

Vodítko pro orgány veřejné správy a poskytovatele cloud computingu ke splnění požadavků vyhlášky č. 412/2025 Sb.

Cílem tohoto vodítka, které vypracovala Digitální a informační agentura ve spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost, je vyjasnění odpovědnosti a možného způsobu splnění jednotlivých bezpečnostních pravidel z přílohy k vyhl. č. 412/2025 Sb., o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu (dále jen “Vyhláška”). Z charakteru uvedených bezpečnostních pravidel je zřejmé, že jejich způsob splnění se v zásadě bude lišit (řádek od řádku) a bude oscilovat mezi odpovědností orgánů veřejné správy (dále jen „OVS“), odpovědností poskytovatele, doložením bezpečnostních opatření na straně OVS, a doložením bezpečnostních opatření na straně poskytovatele, případně bude splnění vyžadovat jejich kombinaci. Z toho důvodu je snahou navrhovaného vodítka vyjasnit pro jednotlivé body přílohy Vyhlášky vhodné způsoby a možnosti jejich splnění.

Tabulka pravidel uvedená níže byla převzata z přílohy Vyhlášky, avšak vpravo jsou přidány sloupce “Způsob zajištění” a “Skupina”, kde se pro jednotlivá pravidla Vyhlášky uvádí, jakým způsobem lze dané požadavky na OVS adekvátně splnit, včetně jejich rozčlenění do skupin za účelem snadnějšího určení zdroje požadovaných podkladů.

Uvádí se v zásadě 4 způsoby (zdroje podkladů) ke splnění těchto požadavků, případně jejich kombinace:

- **sloupec Skupina = „SML“:** specifické požadavky na smluvní ujednání mezi poskytovatelem cloud computingu a OVS.
 - **Celkem: 24 požadavků** na smluvní ujednání mezi OVS a poskytovatelem
- **sloupec Skupina = „VoBK“:** poskytovatel předá k těmto bodům Vyhlášky zjednodušenou verzi svojí deklarace k obdobným řádkům vyhl. č. 505/2025 Sb., o bezpečnostních kritériích (dále jen „VoBK“), tak jak je uvedl v procesu zápisu svojí nabídky cloud computingu (po dobu přechodného období to mohou být i deklarace podle staré vyhl. č. 316/2021 Sb.). Tato zjednodušená verze může vynechat některé důvěrné detaily z pohledu poskytovatele, ale musí zákazníkovi (OVS) objasnit a doložit splnění relevantních kritérií Vyhlášky.
 - **Celkem: 35 požadavků** na deklaraci (ze strany poskytovatele) z VoBK.

- **sloupec Skupina = „ISO“:** poskytovatel zpřístupní popis svých opatření k uvedeným kontrolním bodům certifikace ISO 27001 / 27017 / 27018 na jisté střední úrovni detailu, tedy s uvedením podrobností o zavedených opatřeních na svojí straně, avšak bez detailů, které by zvyšovaly riziko jejich zneužití možnými útočníky. V tomto vodítku je odkazováno na strukturu opatření dle verze ISO 27001:2022, protože k 31.10.2025 již uplynulo tříleté přechodné období a certifikáty vystavené podle předchozí normy ISO/IEC 27001:2013 již nejsou dále považovány za platné.
 - **Celkem: 18 požadavků** na popis opatření z certifikací (nebo z bezpečnostní politiky poskytovatele pro BÚ 1) ISO řady 27000
- **sloupec Skupina = „OVS“:** požadavky na bezpečnostní politiky samotného OVS. V některých případech musí OVS pro splnění daného bezpečnostního pravidla stavět na vyjádření poskytovatele, které obdrží v rámci předání podkladů uvedených výše („VoBK“, „ISO“).
 - **Celkem: 14 požadavků** na bezpečnostní politiky OVS

Poznámka: využívání cloud computingu ze strany OVS se obvykle opírá o ZoISVS § 6l odst. 1 písm. a), tedy o již zapsané služby cloud computingu poskytovatele státního cloud computingu nebo jiného (komerčního) zapsaného poskytovatele, a proto tito poskytovatelé mohou s výhodou využít podklady již dříve doložené v procesu zápisu nabídky. Avšak v případě, kdy OVS využívá cloud computing na základě § 6l odst. 1 písm. b) nebo písm. c) ZoISVS, tyto cloudové služby neprochází procesem zápisu nabídky, avšak stále se na ně uplatňují bezpečnostní pravidla pro OVS dle VoBP dle § 6l odst. 3 ZoISVS. V takovém případě příslušní poskytovatelé cloud computingu nebudou mít k dispozici dále citované podklady z procesu zápisu nabídky dle VoBK a níže uvedené řádky označené „VoBK“ budou muset doložit využívajícím OVS jiným způsobem, např. podklady k certifikaci ISO/IEC 27001 nebo smluvními závazky.

Seznam použitých zkratk:

API – Aplikační programové rozhraní (Application Programming Interface)

BÚ – Bezpečnostní úroveň podle vyhl. č. 411/2025 Sb., o bezpečnostních úrovních informačních systémů veřejné správy

EU/ESVO – Evropská unie/Evropské sdružení volného obchodu

FedRAMP – U.S. Federal Risk and Authorization Management Program pro standardizované hodnocení bezpečnosti

ISMS – Information Security Management System, též jako SRBI – Systém řízení bezpečnosti informací

OVS – Orgán veřejné správy

VoBK – Vyhláška č. 505/2025 Sb., některých požadavcích pro zápis do katalogu cloud computingu

VoBP – Vyhláška č. 412/2025 Sb., o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu

ZoISVS – Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

nZKB – Zákon č. 264/2025 Sb., o kybernetické bezpečnosti

Řádek	Bezpečnostní pravidlo	Bezpečnostní úroveň	Způsob zajištění	Skupina
1. Obecné podmínky pro službu cloud computingu				
1.1	<p>Informace o poloze zpracování zákaznických dat</p> <p>Orgán veřejné správy 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.</p>	nízká střední vysoká kritická	<p>Zajistit, aby ve smlouvě s poskytovatelem byla obsažena základní informace o poloze zpracování dat (na úrovni státu). OVS musí dále obdržet od poskytovatele jeho deklarace o poloze zpracování zákaznických dat, které uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 1 (Příl. 1) ř. 1.1, 1.2 BÚ 2 (Příl. 2) ř. 1,1, 1.2 BÚ 3 (Příl. 3) ř. 1.1 až 1.5 BÚ 4 (Příl. 4) ř. 1,1, 1.2</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použijí řádky 1.1 až 1.8, pokud je vyžadován pro danou BÚ.</p>	SML VoBK
1.2	<p>Posouzení rizika předání nebo zpřístupnění dat cizozemským orgánům</p> <p>Orgán veřejné správy 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. Orgán veřejné správy může využívat službu cloud computingu, u které vyhodnotil rizika pro bezpečnost informací jako přijatelná. Vyhodnocení rizik orgán veřejné správy písemně zaznamenává.</p>	nízká střední vysoká kritická	<p>V zásadě požadavek na OVS, přičemž OVS musí obdržet od poskytovatele za účelem posouzení rizik jeho deklarace, které uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 1 (Příl. 1) ř. 2.1, 2.2 BÚ 2 (Příl. 2) ř. 2.1, 2.2 BÚ 3 (Příl. 3) ř. 2.1, 2.2 BÚ 4 (Příl. 4) ř. 2,1, 2.2</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použijí řádky ř. 1.1 až 1.7 a dále 2.5, pokud je vyžadován pro danou BÚ.</p>	OVS VoBK

