NÚKIB

VĚCNÝ ZÁMĚR CLOUDOVÉ VYHLÁŠKY

Podklad pro připomínky odborné veřejnosti

Verze 1.0, platná ke dni 31. 7. 2020

Obsah

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

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 560

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument není nijak právně závazný a slouží jako podklad pro připomínky ze strany odborné veřejnosti.

Konečná podoba vyhlášky o bezpečnostních pravidlech pro orgány veřejné moci využívající služeb cloud computingu [dle §6 písm. e) ZKB], se může podstatně lišit.

Tento postup nijak nenahrazuje řádné připomínkové řízení podle legislativních pravidel vlády.

1 Základní pojmy

poskytovatel cloud computingu (dále také jen poskytovatel)	Ten kdo žádá o zápis do katalogu cloud computingu a je prodejcem nebo materiálním dodavatelem.
zákazník	Orgán veřejné moci využívající cloudových služeb.
odběratel	Zákazník a ten kdo služeb využívá, např. občan ČR.
prodejce	Ten kdo vstupuje do smluvního vztahu se zákazníkem.
materiální dodavatel	Ten kdo přebírá zákaznická data a provozní údaje do svojí správy (tzn. bezpečnostní politiky) za účelem poskytování cloudové služby. Může se jednat o totožnou osobu s prodejcem.
systematický zpracovatel	Ten kdo zpracovává zákaznická data a provozní údaje, ale není materiálním dodavatelem. Systematický zpracovatel se řídí bezpečnostní politikou materiálního dodavatele.
zákaznická data	Všechna data, která jsou zákazníkem poskytnuta materiálnímu dodavateli během užívání cloudové služby.
zákaznický obsah	Textové, zvukové, video, obrazové nebo jiné binární informace, které byly odběratelem služby do cloud computingu uloženy, a to bez zahrnutí jejich provozních údajů; zákaznický obsah tvoří podmnožinu zákaznických dat. Za zákaznický obsah se považují i indexy k zákaznickému obsahu.
provozní údaje	Data vygenerovaná nebo odvozená materiálním dodavatelem nebo prodejcem během poskytování cloudové služby, jde především o provozní záznamy na straně poskytovatele cloudu; provozní údaje nezahrnují zákaznická data; provozní údaje mohou obsahovat osobní údaje
cloudová služba	Služba informačních technologií poskytovaná v rámci cloud computingu. Zahrnuje modely poskytování formou infrastruktura jako služba (IaaS), platforma jako služba (PaaS), a software jako služba (SaaS).
systémové komponenty	Objekty potřebné pro informační bezpečnost cloudové služby během vytváření, zpracování, ukládání, přenosu, vymazání nebo zničení informací v oblasti odpovědnosti poskytovatele cloudových služeb, např. brány firewall, vyrovnávače zatížení, webové servery, aplikační servery a databázové servery.
významná změna	Změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko.
provozní incident	Narušení poskytování služby s možným ale nikoliv nezbytným vlivem na bezpečnost informací.
bezpečnostní incident	Kybernetický bezpečnostní incident, ve smyslu ZKB= narušení bezpečnosti informací.
ISMS	Systém řízení bezpečnosti informací.
zpracování	Jakákoliv operace nebo soubor operací se zákaznickými daty a provozními údaji v elektronické podobě, prováděné pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

2 Práce s dokumentem

Cíl dokumentu

Cílem dokumentu je poskytnout veřejnosti, zájmovým skupinám, úřadům a odborníkům možnost seznámit se záměrem vyhlášky o obsahu a rozsahu bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu, včetně bezpečnostních úrovní pro využívání cloud computingu orgány veřejné moci a k tomuto záměru podat své připomínky (dále jen vyhláška). Vydáním této vyhlášky bude NÚKIB realizovat zmocnění vyplývající z § 6 písm. e) č. 181/2014 Sb., zákona o kybernetické bezpečnosti.

Vyhláška nestanovuje přímé povinnosti soukromému sektoru. Upravuje však podmínky, za kterých mohou orgány veřejné moci využívat cloud computingové služby ze strany soukromého sektoru.

Dokument nelze považovat za finální a bude na základě připomínek měněn. Výsledný návrh vyhlášky poté bude předložen do řádného legislativního procesu v souladu s legislativními pravidly vlády.[1] Návrh takto předložené vyhlášky bude pomocí informačního systém eKLEP[2] také k dispozici veřejnosti.

