členských států EU/ESVO, v nichž poskytovatel předpokládá zpracování zákaznických dat týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů cizozemským orgánům včetně zdůvodnění, proč uvedené povinnosti na poskytovatele dopadají.	nízká střední vysoká kritická
15.2	**Seznámení se s povinnostmi poskytovatele předávat a zpřístupňovat informace** Orgán veřejné moci se seznámí s povinnostmi poskytovatele vyplývajícími z právních předpisů států odlišných od členských států EU/ESVO, týkajících se zpřístupnění a předávání zákaznických dat a specifických provozních údajů cizozemským orgánům včetně zdůvodnění, proč uvedené povinnosti na poskytovatele dopadají.	nízká střední vysoká kritická
15.3	**Vyrozumění orgánu veřejné moci o žádosti o předání nebo zpřístupnění** V případě, že poskytovatel obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a provozních údajů, odkáže tohoto žadatele na orgán veřejné moci nebo o takové žádosti bezodkladně informuje orgán veřejné moci, pokud to právní řád, jemuž poskytovatel podléhá, nezakazuje.	nízká střední
15.4	**Vyrozumění orgánu veřejné moci o žádosti o předání nebo zpřístupnění** V případě, že poskytovatel obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, odkáže tohoto žadatele na orgán veřejné moci nebo o takové žádosti orgán veřejné moci bezodkladně informuje. Pokud právní řád, jemuž poskytovatel podléhá, poskytovateli zakazuje informovat orgán veřejné moci, vyvine veškeré možné zákonné úsilí, aby dosáhl zrušení tohoto zákazu a využije všech dostupných opravných prostředků s cílem zpochybnit takový zákaz, popřípadě pozastavit účinky zákazu, dokud soud nerozhodne ve věci samé. Pokud nedosáhne zrušení povinnosti zákazu informování orgánu veřejné moci, pak poskytovatel orgán veřejné moci informuje poté, co vyprší platnost právního zákazu, např. po vypršení období mlčenlivosti nařízeného zákonem nebo soudem.	vysoká kritická

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

15.5	**Právní posouzení žádostí o předání nebo zpřístupnění** V případě, že poskytovatel obdrží žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat nebo specifických provozních údajů bez souhlasu orgánu veřejné moci, zajistí poskytovatel její odpovídající právní posouzení. Posouzení zohlední, zda má žádost cizozemského orgánu proveditelný a platný právní základ, zda rozsah zákaznických dat nebo specifických provozních údajů, která má poskytovatel zpřístupnit nebo předat, je přiměřený účelu žádosti a jaké další kroky je třeba podniknout. Poskytovatel uchová právní posouzení žádosti alespoň 5 let od jeho vyhotovení pro účely kontroly nebo ho prokazatelně předá orgánu veřejné moci.	nízká střední
15.6	**Právní posouzení žádostí o předání nebo zpřístupnění** V případě, že poskytovatel obdrží žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat nebo specifických provozních údajů bez souhlasu orgánu veřejné moci, zajistí poskytovatel její odpovídající právní posouzení. Posouzení zohlední, zda má žádost cizozemského orgánu proveditelný a platný právní základ, zda rozsah zákaznických dat nebo specifických provozních údajů, která má poskytovatel zpřístupnit nebo předat, je přiměřený účelu žádosti a jaké další kroky je třeba podniknout. Poskytovatel uchová právní posouzení žádosti alespoň 10 let od jeho vyhotovení pro účely kontroly nebo ho prokazatelně předá orgánu veřejné moci.	vysoká kritická
15.7	**Závazek k vynaložení úsilí před zpřístupněním** V případě, že poskytovatel obdrží žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat nebo specifických provozních údajů bez souhlasu orgánu veřejné moci, vyvine poskytovatel veškeré možné zákonné úsilí, aby zabránil zpřístupnění nebo předání zákaznických dat a specifických provozních údajů na základě této žádosti, zejména zohlední povinnosti vyplývající z právních předpisů České republiky a Evropské unie a bude usilovat o zrušení povinnosti zpřístupnění nebo předání zákaznických dat a specifických provozních údajů.	vysoká kritická
15.8	**Předání nebo zpřístupnění po kladném vyhodnocení** V případě, že poskytovatel obdrží žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat nebo specifických provozních údajů, poskytovatel zpřístupní nebo předá nezbytně nutná zákaznická data a specifické provozní údaje na základě této žádosti, pokud právní posouzení poskytovatele provedené podle pravidla upraveného na řádku 15.5 nebo 15.6 této přílohy ukázalo, že žádost má proveditelný a platný právní základ a na tomto základě musí být žádosti vyhověno.	nízká střední vysoká
15.9	**Odmítnutí žádosti o zpřístupnění** V případě, že poskytovatel obdrží žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, tuto žádost odmítne a data nevydá a nezpřístupní. Toto pravidlo se neuplatní pro zákaznická data a specifické provozní údaje zpracovávané mimo území České republiky s výslovným písemným souhlasem orgánu veřejné moci podle pravidla upraveného na řádku 1.7 této přílohy.	kritická