1.3	<p>Trvalé uložení dat na území členských států Evropské unie a členských států Evropského sdružení volného obchodu</p> <p>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.</p>	vysoká kritická	<p>OVS musí obdržet od poskytovatele jeho deklaráce o trvalém uložení zákaznických dat na území EU/ESVO, které uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 3 (Příl. 3) ř. 1.2 BÚ 4 (Příl. 4) ř. 1.2</p> <p>V případě deklaráce podle staré vyhl. č. 316/2021 Sb. se použije řádek 1.3, pokud je vyžadován pro danou BÚ.</p>	VoBK
1.4	<p>Trvalé uložení specifických provozních údajů na území EU/ESVO</p> <p>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.</p>	vysoká kritická	<p>OVS musí obdržet od poskytovatele jeho deklaráce o trvalém uložení specifických provozních údajů na území EU/ESVO, které uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 3 (Příl. 3) ř. 1.3 BÚ 4 (Příl. 4) ř. 1.2</p> <p>V případě deklaráce podle staré vyhl. č. 316/2021 Sb. se použije řádek 1.4, pokud je vyžadován pro danou BÚ.</p>	VoBK
1.5	<p>Omezení zpracování dat mimo území členských států EU/ESVO</p> <p>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 zákaznická data zpracovávána i na území jiných států, pokud v popisu služby cloud computingu bude popsán způsob ochrany zákaznických dat před narušením bezpečnosti informací.</p>	vysoká kritická	<p>OVS musí obdržet od poskytovatele jeho deklaráce o trvalém uložení zákaznických dat na území EU/ESVO, které uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 3 (Příl. 3) ř. 1.4 BÚ 4 (Příl. 4) ř. 1.2</p> <p>V případě deklaráce podle staré vyhl. č. 316/2021 Sb. se použije řádek 1.5, pokud je vyžadován pro danou BÚ.</p>	VoBK

1.6	<p>Omezení zpracování specifických provozních údajů mimo území členských států EU/ESVO</p> <p>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.</p>	vysoká kritická	<p>OVS musí obdržet od poskytovatele jeho deklarace o trvalém uložení specifických provozních údajů na území EU/ESVO, které uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 3 (Příl. 3) ř. 1.5 BÚ 4 (Příl. 4) ř. 1.2</p>	VoBK
1.7	<p>Omezení zpracování dat mimo území České republiky</p> <p>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 správy.</p>	kritická	Pouze pro BÚ 4: nutné vyřešit smluvními podmínkami poskytovatele státního cloud computingu.	SML
1.8	<p>Smluvní ujednání o dostupnosti během běžného provozu</p> <p>Orgán veřejné správy uzavře pouze takovou smlouvu o poskytování služby cloud computingu, která jasně a srozumitelně vymezuje rozsah dostupnosti služby cloud computingu, včetně právních následků porušení sjednaného rozsahu dostupnosti služby cloud computingu.</p>	nízká střední vysoká kritická	Smluvní ujednání o úrovni služeb (SLA) může být součástí smlouvy nebo odkazem na samostatný dokument.	SML
1.9	<p>Soulad s certifikací systému řízení bezpečnosti</p> <p>Služba cloud computingu je provozována v rozsahu systému řízení bezpečnosti informací, který je v souladu s požadavky vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností nebo s požadavky ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001.</p>	nízká	<p>Zajistit, aby ve smlouvě byl obsažen adekvátní závazek bezpečnosti poskytované služby včetně zákaznických dat. Pro BÚ 1 je třeba mít ve smlouvě závazek, že je služba provozována v rámci ISMS, který je v souladu s požadavky ISO/IEC 27001. OVS musí dále obdržet od poskytovatele deklaraci o aplikovatelnosti jednotlivých opatření, kterou poskytovatel uvedl při zápisu nabídky dle VoBK, BÚ 1 (Příl. 1) ř. 6.1.</p>	VoBK SML
			V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije řádek 8.1.	

1.10	<p>Certifikace systému řízení bezpečnosti informací</p> <p>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).</p>	střední vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku prokázáním certifikace služby podle standardu ISO/IEC 27001 a rozsahu certifikace, který uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 2 (Příl. 2) ř. 6.1 BÚ 3 (Příl. 3) ř. 6.1 BÚ 4 (Příl. 4) ř. 6.1</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije pro BÚ 2 řádek 8.2; pro BÚ 3 a BÚ 4 řádek 8.3.</p>	VoBK
1.11	<p>Certifikace služby cloud computingu podle ISO/IEC 27017</p> <p>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.</p>	střední vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku prokázáním certifikace služby podle standardu ISO/IEC 27017 a rozsahu certifikace, který uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 2 (Příl. 2) ř. 6.1 BÚ 3 (Příl. 3) ř. 6.1 BÚ 4 (Příl. 4) ř. 6.1</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije pro BÚ 2 řádek 8.4; pro BÚ 3 a BÚ 4 řádek 8.5.</p>	VoBK
1.12	<p>Certifikace služby cloud computingu podle ISO/IEC 27018</p> <p>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</p>	vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku prokázáním certifikace služby podle standardu ISO/IEC 27018 a rozsahu certifikace, který uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 3 (Příl. 3) ř. 6.1 BÚ 4 (Příl. 4) ř. 6.1</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije řádek 8.6.</p>	VoBK

	systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven.			
1.13	<p>Prohlášení o aplikovatelnosti</p> <p>Orgán veřejné správy 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 této přílohy.</p>	vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku předáním prohlášení o aplikovatelnosti k certifikacím ISO/IEC 27001, ISO/IEC 27017 a ISO/IEC 27018 a předáním on-line přístupu k jejich úložišti na straně poskytovatele. Pro doložení uvedených pravidel 1.10 až 1.12 lze využít deklaráce ze zápisu nabídky:</p> <p>BÚ 3 (Příl. 3) ř. 6.1 BÚ 4 (Příl. 4) ř. 6.1</p>	VoBK
			V případě deklaráce podle staré vyhl. č. 316/2021 Sb. se použijí řádky 8.3, 8.5, 8.6.	
1.14	<p>Právo odstoupit od smlouvy</p> <p>Orgán veřejné správy ve smlouvě s poskytovatelem sjedná podmínky pro odstoupení od smlouvy bez sankcí v případě, že dojde k podstatnému zvýšení rizika z hlediska bezpečnosti informací u poskytovatele:</p> <p>a. změnou skutečného majitele poskytovatele podle zákona o evidenci skutečných majitelů¹; za změnu skutečného majitele se pro účely tohoto pravidla nepovažuje změna osoby ve vrcholovém vedení poskytovatele,</p> <p>b. změnou sídla poskytovatele do jiné země mimo území EU/EHP,</p> <p>c. vydáním protiopatření podle zákona o kybernetické bezpečnosti² Úřadem ve vztahu k poskytovateli nebo subdodavateli poskytovatele nebo dané služby cloud computingu,</p> <p>d. výmazem poskytovatele cloud computingu z katalogu cloud computingu z důvodu neplnění požadavků na poskytovatele cloud computingu podle § 6m ve spojení s § 6s odst. 1 zákona,</p>	vysoká kritická	Smlouva musí obsahovat zde uvedená ujednání. (pouze pro BÚ 3 a 4)	SML