Naložení s připomínkami

Kdokoli může k tomuto věcnému záměru podat své připomínky. NÚKIB se bude připomínkami zabývat, pokud splní následující podmínky:

- Připomínka bude relevantní k řešené problematice;
- Připomínka bude alespoň stručně zdůvodněna;
- Připomínka bude zaslána emailem na adresu regulace@nukib.cz s předmětem „připomínky – cloudová vyhláška“;
- Připomínka bude podána na formuláři, který je přílohou tohoto dokument (viz příloha). Na jeden formulář lze vložit více připomínek;
- Připomínka bude podána do 17. srpna 2020;
- Připomínka bude obsahovat i návrh řešení.

[1] https://www.vlada.cz/cz/ppov/lrv/dokumenty/legislativni-pravidla-vlady-91209/
[2] https://apps.odok.cz/eklep

NÚKIB si vyhrazuje právo připomínky akceptovat, částečně akceptovat či neakceptovat.

Pokud předkladatel připomínky vyplní do formuláře své kontaktní údaje (jméno, příjmení, telefon, email) souhlasí s tím, aby jej NÚKIB v případě potřeby kontaktoval a to zejména za účelem doplnění, vysvětlení či vypořádání připomínky. V souvislosti s tím NÚKIB zadané údaje zpracuje.

NÚKIB bude obdržené připomínky zpracovávat v období od 18. srpna 2020.

3 Kontext a architektura vyhlášky

Využití a kontext cloudové vyhlášky lze rámcově popsat následovně. V souvislosti s novelou zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen ZoISVS) budou muset být informační systémy orgánu veřejné moci, které by měly být provozovány s využitím cloudových služeb, ohodnoceny podle dopadu narušení bezpečnosti informací a zařazeny do příslušné bezpečnostní úrovně. Kritéria pro tuto kategorizaci stanoví třetí část vyhlášky.

Cloudové služby nabízené ze strany poskytovatelů služeb orgánům veřejné moci budou taktéž rozděleny do bezpečnostních úrovní podle úrovně zabezpečení, kterou nabízejí. K této kategorizaci a k prokázání způsobilosti poskytovat služby příslušné bezpečnostní úrovně slouží první část vyhlášky.

V případě, že informační systém orgánu veřejné moci zařazený do příslušné bezpečnostní úrovně podle třetí části vyhlášky bude provozován v cloudu, bude orgán veřejné moci oprávněn využít pouze cloudovou službu odpovídající bezpečnostní úrovně určené podle první části vyhlášky. Zároveň zajistí splnění bezpečnostních pravidel pro tuto úroveň stanovených v druhé části vyhlášky.

Soukromý sektor bude moci poskytovat služby v bezpečnostní úrovni 1. - 3. Čtvrtou, nejvyšší bezpečnostní úroveň, bude moci poskytovat pouze státní poskytovatel.

Na základě tohoto konceptu bude vyhláška rozdělena do tří částí. Jedná se o:

1. **Kritéria pro ověření, zda cloudový poskytovatel splňuje požadavky jednotlivých bezpečnostních úrovní služby.**

V první části budou stanovena kritéria, která musí poskytovatel cloudových služeb splnit, aby mohl vstoupit do tzv. katalogu nabídek a nabídnout tak své služby orgánům veřejné moci. Tyto kritéria budou rozdílné podle bezpečnostních úrovní služby. Pokud poskytovatel služeb stanovené požadavky splní a doloží, bude mu umožněno vstoupit do příslušné bezpečnostní úrovně služby katalogu nabídek a nabízet orgánům veřejné moci cloudové služby.

Splnění těchto podmínek bude ověřovat Ministerstvo vnitra ve spolupráci s NÚKIB. Tento proces je nazýván jako EX ANTE KONTROLA.

2. **Stanovení obsahu a rozsahu bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.**

Druhá část vyhlášky stanoví obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci, které budou chtít cloudových služeb využívat. Jde tedy o seznam bezpečnostních požadavků, jejichž splnění budou muset orgány veřejné moci zajistit, pokud budou chtít využít cloudových

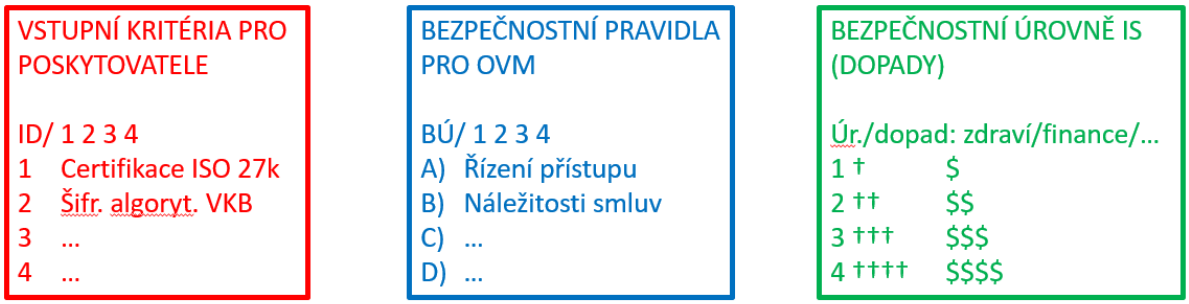
služeb. Tyto bezpečnostní pravidla budou často součástí výběrového řízení na poskytnutí cloudových služeb.