	e. změnou subdodavatele poskytovatele bez souhlasu orgánu veřejné správy, f. změnou kontroly nad zásadními podpůrnými aktivy ³ využívanými poskytovatelem k poskytování služby cloud computingu, g. hrubým porušením smluvních podmínek ze strany poskytovatele a h. významnou změnou v poskytování služby cloud computingu.			
2. Organizace bezpečnosti informací				
2.1	Systém řízení bezpečnosti informací Poskytovatel má zaveden systém řízení bezpečnosti informací ⁴ . Rozsah systému řízení bezpečnosti informací zahrnuje organizační jednotky poskytovatele, lokality a procesy využívané k poskytování služby cloud computingu ⁵ , 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	Zajistit, aby ve smlouvě bylo obsaženo adekvátní ujednání o bezpečnosti poskytované služby včetně zákaznických dat. Poskytovatel zpřístupní dohodnutým způsobem: <ul style="list-style-type: none"> rozsah ISMS zpřístupněním certifikátu ISO/IEC 27001 (BÚ 2 / 3 / 4), nebo deklarací dle ID 6.1 z procesu zápisu nabídky dle VoBK (pro BÚ 1); V případě deklarace podle staré vyhl. č. 316/2021 Sb. se pro BÚ 1 použije řádek 8.1. popis zavedených opatření v rozsahu všech aplikovaných kontrolních bodů ISO/IEC 27001, 27017, 27018 (adekvátně pro BÚ 1 / 2 / 3 / 4) na takové úrovni, aby jim OVS porozuměl, avšak aby tento popis nepředstavoval riziko pro samotného poskytovatele a jeho služby. výsledky posledního auditu ISMS u poskytovatele. 	ISO VoBK SML
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,	nízká střední vysoká kritická	Zajistit, aby ve smlouvě bylo obsaženo ujednání o bezpečnosti poskytované služby vč. zákaznických dat, které uvádí existenci zavedené politiky bezpečnosti informací, případně (dle předmětné BÚ) je zavedení této politiky prokázáno v rámci auditní zprávy nebo zkráceného popisu bezpečnostních opatření dle řádku 2.1 výše.	SML ISO

	nejvýznamnější aspekty bezpečnostní strategie k dosažení stanovených cílů a organizační strukturu poskytovatele služby cloud computingu v rozsahu systému řízení bezpečnosti informací.			
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	Viz bod 2.1 výše: Poskytovatel zpřístupní dohodnutým způsobem: Popis zavedených opatření v rozsahu všech aplikovaných kontrolních bodů ISO/IEC 27001, 27017, 27018 (adekvátně pro BÚ 1 / 2 / 3 / 4) na takové úrovni, aby jim OVS porozuměl, avšak aby tento popis nepředstavoval riziko pro samotného poskytovatele a jeho služby.	ISO
3. Politiky				
3.1	Politika bezpečnosti informací Politika bezpečnosti informací, kterou se řídí poskytování služby cloud computingu, je v souladu s požadavky orgánu veřejné správy na bezpečnost informací.	nízká střední vysoká kritická	Požadavky na souladnost bezpečnostní politiky zachycené ve smlouvě (viz bod 2.2 výše) s bezpečnostními cíli OVS.	OVS SML
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	Poskytovatel zpřístupní dohodnutým způsobem popis zavedených opatření pro tématickou skupinu opatření 7 ISO/IEC 27001:2022 (Fyzická bezpečnost). Viz rovněž bod 2.1 výše.	ISO VoBK SML
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	Poskytovatel doloží splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle VoBK: BÚ1 (Příl. 1) ř. 4.2 BÚ 2 (Příl. 2) ř. 6.1 BÚ 3 (Příl. 3) ř. 4.2, 4.3 BÚ 4 (Příl. 4) ř. 4.2, 4.3	VoBK

			V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použijí řádky 6.3, 6.4, 6.5, 6.6, tak jak jsou vyžadovány pro jednotlivé BÚ.	
4.3	<p>Vzdálenost datových center od zdrojů rizik</p> <p>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.</p>	vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle – VoBK: BÚ 3 (Příl. 3) ř. 4.2 BÚ 4 (Příl. 4) ř. 4.2</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije řádek 6.4.</p>	VoBK
4.4	<p>Opatření k detekci a zabránění neoprávněného přístupu</p> <p>U budov a prostor vztahujících se k poskytování služby cloud computingu, včetně vstupu do 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.</p>	střední vysoká kritická	Poskytovatel zpřístupní dohodnutým způsobem popis zavedených opatření pro opatření 7.1, 7.2, 7.3 z certifikace ISO/IEC 27001:2022. (pouze pro BÚ 2 / 3 / 4)	ISO
5. Zajištění provozu služby cloud computingu				
5.1	<p>Bezpečné nakládání se zákaznickým obsahem</p> <p>Zákaznický obsah je zpracováván pouze způsobem sjednaným ve smlouvě o poskytování služby cloud computingu.</p>	nízká střední vysoká kritická	Zajistit, aby ve smlouvě bylo obsaženo adekvátní ujednání.	SML
5.2	Hodnocení informací o zranitelnostech a hrozbách	vysoká	Nemá přímý dopad na smluvní podmínky.	OVS

	Orgán veřejné správy vyhodnocuje informace a podklady týkající se zranitelností a hrozeb využívané služby cloud computingu a přijímá odpovídající opatření.	kritická	OVS využívá jako podklady dokumentaci dle bodu 2.1 výše.	
5.3	Rozdělení prostředí v cloudu Zákaznická data jsou bezpečně a striktně oddělována od jiných dat, která jsou uložena a zpracovávána na sdílených virtuálních a fyzických zdrojích využívaných k poskytování služby cloud computingu tak, aby byla zajištěna bezpečnost zákaznických dat.	střední vysoká kritická	Poskytovatel zpřístupní dohodnutým způsobem popis zavedených opatření; bezpečné oddělení zákaznických dat tenantů mezi sebou je zpravidla adresováno kontrolním bodem 8.22 - Oddělení sítí, z certifikace ISO/IEC 27001:2022. (pouze pro BÚ 2 / 3 / 4)	ISO
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 aktuálně odolnými kryptografickými prostředky nebo kryptografickými prostředky, které jsou v souladu s doporučením Úřadu v oblasti kryptografických prostředků zveřejněným na internetových stránkách Úřadu.	vysoká kritická	Poskytovatel zpřístupní dohodnutým způsobem popis zavedených opatření; šifrování zákaznických dat při přenosu do záložní lokality a v úložištích je zpravidla adresováno opatřením 5.14 - Přenos informací, a případně i 8.26 Požadavky na bezpečnost aplikací, z certifikace ISO/IEC 27001:2022. (pouze pro BÚ 3 / 4)	ISO

5.5	<p>Shromažďování provozních údajů a jejich náležitosti</p> <p>Provozní údaje se vztahem ke službě cloud computingu se shromažďují zejména o událostech:</p> <p>a) přihlašování a odhlašování u všech účtů, a to včetně neúspěšných pokusů,</p> <p>b) činnosti provedené administrátory⁶ 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 správy,</p> <p>c) činnosti provedené technickými aktivy, které mohou mít vliv na bezpečnost, zejména pokud hrozí jejich zneužití nebo změna chování, kterou není možné jiným způsobem detekovat.</p> <p>d) úspěšné i neúspěšné manipulace s účty, oprávněními a přístupovými právy,</p> <p>e) neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,</p> <p>f) činnosti uživatelů a technických aktiv na straně orgánu veřejné správy, které mohou mít vliv na bezpečnost informací ve službě cloud computingu,</p> <p>g) zahájení a ukončení činností technických aktiv,</p> <p>h) kritická i chybová hlášení technických aktiv a</p> <p>i) pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí.</p> <p>Provozní údaje zaznamenané podle tohoto pravidla obsahují zejména:</p> <p>a) datum a čas, včetně specifikace časového pásma,</p> <p>b) typ činnosti,</p> <p>c) identifikaci technického aktiva, které činnost zaznamenalo,</p> <p>d) jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,</p> <p>e) jednoznačnou síťovou identifikaci zařízení původce a</p> <p>f) úspěšnost nebo neúspěšnost činnosti.</p>	střední vysoká kritická	<p>Poskytovatel zpřístupní dohodnutým způsobem popis rozsahu shromažďovaných provozních údajů; pořizování provozních záznamů je adresováno opatřením 8.15 - Logování (včetně logů o činnosti administrátorů a operátorů), z certifikace ISO/IEC 27001:2022, případně poskytovatel cituje ze svých politik nebo jiných auditních zpráv (např. ISO/IEC 20000, SOC 2 Type 2, případně z bezpečnostních opatření pro certifikaci U.S. FedRAMP).</p> <p>(pouze pro BÚ 2 / 3 / 4)</p> <p>Pokud poskytovatelé služeb cloud computingu dokládají splnění požadavku dle bodu 5.5 písm. c) prostřednictvím bezpečnostní politiky nebo citací z auditních zpráv, měl by takový dokument jasně vymezit rozsah technických aktiv zahrnutých do logování. Tento rozsah by měl být definován alespoň typově. Současně by měl dokument obsahovat přehled typů (kategorií) činností nebo událostí, které jsou monitorovány a které mohou mít vliv na bezpečnost.</p>	ISO OVS
-----	---	-------------------------------	---	------------

5.6	<p>Monitorování a zaznamenávání událostí</p> <p>Služba cloud computingu zahrnuje nástroj pro monitorování a zaznamenávání událostí. Orgán veřejné správy má přístup k informacím o stavu zabezpečení, zejména k informacím vyplývajícím z provozních údajů shromážděných podle pravidla upraveného na řádku 5.5 této přílohy.</p>	střední vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 2 (Příl. 2) ř. 7.1 BÚ 3 (Příl. 3) ř. 7.1 BÚ 4 (Příl. 4) ř. 7.1 (pouze pro BÚ 2 / 3 / 4)</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije řádek 9.2, příp. řádek 9.3.</p>	VoBK
5.7	<p>Doba uchování provozních údajů</p> <p>Provozní údaje shromážděné podle pravidla upraveného na řádku 5.5 této přílohy jsou uchovány po dobu alespoň 12 měsíců od jejich vytvoření.</p>	vysoká	<p>Pro delší retenční dobu provozních záznamů, týkajících se služeb cloud computingu, musí OVS využít některou z dostupných alternativ archivace logů, například:</p> <p>a) využít speciální volby (options) platformních služeb provozních záznamů cloudových poskytovatelů, které umožní delší uchovávání provozních záznamů než 12 měsíců. např. v cloudu Microsoft to umožňuje Azure Log Analytics Long-term retention, u AWS to umožňuje AWS CloudWatch Retention Options, u Oracle to je OCI Logging Analytics Archive Storage.</p> <p>b) využít k tomu určené služby cloudového archivního úložiště, kam lze provozní záznamy odkládat pro dlouhodobé uložení, např. Azure Storage with Lifecycle policy, AWS S3 Lifecycle with Glacier option, Oracle OCI Logging with Log Routing option do OCI Object Storage Archive Tier. Tyto služby mají vestavěné mechanismy pro archivaci logů za účelem splnění takových povinností.</p> <p>c) využít k tomu vlastní archivní úložiště on-premise a logy si pravidelně do tohoto úložiště odkládat.</p> <p>(pouze pro BÚ 3)</p>	OVS, SML
5.8	<p>Doba uchování provozních údajů</p>	kritická	<p>Pouze pro BÚ 4: nutné vyřešit smluvními podmínkami poskytovatele státního cloud computingu.</p>	SML

	Provozní údaje shromážděné podle pravidla upraveného na řádku 5.5 této přílohy jsou uchovány po dobu alespoň 18 měsíců od jejich vytvoření.			
5.9	<p>Ukládání provozních údajů</p> <p>Vygenerované provozní údaje jsou uchovávány ve vhodné, neměnné a sdružené formě bez ohledu na jejich zdroj tak, aby bylo možné centrální 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 technického aktiva. 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 je zabezpečen aktuálně odolnými kryptografickými prostředky.</p>	střední vysoká kritická	<p>Poskytovatel zpřístupní dohodnutým způsobem citace ze zavedených opatření k opatření 8.15 ISO/IEC 27001:2022: rozsah pořizování provozních logů, jejich ochrana před neoprávněnou manipulací a jejich pravidelný přezkum (včetně logů o činnosti administrátorů a operátorů).</p> <p>Možnost sdružování provozních údajů a jejich centrálního vyhodnocení může být jak implicitní funkcionalitou cloudových služeb, nebo může být realizována nástroji OVS. Za způsob splnění tohoto požadavku musí být nakonec odpovědné OVS.</p> <p>Poskytovatel musí splňovat požadavek ověřování identity mezi technickými aktivy shromažďujícími provozní údaje a mezi technickými aktivy na nichž jsou provozní údaje vytvářeny, a dále ochranu přenosu provozních údajů mezi technickými aktivy aktuálně odolnými kryptografickými prostředky.</p> <p>(pouze pro BÚ 2 / 3 / 4)</p>	ISO OVS
5.10	<p>Poskytnutí provozních údajů orgánu veřejné správy</p> <p>Orgán veřejné správy má na žádost k dispozici provozní údaje o činnostech uživatelů, ve vhodné formě a v přiměřeném čase tak, aby mohl provést analýzu jakékoliv kybernetické bezpečnostní události, která se ho týká.</p>	střední vysoká kritická	<p>Ukládání provozních údajů na straně poskytovatele je vyžadováno v rámci ISO/IEC 27001:2022, opatření 8.15 - Zaznamenávání událostí formou logů. Kromě toho musí poskytovatel doložit i způsob předávání provozních údajů OVS; za tímto účelem může poskytovatel citovat z deklarace, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 2 (Příl. 2) ř. 7.1 BÚ 3 (Příl. 3) ř. 7.1 BÚ 4 (Příl. 4) ř. 7.1</p> <p>(pouze pro BÚ 2 / 3 / 4)</p>	ISO, VoBK