Splnění těchto podmínek bude kontrolováno ze strany Ministerstva vnitra a NÚKIB. Kontrola bude probíhat v době, kdy bude služba poskytována. Každá z bezpečnostních úrovní bude mít stanovena příslušná bezpečnostní opatření. Tento proces je nazýván jako EX POST KONTROLA.

3. Stanovit bezpečnostní úrovně informačních systémů

Informační systémy orgánů veřejné moci, které by měly být provozovány v cloudu, budou podle dopadů narušení bezpečnosti informací zařazeny do některé ze čtyř bezpečnostních úrovní (1 - nízká, 2 – střední, 3 – vysoká, 4 - kritická). Příslušně zařazený systém bude moci využít pouze ty nabídky služeb, které jsou zařazeny do stejné nebo vyšší bezpečností úrovně.

Graficky se jednotlivé část vyhlášky dají znázornit takto:



Návrh znění jednotlivých částí k připomínkám obsahují další kapitoly tohoto dokumentu.

4 Vstupní kritéria

Obsah této části podstatně vychází ze Souhrnné analytické zprávy k projektu Příprava vybudování eGovernment cloudu schválené vládou ČR dne 14. 11. 2018 a z poznatků a diskusí expertní skupiny vedené NÚKIB v období leden až červenec 2020.

Tabulka č. 1 Vstupní kritéria

ID VK	Vstupní kritérium	Čím doloží	Bezpečnostní úroveň				Distribuční model			Komentář NÚKIB
			1	2	3	4	IaaS	PaaS	SaaS	
1	Prodejce má sídlo nebo bydliště v členském státě EU (EHS) nebo má určeného svého zástupce ve členském státě EU obdobně dle čl. 27 GDPR.	výpis z obchodního rejstříku nebo obdobné zahraniční evidence, nebo písemné čestné prohlášení v rozsahu údajů obsažených v obchodním rejstříku v případě, že není v obchodním rejstříku zapsán	X	X	X	X	X	X	X	
2	Prodejce a materiální dodavatel nebyl pravomocně uznán vinným ze spáchání přestupku dle zákona o kybernetické bezpečnosti.	čestné prohlášení	X	X	X	X	X	X	X	
3	Prodejce a materiální dodavatel nebyl v posledních 5 letech před podáním žádosti o zápis do katalogu cloud computingu v České republice, žádném ze států EU nebo NATO a v zemi svého sídla pravomocně odsouzen pro trestný čin uvedený v příloze č. X (viz níže pod tabulkou) k této vyhlášce nebo obdobný trestný čin podle právního řádu konkrétní země; k zahlazeným odsouzením se nepřihlíží,	výpis z evidence Rejstříku trestů nebo obdobné evidence v zemi jeho sídla + čestné prohlášení o tom že za posledních 5 let nebyl pravomocně odsouzen v žádné zemi EU nebo NATO.	X	X	X	X	X	X	X	
4	Prodejce a materiální dodavatel nemá v České republice, v zemi svého sídla a zemích, kde jsou umístěna datacentra, ze kterých je poskytována služba v evidenci daní zachycen splatný daňový nedoplatek, včetně příslušného penále z dlužné částky, popřípadě na vyměřeném clu, včetně případných úroků	čestné prohlášení/informace z registru	X	X	X	X	X	X	X	

5	Prodejce a materiální dodavatel nemá v České republice, v zemi svého sídla a zemích, kde jsou umístěna datacentra, ze kterých je poskytována služba splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění	čestné prohlášení/informace z registru	X	X	X	X	X	X	X	
6	Prodejce a materiální dodavatel nemá v České republice, v zemi svého sídla a zemích, kde jsou umístěna datacentra, ze kterých je poskytována služba splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti	čestné prohlášení/informace z registru	X	X	X	X	X	X	X	
7	Zákaznická data a provozní údaje jsou trvale a nepřetržitě uloženy výlučně na území členských států EU/EHP.	Odkaz na část smluvních podmínek, kde je vymezen závazek trvalého uložení zákaznického obsahu na území EU/EHS + odkaz na tu část certifikace ISO 27001/auditní zprávy SOC 2®, ze které bude patrný úplný výčet datacenter a jejich lokace po úroveň katastrálního území/obce ve kterých bude zákaznický obsah trvale uložen.		X	X		X	X	X	