			V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije řádek 9.2, příp. řádek 9.3.	
6. Správa identit a řízení přístupu				
6.1	Vícefaktorová autentizace pro přístup Přístup orgánu veřejné správy do správy služby cloud computingu je zabezpečen vícefaktorovou autentizací.	střední vysoká kritická	Nejedná se o smluvní požadavek, ale o povinnost, OVS si vícefaktorovou autentizaci pro administraci služeb CC musí správně nastavit a vynucovat. Poskytovatelé se zapsanými nabídkami v BÚ 2 / 3 / 4 mají povinnost doložit certifikaci na ISO/IEC 27001:2022, přičemž opatření 8.5 vyžaduje možnost vícefaktorové autentizace do správy služby cloud computingu.	OVS
6.2	Řízení přístupu orgánu veřejné správy Orgán veřejné správy řídí přístupy uživatelů a technických aktiv na straně orgánu veřejné správy do služby cloud computingu, zejména: a) přiřazuje jedinečná uživatelská jména, b) uděluje a upravuje uživatelské účty a účty technických aktiv na straně orgánu veřejné správy 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 ¹ a účty technických aktiv na straně orgánu veřejné správy 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	Toto pravidlo představuje požadavek na bezpečnostní politiku a opatření na straně OVS.	OVS
6.3	Řízení přístupu poskytovatele Poskytovatel v rámci své organizace řídí přístupy k informačnímu systému využívanému k poskytování služby cloud computingu orgánu veřejné správy.	nízká střední vysoká kritická	Poskytovatel zpřístupní dohodnutým způsobem popis zavedených opatření; řízení přístupu v rámci organizace je adresováno skupinou opatření 5.15 – 5.18 (Řízení přístupu, správa identit a přístupová práva), z certifikace ISO/IEC 27001:2022.	ISO

6.4	<p>Dohody o mlčenlivosti a důvěrnosti</p> <p>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.</p>	nízká střední vysoká kritická	Poskytovatel zpřístupní dohodnutým způsobem popis zavedených opatření; mlčenlivost a důvěrnost zaměstnanců poskytovatele jsou adresovány skupinou opatření 5.4, 6.3 a 6.4 (Odpovědnosti vedení; Povědomí, vzdělávání a školení; Disciplinární proces), z certifikace ISO/IEC 27001:2022.	ISO
6.5	<p>Přístupová práva administrátorů⁹⁾ a technických aktiv na straně poskytovatele</p> <p>Přístupová práva jsou přidělována konkrétním administrátorům⁹⁾ a technickým aktivům na straně poskytovatele podle principu nutnosti vědět (need-to-know principle) a časově omezena na základě hodnocení rizik poskytovatele.</p>	nízká střední vysoká kritická	Poskytovatel zpřístupní dohodnutým způsobem popis zavedených opatření; přístupová práva administrátorů a technických aktiv a jejich správa podle principů nutnosti vědět (need-to-know, least privilege) jsou obvykle adresovány opatřeními 8.2 - Privilegovaná přístupová práva, případně 8.3 – Omezení přístupu k informacím, případně pro technická aktiva 8.18 - Použití privilegovaných nástrojů, z certifikace ISO/IEC 27001:2022.	ISO
6.6	<p>Souhlas pro přístup k zákaznickým datům nebo specifickým provozním údajům</p> <p>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 správy.</p> <p>Pro potřeby udělení tohoto souhlasu je orgán veřejné správy informován o důvodu, době trvání, času, typu a rozsahu přístupu tak, aby byl schopen vyhodnotit rizika spojená s tímto přístupem.</p>	kritická	Pouze pro BÚ 4: nutné vyřešit smluvními podmínkami poskytovatele státního cloud computingu.	SML
7. Šifrování zákaznického obsahu				

7.1	<p>Šifrování zákaznického obsahu při přenosu</p> <p>Poskytovatel má zavedené procesy a technická opatření zabezpečeného přenosu využívajícího aktuálně odolné kryptografické prostředky a ověření identity při přenosu zákaznického obsahu po sítích mimo kontrolu poskytovatele.</p>	nízká střední vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 1 (Příl. 1) ř. 5.2 BÚ 2 (Příl. 2) ř. 5.2 a 5.3 BÚ 3 (Příl. 3) ř. 5.2 a 5.3 BÚ 4 (Příl. 4) ř. 5.2 a 5.3</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použijí řádky 7.2 a 7.3.</p>	VoBK
7.2	<p>Šifrování zákaznického obsahu při uchovávání</p> <p>Poskytovatel má zavedené procesy a technická opatření pro zabezpečení zákaznického obsahu během uchovávání využívající aktuálně odolné kryptografické prostředky.</p>	nízká střední vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 1 (Příl. 1) ř. 5.2 BÚ 2 (Příl. 2) ř. 5.2 a 5.3 BÚ 3 (Příl. 3) ř. 5.2 a 5.3 BÚ 4 (Příl. 4) ř. 5.2 a 5.3</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použijí řádky 7.2 a 7.3.</p>	VoBK
7.3	<p>Úroveň šifrování zákaznického obsahu</p> <p>Zákaznický obsah je při všech síťových přenosech a v úložištích ve službě cloud computingu šifrován v souladu s aktuálně odolnými kryptografickými prostředky nebo alespoň pomocí některého ze schválených algoritmů uvedených v doporučení Úřadu v oblasti kryptografických prostředků zveřejněném na internetových stránkách Úřadu.</p>	vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 3 (Příl. 3) ř. 5.3 BÚ 4 (Příl. 4) ř. 5.3</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije řádek 7.3.</p>	VoBK
8. Zabezpečení komunikace				