8	Zákaznická data a provozní údaje jsou zpracovávány na území členských států EU (EHP). Aniž je dotčeno pravidlo v ID 7, v odůvodněných případech, po nezbytně nutnou dobu, v nezbytném rozsahu mohou být zákaznická data a provozní údaje zpracovávány i na území jiných států, které zajišťují odpovídající úroveň ochrany ve smyslu čl. 45 GDPR, nebo jinde pokud materiální dodavatel poskytl vhodné záruky ve smyslu čl. 46, 47 GDPR. Výjimky pro specifické situace dle čl. 49 GDPR nejsou dotčeny.	Materiální dodavatel uvede u služby, u níž: * jsou zákaznická data i provozní údaje zpracovávány na území členských států EU/EHP, transparentní **označení takové služby a deklaraci závazku** zpracování zákaznických dat a provozních údajů na území členských států EU/EHP. * je zákaznický obsah zpracováván pouze na území členských států EU/EHP a zákaznická data bez zákaznického obsahu a provozní údaje jsou nebo mohou být zpracovávány mimo území členských států EU/EHP, transparentní **označení takové služby, výčet států** mimo území členských států EU/EHP, ve kterých zákaznická data bez zákaznického obsahu a provozní údaje jsou nebo mohou být zpracovávána. U zákaznických dat a provozních údajů zpracovávaných mimo EU popis toho, jak budou chráněny ve smyslu čl. 44 až 47 GDPR. * jsou nebo mohou být zákaznická data a provozní údaje zpracovávány mimo území členských států EU/EHP, transparentní **označení takových služeb**, **výčet států** mimo území členských států EU/EHP, ve kterých jsou nebo mohou být zákaznická data a provozní údaje zpracovávány a ve vztahu k zákaznickému obsahu, **důvody** za nichž je nebo může být zákaznický		X	X		X	X	X	Uvedené označení služeb bude propsáno do katalogu cloud computingu.

		obsah **obvykle zpracováván** mimo území členských států EU/EHP, **průměrnou dobu** po kterou je nebo může být zákaznický obsah **obvykle zpracováván** mimo EU/EHP a **obvyklý rozsah zákaznického obsahu**, který takto může být zpracováván. U zákaznických dat a provozních údajů zpracovávaných mimo EU popis toho, jak budou chráněny ve smyslu čl. 44 až 47 GDPR.								

9	Materiální dodavatel umožňuje vyžádání svolení zákazníka v případě zpracování zákaznického obsahu mimo území členských států EU/EHP pro účely zajištění podpory služby.	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy, ve které je popsán způsob vyžádání souhlasu zákazníka v případě exportu zákaznického obsahu mimo EU (EHS) pro účely zajištění podpory služby		X	X		X	X	X	Materiální dodavatel musí být schopen umožnit vyžádání svolení zákazníka, avšak bude na rozhodnutí zákazníka, zda uvedenou doplňkovou službu zakoupí či ne.
10	Zákaznický obsah je zpracováván pouze na území České republiky. Mimo Českou republiku může být zákaznický obsah zpracován pouze se svolením zákazníka (v každém jednotlivém případě) nebo za účelem udržení kontinuity poskytované služby.	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy, ve které závazek zpracovávat zákaznický obsah pouze na území České republiky + odkaz na tu část certifikace ISO 27001/auditní zprávy SOC 2®, ze které bude patrný úplný výčet datacenter a jejich lokace po úroveň katastrálního území/obce ve kterých bude zákaznický obsah zpracováván				X	X	X	X	Povolen export mimo ČR pro zajištění podpory a servisu ze zahraničí.
11	Prodejce a materiální dodavatel umožní Ministerstvu vnitra nebo Národnímu úřadu pro kybernetickou a informační bezpečnost zdarma ve vztahu k dané službě cloud computingu provedení kontroly ve smyslu zákona o kontrole na všech místech, souvisejících s poskytováním služby a zároveň poskytnou veškerou součinnost, kterou si tyto orgány vyžádají.	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy, ve které bude uveden závazek umožnění kontroly regulátorem, nebo závazek dodržet veškeré právní předpisy, které se vztahují k poskytování dané služby	X	X	X	X	X	X	X	