8.1	<p>Ochrana proti útokům typu odepření služby</p> <p>Orgán veřejné správy využívá nástroje nebo služby pro detekci a zmírnění útoků typu odepření služby (DoS/DDoS) jak na síťové, tak na aplikační úrovni.</p>	<p>vysoká kritická</p>	<p>V případě, že OVS využívá pro zajištění této funkcionality některou službu poskytovatele cloud computingu, doloží poskytovatel požadované vlastnosti takové služby deklarací, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 3 (Příl. 3) ř. 4.5 BÚ 4 (Příl. 4) ř. 4.5</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije řádek 6.7, avšak poskytovatel jej musí doplnit o informaci, jestli jeho nástroje pro detekci a zmírnění útoků pracují jak na síťové, tak i na aplikační úrovni.</p>	VoBK
8.2	<p>Ochrana datových přenosů do služby cloud computingu</p> <p>Zákaznická data přenášená do služby cloud computingu jsou chráněna proti narušení bezpečnosti informací v souladu s požadavky orgánu veřejné správy na zajištění bezpečnosti informací.</p>	<p>nízká střední vysoká kritická</p>	<p>Poskytovatel doloží podklady pro toto pravidlo deklarací, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 1 (Příl. 1) ř. 5.2 BÚ 2 (Příl. 2) ř. 5.2 a 5.3 BÚ 3 (Příl. 3) ř. 5.2 a 5.3 BÚ 4 (Příl. 4) ř. 5.2 a 5.3</p> <p>Dále může poskytovatel využít popis k opatření 5.14 - Přenos informací (včetně dohod o přenosu informací) z certifikace ISO/IEC 27001:2022.</p> <p>OVS pak musí vyhodnotit, zda ochrana zákaznických dat při přenosech do služby cloud computingu je v souladu s bezpečnostní politikou daného OVS.</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použijí řádky 7.2 a příp. 7.3.</p>	VoBK ISO OVS

8.3	<p>Ochrana datových přenosů ze služby cloud computingu</p> <p>Zákaznická data přenášená ze služby cloud computingu jsou chráněna proti narušení bezpečnosti informací v souladu se zavedenou politikou bezpečnosti informací poskytovatele.</p>	nízká střední vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 1 (Příl. 1) ř. 5.2 BÚ 2 (Příl. 2) ř. 5.2 a 5.3 BÚ 3 (Příl. 3) ř. 5.2 a 5.3 BÚ 4 (Příl. 4) ř. 5.2 a 5.3</p> <p>Dále může poskytovatel využít popis k opatření 5.14 - Přenos informací (včetně dohod o přenosu informací) z certifikace ISO/IEC 27001:2022.</p>	VoBK ISO OVS
			V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použijí řádky 7.2 a příp. 7.3.	
8.4	<p>Připojení do výměnného uzlu internetu</p> <p>Poskytovatel má zajištěno připojení do výměnného uzlu internetu (IXP) v České republice.</p>	vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 3 (Příl. 3) ř. 9.1 BÚ 4 (Příl. 4) ř. 9.1 (pouze pro BÚ 3 / 4)</p>	VoBK
			V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije řádek 5.1.	
9. Přenositelnost, propojení a exit strategie				
9.1	<p>Zajištění kontinuity informačního systému orgánu veřejné správy</p> <p>Orgán veřejné správy má při ukončení využívání služby zákaznická data a provozní údaje ve formátu a rozsahu nezbytném pro zajištění kontinuity informačního systému, 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</p>	nízká střední vysoká kritická	Smlouva musí obsahovat zde uvedená ujednání.	SML

	předem sjednán.			
9.2	<p>Plán pro ukončení využívání služby cloud computingu</p> <p>Orgán veřejné správy vytvoří plán pro ukončení využívání služby cloud computingu (dále jen „exit strategie“), který zahrnuje zejména:</p> <p>a) cíle, kterých má exit strategie dosáhnout,</p> <p>b) definici kritérií pro spuštění exit strategie,</p> <p>c) definici situací pro spuštění exit strategie, například:</p> <ol style="list-style-type: none"> 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 regulačními 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 změna⁶⁾ kontroly nad poskytovatelem, 8. významná změna⁶⁾ kontroly nad technickými aktivy využívanými poskytovatelem k poskytování služby cloud computingu, 9. významná změna⁶⁾ u subdodavatelů, 10. jiná významná změna⁶⁾ na straně poskytovatele relevantní pro poskytování služby cloud computingu, 11. podstatná nemožnost orgánu veřejné správy využívat službu cloud computingu, <p>d) definici možných variant řešení migrace,</p> <p>e) analýzu dopadů zaměřenou na náklady a lidské zdroje nutné k úspěšnému provedení exit strategie,</p> <p>f) rozdělení rolí a zodpovědností v průběhu exit strategie a transferu systémů k jiným poskytovatelům,</p> <p>g) určení dat nutných pro úspěšné zvládnutí exit strategie včetně určení formátu těchto dat,</p> <p>h) definici opatření k zajištění součinnosti poskytovatele při předání dat,</p> <p>i) určení doby pro provedení exit strategie,</p>	nízká střední vysoká kritická	Toto je primárně požadavek na OVS, avšak poskytovatel se musí smluvně zavázat poskytnout součinnost a podklady minimálně v rozsahu bodů d) až k) zde uvedených.	OVS SML

	j) definici parametrů úspěchu při provádění exit strategie a k) opatření pro zajištění úspěšného provedení exit strategie.			
9.3	Specifické požadavky na exit strategii v návaznosti na umístění dat orgánu veřejné správy V případě, že poskytovatel využívané služby cloud computingu tuto službu provozuje z datacenter umístěných a. na území pouze jednoho státu, nebo b. mimo území EU/ESVO, orgán veřejné správy do své exit strategie zahrne opatření zajišťující import a export dat orgánu veřejné správy v dostatečném objemu prostřednictvím zaslání šifrovaných fyzických paměťových médií.	vysoká kritická	Toto pravidlo je samostatný požadavek na OVS.	OVS
9.4	Zajištění požadavků na exit strategii Smlouva o poskytování služby cloud computingu zohledňuje požadavky orgánu veřejné správy na exit strategii podle pravidla upraveného na řádku 9.2 této přílohy.	nízká střední vysoká kritická	Smlouva musí zahrnovat součinnost poskytovatele a povinnost předat podklady pro vytvoření exit plánu na straně OVS.	SML
9.5	Dokumentace bezpečnosti vstupů a výstupů Služba cloud computingu je přístupná pro jiné služby cloud computingu nebo IT systémy orgánu veřejné správy skrze zdokumentované rozhraní příchozích a odchozích zákaznických dat tak, aby z nich orgán veřejné správy 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 správy zpřístupní příslušnou dokumentaci.	střední vysoká kritická	Požadavek na smlouvu – možnost importu/exportu zákaznických dat bez manuálního zásahu pracovníků poskytovatele. Týká se služeb CC, které ukládají zákaznická data ve stavu neaktivních dat.	SML
9.6	Smluvní podmínky o poskytování zákaznických dat Orgán veřejné správy uzavře pouze takovou smlouvu o poskytování služby cloud computingu, která ve vztahu k jejímu ukončení upravuje zejména:	nízká střední vysoká kritická	Požadavek na smlouvu – podrobnosti o způsobu předání dat OVS při exitu služby	SML