12	Prodejce je schopen zajistit dostupnost služby s provozní dobou 24x7 alespoň v uvedených úrovních vyhodnocované na měsíční bázi včetně časů nutných pro servisní zásahy, měřeno v peeringovém uzlu deklarovaném prodejcem nebo materiálním dodavatelem.	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy, ve které bude prodejce garantovat zajištění dostupnosti alespoň v uvedených úrovních	96,16 (%)	99,45 (%)	99,90 (%)	99,99 (%)				Prodejce musí být schopen služby v této úrovni SLA zajistit, avšak v případě požadavku zákazníka může v dané bezpečnostní úrovni nabízet alternativu služby s nižší nebo vyšší úrovní dostupnosti v SLA.
13	Materiální dodavatel má vyhotoven plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby pro zajištění dostupnosti uvedené v ID 13.	strategie zajištění kontinuity provozu + strategie na obnovu po havárii + odkaz na část certifikace nebo auditní zprávy ISO 27001/ISO 22301/ISO 20000/SOC 2®, která dokládá vyhotovení plánu zajištění kontinuity provozu a plánu na obnovu po havárii		X	X	X	X	X		
14	Materiální dodavatel umožňuje bulk import/export dat“ pro import či export velkých objemů dat prostřednictvím zaslání šifrovaných paměťových médií.	odkaz na konkrétní část podmínek poskytování služby, část návrhu smlouvy, nebo produktovou specifikaci, ze které bude patrné, že materiální dodavatel umožňuje bulk import/export dat“ pro import či export velkých objemů dat prostřednictvím zaslání šifrovaných paměťových médií	X	X	X	X	X	X	X	

15	Materiální dodavatel umožňuje uložení klíčů v certifikovaném hardware security modulu (HSM) úrovně ochrany FIPS 140-2 level 2 a vyšší, FIPS 140-3 level 2 a vyšší nebo certifikaci dle Common Criteria minimálně na EAL4 a vyšší, který je pod vzdálenou správou zákazníka.	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy nebo produktovou specifikaci služby, ze které bude patrné, že materiální dodavatel umožňuje uložení klíčů v HSM modulu úrovně ochrany FIPS 140-2 level 2 a vyšší, FIPS 140-3 level 2 a vyšší nebo certifikaci dle Common Criteria minimálně na EAL4 a vyšší, který je pod správou zákazníka			X	X	X	X	X	HSM modul je uložen v datacentru a je ve vlastnictví materiálního dodavatele. Materiální dodavatel umožní vzdálenou instalaci vlastního klíče. Bude na rozhodnutí zákazníka, zda využije.
16	Materiální dodavatel umožňuje ochranu zákaznického obsahu šifrováním při přenosu a v úložištích v cloudové službě pomocí některého z algoritmů uvedených v doporučení v oblasti kryptografických prostředků vydané NÚKIB, které je zveřejněno na jeho internetových stránkách	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy nebo produktovou specifikaci služby, ze které bude patrný způsob šifrování při přenosu a v úložištích v cloudové službě		X	X	X	X	X	X	
17	Materiální dodavatel zajišťuje ochranu zákaznického obsahu šifrováním na úrovni operačního systému.	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy nebo produktovou specifikaci služby, ze které bude patrné, že materiální dodavatel zajišťuje ochranu zákaznického obsahu šifrováním na úrovni operačního systému	X	X	X	X		X	X	

18	Materiální dodavatel vyhotovuje záznam o přístupu jeho servisních pracovníků do virtuálního prostoru vyhrazeného zákazníkovi, který obsahuje zákaznický obsah. Tento záznam obsahuje jedinečný identifikátor servisního pracovníka materiálního dodavatele, údaj o tom, kdy, z jakého důvodu a na jakou datovou entitu došlo k přístupu. Tento záznam materiální dodavatel umožňuje zpřístupnit zákazníkovi.	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy nebo produktovou specifikaci služby, ze které bude patrné, že materiální dodavatel vyhotovuje záznam o přístupu servisních pracovníků do virtuálního prostoru vyhrazeného zákazníkovi, který obsahuje zákaznický obsah, a zpřístupní tento záznam zákazníkovi.		X	X	X	X	X	X	
19	Materiální dodavatel umožňuje bezpečnou likvidaci kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM) řízenou zákazníkem. Materiální dodavatel umožňuje při ukončení služby bezpečnou likvidaci dat v souladu s vyhláškou o kybernetické bezpečnosti.	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy nebo produktovou specifikaci služby, ze které bude patrné umožnění bezpečné likvidaci kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM) řízenou zákazníkem a závazek umožnit/zajistit při ukončení služby likvidaci vrchního přístupového klíče a popis bezpečné likvidace dat v souladu s vyhláškou o kybernetické bezpečnosti.			X	X	X	X	X	
20	Materiální dodavatel umožňuje synchronní replikaci dat alespoň do jednoho záložního datového centra, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra.	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy nebo produktovou specifikaci, ze které bude patrný způsob zálohování do záložního datového centra			X	X		X	X	
21	Materiální dodavatel zajišťuje alespoň jednoho záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra.	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy nebo produktovou specifikaci, ze které bude patrné zajištění záložního datového centra			X	X	X			