	<p>a) typ, rozsah, strukturu a formát dat, které poskytovatel předá orgánu veřejné správy; nedohodne-li se orgán veřejné správy s poskytovatelem jinak, zajistí orgán veřejné správy, že zákaznická data budou poskytovatelem předána ve strukturovaném, běžně používaném, strojově čitelném a interoperabilním formátu,</p> <p>b) určení lhůty k předání nebo zpřístupnění zákaznických dat ze strany poskytovatele orgánu veřejné správy,</p> <p>c) určení doby, po kterou budou data uchována poskytovatelem po ukončení smlouvy o poskytování služby cloud computingu a</p> <p>d) určení lhůty k vymazání zákaznických dat poskytovatelem.</p>			
9.7	<p>Vlastnictví zákaznických dat</p> <p>Orgán veřejné správy má v plném rozsahu po celou dobu využívání služby cloud computingu zachována vlastnická práva k zákaznickým datům. Příпустné případy využití zákaznických dat poskytovatelem jsou definovány ve smlouvě s poskytovatelem.</p>	<p>nízká</p> <p>střední</p> <p>vyšoká</p> <p>kritická</p>	Požadavek na smlouvu – klauzule o vlastnictví dat	SML
9.8	<p>Bezpečný výmaz dat</p> <p>Zákaznická data jsou po ukončení smluvního vztahu vymazána způsobem, který je v souladu s relevantními právními a regulatorními požadavky.</p>	<p>nízká</p> <p>střední</p> <p>vyšoká</p> <p>kritická</p>	<p>V souladu s nZKB se způsob likvidace dat bude řídit primárně požadavky nových vyhlášek o bezpečnostních opatřeních pro poskytovatele regulované služby č. 409/2025 Sb. a č. 410/2025 Sb. - dle zařazení OVS do režimu vyšších nebo nižších povinností. Pro ISVS (nebo jejich části) v BÚ 1 a BÚ 2 a pro OVS, která nejsou zahrnuta v rozsahu regulace nZKB, se „přiměřeně“ aplikují bezpečnostní opatření v režimu nižších povinností, viz také nový § 5b v ZoISVS. Bez ohledu na zařazení konkrétního ISVS do nižších BÚ 1 nebo BÚ2 však může mít OVS vyšší požadavky podle znění „jeho“ režimu povinností jakožto poskytovatele regulované služby a podle jeho interní bezpečnostní politiky. Z toho důvodu se doporučuje, aby poskytovatelé sdělili a doložili pro OVS, jaké možnosti likvidace dat v cloudových službách nabízejí, ve vztahu k Příloze č. 2 vyhl. č. 409/2025 Sb., o bezpečnostních opatřeních</p>	VoBK ISO

			<p>poskytovatele regulované služby v režimu vyšších povinností.</p> <p>Poskytovatel se zapsanou nabídkou v BÚ 3 nebo BÚ 4 může doložit splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 3 (Příl. 3) ř. 5.5 BÚ 4 (Příl. 4) ř. 5.4</p> <p>Další možnost doložení způsobu bezpečného výmazu dat je popisem opatření CLD 8.1.5 Removal of cloud service customer assets z certifikace ISO/IEC 27017, případně též 7.10 Úložná média, 7.14 Bezpečná likvidace nebo opakované použití zařízení z certifikace ISO/IEC 27001:2022. V případě, že poskytovatel deklaruje vlastnosti bezpečného výmazu dat cloudové služby zapsané v BÚ 1 a nemá k dispozici certifikace ISO 27017 nebo ISO 27001 viz výše, pak může doložit (ve vztahu k Příloze 2 vyhl. č. 409/2025 Sb.) pouze způsob likvidace dat podle odst. 4 písm. a) „Odstranění“.</p>	
			V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije pro BÚ 3 řádek 7.7, a pro BÚ 4 se použije řádek 7.6.	
10. Nákup, vývoj a úprava informačních systémů				
10.1	<p>Oddělení prostředí</p> <p>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 nejsou data obsažená v provozním prostředí používána v testovacím ani v jakémkoliv jiném prostředí.</p>	<p>střední vysoká kritická</p>	<p>Poskytovatel zpřístupní dohodnutým způsobem popis zavedených opatření; oddělení prostředí je adresováno opatřením 8.31 - Oddělení prostředí vývoje, testování a produkce, z certifikace ISO/IEC 27001:2022, a dále CLD 9.5.1 - Oddělení ve virtuálních výpočetních prostředích z ISO/IEC 27017.</p>	ISO

10.2	Informování o významných změnách Orgán veřejné správy je s dostatečným předstihem předem definovaným způsobem informován o plánované významné změně ⁶⁾ v poskytování služby cloud computingu a jejích dopadech.	vysoká kritická	Požadavek na smlouvu – ustanovení o informování o významných změnách ze strany poskytovatele cloud computingu.	SML
11. Řízení dodavatelů				
11.1	Informování o subdodavatelích Orgán veřejné správy 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	Požadavek na smlouvu, který je dnes již obvyklý vzhledem k procesu schvalování podzpracovatelů poskytovatele podle GDPR. Rozsah zde použitého pojmu „subdodavatelé poskytovatele“ je vymezen v ZolSVS, a to v těchto případech: 1) závislost na jiném cloud computingu, a to podle ZolSVS § 6n písm. e), což je případ podpůrného cloud computingu, dále vysvětlený v ZolSVS § 6t odst. 7 písm. a) 2) závislost na jiném cloud computingu, a to podle ZolSVS § 6n písm. f), což je případ přeprodávaného cloud computingu 3) ostatní dodavatelé poskytovatele, u kterých OVS předpokládá zpracovávání informací orgánu veřejné správy, a to dle ZolSVS § 6t odst. 6 písm. a), § 6t odst. 7 písm. b), a § 6t odst. 8 písm. b).	SML
12. Správa kybernetických bezpečnostních událostí a incidentů				
12.1	Informování o kybernetickém bezpečnostním incidentu Poskytovatel informuje orgán veřejné správy 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	nízká střední vysoká kritická	Poskytovatel doloží splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle VoBK: BÚ1 (Příl. 1) ř. 7.2 BÚ 2 (Příl. 2) ř. 7.2 BÚ 3 (Příl. 3) ř. 7.2 BÚ 4 (Příl. 4) ř. 7.2	SML VoBK

	incidentu uzavřeno, informuje poskytovatel orgán veřejné správy o přijatých opatřeních.		Současně je tento požadavek vhodné upravit ve smlouvě (běžná praxe vzhledem k obdobné úpravě v GDPR, čl. 33).	
			V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije řádek 9.3.	
12.2	Vyhodnocování kybernetických bezpečnostních událostí Poskytovatel má zavedeny a využívá nástroje pro detekci, sběr a vyhodnocování kybernetických bezpečnostních událostí.	nízká střední vysoká kritická	Poskytovatel doloží splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle VoBK: BÚ1 (Příl. 1) ř. 7.1 BÚ 2 (Příl. 2) ř. 7.1 BÚ 3 (Příl. 3) ř. 7.1 BÚ 4 (Příl. 4) ř. 7.1	VoBK
			V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije řádek 9.1 pro BÚ 1, a řádek 9.2 pro ostatní BÚ.	
13. Řízení kontinuity činností				
13.1	Plán kontinuity činností Orgán veřejné správy 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	Toto pravidlo je samostatný požadavek na OVS.	OVS
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	střední vysoká kritická	Poskytovatel zpřístupní dohodnutým způsobem popis zavedených opatření; soulad s regulačními požadavky viz skupina opatření 5.31 – 5.36 - Soulad s právními, smluvními a interními požadavky, z certifikace ISO/IEC	ISO

	se bezpečnosti informací služby cloud computingu. Poskytovatel dokumentuje způsob, jakým tyto povinnosti dodržuje.		27001:2022. (pouze pro BÚ 2 / 3 / 4)	
14.2	<p>Právo auditu Úřadem</p> <p>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 provedení kontroly splnění požadavků 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 správy.</p>	nízká střední vysoká kritická	Právo auditu Úřadem vyplývá ze zákonné povinnosti dle ZolSVS § 6n písm. b) až f), ve vazbě na § 6i (3)	VoBK
14.3	<p>Zákaznický audit</p> <p>Orgán veřejné správy je oprávněn provést audit souladu systému řízení bezpečnosti informací poskytovatele s právem České republiky nebo smluvními podmínkami a dodržování politik poskytovatele.</p>	vysoká kritická	Požadavek na smlouvu, který je dnes již obvyklý vzhledem k GDPR (čl. 28 – Zpracovatel, odst. 3 písm. h))	SML
15. Žádosti cizozemských orgánů o zpřístupnění nebo předání dat				

15.1	<p>Popis povinností poskytovatele předávat a zpřístupňovat informace</p> <p>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.</p>	nízká střední vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku deklarácí, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ1 (Příl. 1) ř. 2.2 BÚ 2 (Příl. 2) ř. 2.2 BÚ 3 (Příl. 3) ř. 2.2 BÚ 4 (Příl. 4) ř. 2.2</p> <p>V případě deklaráce podle staré vyhl. č. 316/2021 Sb. se použije řádek 2.5</p>	VoBK
15.2	<p>Seznámení se s povinnostmi poskytovatele předávat a zpřístupňovat informace</p> <p>Orgán veřejné správy 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.</p>	nízká střední vysoká kritická	Toto pravidlo je samostatný požadavek na OVS.	OVS
15.3	<p>Vyrozumění orgánu veřejné správy o žádosti o předání nebo zpřístupnění</p> <p>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 správy nebo o takové žádosti bezodkladně informuje orgán veřejné správy, pokud to právní řád, jemuž poskytovatel podléhá, nezakazuje.</p>	nízká střední	<p>Poskytovatel doloží splnění tohoto požadavku deklarácí, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ1 (Příl. 1) ř. 2.1 BÚ 2 (Příl. 2) ř. 2.1 (Pouze pro BÚ 1 a BÚ 2)</p> <p>V případě deklaráce podle staré vyhl. č. 316/2021 Sb. se použije řádek 2.1.</p>	VoBK

15.4	<p>Vyrozumění orgánu veřejné správy o žádosti o předání nebo zpřístupnění</p> <p>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 správy nebo o takové žádosti orgán veřejné správy bezodkladně informuje. Pokud právní řád, jemuž poskytovatel podléhá, poskytovateli zakazuje informovat orgán veřejné správy, vyvine veškeré možné zákonné úsilí, aby dosáhl zrušení tohoto zakazu a využije všech dostupných opravných prostředků s cílem zpochybnit takový zákaz, popřípadě pozastavit účinky zakazu, dokud soud nerozhodne ve věci samé. Pokud nedosáhne zrušení povinnosti zakazu informování orgánu veřejné správy, pak poskytovatel orgán veřejné správy informuje poté, co vyprší platnost právního zakazu, např. po vypršení období mlčenlivosti nařízeného zákonem nebo soudem.</p>	vysoká kritická	<p>Poskytovatel doloží splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ3 (Příl. 3) ř. 2.1 BÚ 4 (Příl. 4) ř. 2.1 (Pouze pro BÚ 3 a BÚ 4)</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije řádek 2.2.</p>	VoBK
15.5	<p>Právní posouzení žádostí o předání nebo zpřístupnění</p> <p>V případě, že poskytovatel obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat nebo specifických provozních údajů bez souhlasu orgánu veřejné správy, 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 správy.</p>	nízká střední	<p>Poskytovatel doloží splnění tohoto požadavku deklarací, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ1 (Příl. 1) ř. 2.1 BÚ 2 (Příl. 2) ř. 2.1 (Pouze pro BÚ 1 a BÚ 2)</p> <p>V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použije řádek 2.3.</p>	VoBK

15.6	<p>Právní posouzení žádostí o předání nebo zpřístupnění</p> <p>V případě, že poskytovatel obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat nebo specifických provozních údajů bez souhlasu orgánu veřejné správy, 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 správy.</p>	vysoká	<p>Poskytovatel doloží splnění tohoto požadavku deklarácí, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 3 (Příl. 3) ř. 2.1 (pouze pro BÚ 3)</p> <p>V případě deklaráce podle staré vyhl. č. 316/2021 Sb. se použije řádek 2.4.</p>	VoBK
15.7	<p>Závazek k vynaložení úsilí před zpřístupněním</p> <p>V případě, že poskytovatel obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat nebo specifických provozních údajů bez souhlasu orgánu veřejné správy, 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.</p>	vysoká	<p>Poskytovatel doloží splnění tohoto požadavku deklarácí, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ 3 (Příl. 3) ř. 2.1 (pouze pro BÚ 3)</p> <p>V případě deklaráce podle staré vyhl. č. 316/2021 Sb. se použije řádek 2.4.</p>	VoBK
15.8	<p>Předání nebo zpřístupnění po kladném vyhodnocení</p> <p>V případě, že poskytovatel obdrží právně závaznou 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</p>	nízká střední vysoká	<p>Poskytovatel doloží splnění tohoto požadavku deklarácí, kterou uvedl při zápisu nabídky dle VoBK:</p> <p>BÚ1 (Příl. 1) ř. 2.1 BÚ 2 (Příl. 2) ř. 2.1 BÚ 3 (Příl. 3) ř. 2.1 (pouze pro BÚ 1 / 2 / 3)</p>	VoBK

	platný právní základ a na tomto základě musí být žádosti vyhověno.		V případě deklarace podle staré vyhl. č. 316/2021 Sb. se použijí řádky 2.1, 2.2, 2.3, 2.4. V tomto novém pravidle se jedná o průřez uvedených kritérií ve vyhl. č. 316/2021 Sb.)	
15.9	<p>Odmítnutí žádosti o zpřístupnění</p> <p>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 správy podle pravidla upraveného na řádku 1.7 této přílohy.</p>	kritická	Pouze pro BÚ 4: nutné vyřešit smluvními podmínkami poskytovatele státního cloud computingu.	SML

¹ Zákon č. 37/2021 Sb., o evidenci skutečných majitelů, ve znění pozdějších předpisů.

² § 20 zákona č. 264/2025 Sb., o kybernetické bezpečnosti.

³ § 2 odst. 1 písm. c) zákona č. 264/2025 Sb., o kybernetické bezpečnosti.

⁴ § 2 písm. g) vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

⁵ § 8 odst. 1 písm. f) vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

⁶ § 2 písm. c) vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.