22	Materiální dodavatel zajistí, že primární i záložní datacentrum, ze kterého jsou poskytovány služby, jsou v dostatečné vzdálenosti od relevantních naturogenních a antropogenních zdrojů rizik nebo je přijato adekvátní bezpečnostní opatření.	zpráva nebo jiný doklad o zhodnocení naturogenních či antropogenních zdrojů rizik			X	X	X	X	X	
23	Materiální dodavatel zajistí, že primární a záložní datové centrum se nacházejí v rozdílných distribučních oblastech elektřiny a ve vzdálenosti alespoň 10km od sebe navzájem.	odkaz na tu část certifikace ISO 27001/auditní zprávy SOC 2®, ze které bude patrný úplný výčet datacenter a jejich lokace po úroveň katastrálního území/obce ve kterých bude zákaznický obsah trvale uložen.			X	X	X	X	X	
24	Materiální dodavatel zajistí, že primární i záložní datové centrum se nacházejí buďto obě v České republice nebo ve dvou různých státech EU (EHS).	odkaz na tu část certifikace ISO 27001/auditní zprávy SOC 2®, ze které bude patrný úplný výčet datacenter a jejich lokace po úroveň katastrálního území/obce ve kterých bude zákaznický obsah trvale uložen.			X	X	X	X	X	
25	Materiální dodavatel je držitelem certifikace ČSN EN ISO/IEC 27001 nebo ISO/IEC 27001 do jehož certifikovaného rozsahu náleží posuzovaná služba cloud computingu	Certifikát ČSN EN ISO/IEC 27001 nebo ISO/IEC 27001 a příslušné auditní zprávy od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů IAF, který podepsal MLA	X	X	X	X	X	X	X	Materiální dodavatel dodá každých 15 měsíců do evidence v katalogu nabídek cloud computingu Ministerstva vnitra platný certifikát, a dále auditní zprávu ne starší jak 3 měsíců. (https://www.iaf.nu//articles/IAF_MLA/14)

26	Materiální dodavatel je držitelem certifikace ČSN ISO/IEC 27001 nebo ISO/IEC 27001 jehož rozsah zahrnuje identifikace normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017 pro posuzovanou službu cloud computingu	Certifikát ČSN EN ISO/IEC 27001 nebo ISO/IEC 27001 jehož rozsah zahrnuje identifikaci normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017 a příslušné auditní zprávy od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů IAF, který podepsal MLA		X	X	X	X	X	X	Materiální dodavatel dodá každých 15 měsíců do evidence v katalogu nabídek cloud computingu Ministerstva vnitra platný certifikát, a dále auditní zprávu ne starší jak 3 měsíců. (https://www.iaf.nu//articles/IAF_MLA/14)
27	Materiální dodavatel je držitelem certifikace ČSN ISO/IEC 27001 nebo ISO/IEC 27001 jehož rozsah zahrnuje identifikaci normy ČSN ISO/IEC 27018 nebo ISO/IEC 27018 pro posuzovanou službu cloud computingu	Certifikát ČSN EN ISO/IEC 27001 nebo ISO/IEC 27001 jehož rozsah zahrnuje identifikaci normy ČSN ISO/IEC 27018 nebo ISO/IEC 27018 a příslušné auditní zprávy od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů IAF, který podepsal MLA		X	X	X	X	X	X	Materiální dodavatel dodá každých 15 měsíců do evidence v katalogu nabídek cloud computingu Ministerstva vnitra platný certifikát, a dále auditní zprávu ne starší jak 3 měsíců. (https://www.iaf.nu//articles/IAF_MLA/14)

28	Materiální dodavatel má zaveden systém sledování a vyhodnocování bezpečnostních událostí (např. SIEM) a umožní zpřístupnění vzdáleně všech událostí tykajících se konkrétního zákazníka, zákazníkovi, bez zbytečného prodlení po vzniku události.	odkaz na konkrétní část podmínek poskytování služby, část návrhu smlouvy nebo jiný popis služby, ze které bude patrné zavedení systému sledování a vyhodnocování bezpečnostních událostí a závazek materiálního dodavatele zpřístupnění prioritních událostí zákazníkovi	X	X	X	X	X	X	X	Volba priorit je na zákazníkovi, následně si zákazník ve smlouvě s materiálním dodavatelem vyjasní, o které události mu jde.
29	Materiální dodavatel informuje zákazníka v případě narušení bezpečnosti informací zákaznických dat a provozních údajů.	odkaz na konkrétní část podmínek poskytování služby, část návrhu smlouvy nebo jiný popis služby, ze které bude patrné, že materiální dodavatel informuje zákazníka v případě narušení bezpečnosti informací zákaznických dat	X	X	X	X	X	X	X	
30	Materiální dodavatel informuje zákazníka o žádosti cizích státních orgánů o zpřístupnění nebo předání zákaznických dat a provozních údajů, ledaže příslušný právní základ, na kterém je státní orgán zřízen nebo na kterém stojí žádost o vyšetřování, to zakazuje. V takovém případě materiální dodavatel zákazníka informuje poté, co vyprší platnost právního zákazu, např. po vypršení období mlčenlivosti nařízeného zákonem nebo soudem.	odkaz na konkrétní část podmínek poskytování služby, část návrhu smlouvy nebo jiný popis služby, ze které bude patrné, že materiální dodavatel informuje zákazníka v případě žádosti cizích státních orgánů o zpřístupnění nebo předání zákaznických dat a provozních údajů, ledaže příslušný právní základ, na kterém je státní orgán zřízen nebo na kterém stojí žádost o vyšetřování, to zakazuje	X	X	X	X	X	X	X	

31	Materiální dodavatel žádost státního orgánu třetí země (stát mimo členský stát EU/EHP) uzná a zákaznická data a provozní údaje poskytne nebo zpřístupní, pouze pokud žádost vychází z mezinárodní dohody, například úmluvy o vzájemné právní pomoci, která je v platnosti mezi třetí zemí a EU nebo členským státem EU (viz čl. 48 GDPR). Výjimky pro specifické situace dle č. 49 GDPR tímto nejsou dotčeny.	odkaz na konkrétní část podmínek poskytování služby, část návrhu smlouvy nebo jiný popis služby, ze které bude patrné, že materiální dodavatel žádost státního orgánu třetí země (stát mimo členský stát EU/EHP) uzná a zákaznická data a provozní údaje poskytne nebo zpřístupní, pouze pokud žádost vychází z mezinárodní dohody, například úmluvy o vzájemné právní pomoci, která je v platnosti mezi třetí zemí a EU nebo členským státem EU	X	X	X	X	X	X	X	
32	Materiální dodavatel neumožní předání zákaznických dat a provozních údajů z EU do třetí země za účelem poskytnutí nebo zpřístupnění zákaznických dat a provozních údajů státním orgánům třetí země na základě jejich žádosti o zpřístupnění nebo předání zákaznických dat a provozních údajů. Výjimky pro specifické situace dle č. 49 GDPR tímto nejsou dotčeny.	odkaz na konkrétní část podmínek poskytování služby, část návrhu smlouvy nebo jiný popis služby, ze které bude patrné, že materiální dodavatel neumožní předání zákaznických dat a provozních údajů z EU do třetí země za účelem poskytnutí nebo zpřístupnění zákaznických dat a provozních údajů státním orgánům třetí země na základě jejich žádosti o zpřístupnění nebo předání zákaznických dat a provozních údajů		X	X	X	X	X	X	Směřuje proti tomu, aby státní orgány třetí země nezneužívaly na jejich území usazené mateřské nebo dceřiné společnosti, nebo pobočky a prostřednictvím nich neobcházely ustanovení mezinárodních dohod.

33	Materiální dodavatel zpřístupní nebo předá zákaznická data nebo provozní údaje cizímu státnímu orgánu na základě jeho žádosti o zpřístupnění nebo předání dat, pouze po svém předchozím právním posouzení, ze kterého bude vyplývat, že žádost cizího státního orgánu má proveditelný a platný právní základ a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a provozních údajů je přiměřený účelu žádosti. O provedeném posouzení materiální dodavatel provede záznam, který uchová alespoň 10 let pro účely kontroly.	odkaz na konkrétní část podmínek poskytování služby, část návrhu smlouvy nebo jiný popis služby, ze které bude patrné, že materiální dodavatel zpřístupní nebo předá zákaznická data nebo provozní údaje cizímu státnímu orgánu na základě jeho žádosti o zpřístupnění nebo předání dat, pouze po svém předchozím právním posouzení, ze kterého bude vyplývat, že žádost cizího státního orgánu má proveditelný a platný právní základ a rozsah poskytovaných zákaznických dat a provozních údajů je přiměřený účelu žádosti.	X	X	X	X	X	X	X	
34	Materiální dodavatel je schopen poskytovat nástroje nebo služby pro zvýšení odolnosti vůči útokům typu DoS/DDoS	odkaz na konkrétní část podmínek poskytování služby nebo na popis volitelné služby, ze které bude patrný nástroj nebo služba využívaná pro zvýšení odolnosti vůči útokům typu DoS/DDos		X	X	X	X	X	X	Vyjadřuje schopnost materiálního dodavatele, následně si zákazník ve smlouvě s materiálním dodavatelem vyjasní, zda o tyto nástroje stojí.

35	Materiální dodavatel realizoval alespoň tři zakázky v oblasti poskytování služeb IaaS a PaaS, kdy souhrnná fakturace za služby IaaS nebo PaaS činila alespoň 300 000 Kč za každou zakázku po dobu dvanácti měsíců v uplynulých 5 letech nebo tři zakázky v oblasti poskytování ICT služeb nad infrastrukturou zákazníka, nebo vlastní infrastrukturou poskytovanou jako služba zákazníkovi, kde platba za poskytované ICT služby je u každé zakázky alespoň 1 000 000 Kč ročně. Předmětné ICT služby musí zahrnovat služby podpory s uvedením SLA.	Potvrzení od poskytovatelova zákazníka o řádném plnění předmětné smlouvy		X	X		X	X		
36	Materiální dodavatel má v době podání žádosti o zápis do katalogu cloud computingu pro nabízenou službu cloud computingu alespoň 2 zákazníky v aktivním provozu.	Potvrzení od poskytovatelova zákazníka o řádném plnění předmětné smlouvy		X	X				X	
37	Materiální dodavatel poskytuje podporu služby alespoň v pracovní dny 7:00-19:00.	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy, ze které bude patrné, že materiální dodavatel poskytuje podporu služby alespoň v pracovní dny 7:00-19:00	X				X	X	X	
38	Materiální dodavatel umožňuje podporu služby 7x24.	odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy nebo produktovou, ze které bude patrné, že materiální dodavatel umožňuje podporu služby 7x24		X	X	X	X	X	X	

39	Materiální dodavatel provádí penetrační testy.	Zpráva z provedení penetračního testu, nesmí být starší než 36 měsíců před podáním žádosti o zápis do katalogu.	X	X			X	X	X	"Materiální dodavatel dodá každých 36 měsíců evidence v katalogu nabídek cloud computingu zprávu ne starší jak 35 měsíců Ministerstvu vnitra. (https://www.iaf.nu//articles/IAF_MLA/14)"
40	Materiální dodavatel provádí penetrační testy.	Zpráva z provedení penetračního testu provedeného dle standardu NIST 800-115 nebo v souladu s metodikou OSSTMM. Penetrační test provede subjekt, který je nezávislý na materiálním dodavateli cloud computingu. Zpráva z provedení penetračního testu, nesmí být starší než 36 měsíců před podáním žádosti o zápis do katalogu. Služba cloud computingu zapisovaná do katalogu musí být zahrnuta do rozsahu penetračního testu.			X	X	X	X		NIST: https://csrc.nist.gov/publications/detail/sp/800-115/final OSSTMM: https://www.isecom.org/OSSTMM.3.pdf https://www.isecom.org/research.html#content5-9d
41	Materiální dodavatel provádí penetrační testy.	Zpráva z provedení penetračního testu, při kterém budou ověřena rizika alespoň dle standardu OWASP Top 10 Web Application Security Risks. Penetrační test provede subjekt, který je nezávislý na materiálním dodavateli cloud computingu. Zpráva z provedení penetračního testu, nesmí být starší než 36 měsíců před podáním žádosti o zápis do katalogu. Služba cloud computingu			X	X			X	OWASP Top ten web application security risks: https://owasp.org/www-project-top-ten/

		zapisovaná do katalogu musí být zahrnuta do rozsahu penetračního testu.								

Příloha ke vstupním kritériím – ID 3

Trestné činy, při jejichž spáchání představují prostředky informačních a komunikačních technologií předmět ochrany a trestné činy, při jejichž páchání jsou prostředky informačních a komunikačních technologií užity ke spáchání trestného činu a další trestné činy, zejména proti České republice, cizímu státu a mezinárodní organizaci.

- § 180 neoprávněné nakládání s osobními údaji
- § 181 poškození cizích práv
- § 182 porušení tajemství dopravovaných zpráv
- § 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí
- § 184 pomluva
- § 191 šíření pornografie
- § 192 výroba a jiné nakládání s dětskou pornografií
- § 193 zneužití dítěte k výrobě pornografie
- § 193b navazování nedovolených kontaktů s dítětem
- § 205 krádež
- § 206 neoprávněné užívání cizí věci
- § 209 podvod
- § 213 provozování nepoctivých her a sázek
- § 214 podílnictví
- § 216 legalizace výnosů z trestné činnosti
- § 228 poškození cizí věci
- § 230 neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
- § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku
- § 236 výroba a držení padělatelského náčiní
- § 264 zkreslení údajů a nevedení podkladů ohledně vývozu zboží a technologií dvojího užití
- § 268 porušení práv k ochranné známce a jiným označením

- § 267 zkreslení údajů a nevedení podkladů ohledně zahraničního obchodu s vojenským materiálem
- § 269 porušení chráněných průmyslových práv
- § 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi
- § 272 obecné ohrožení
- § 276 poškození a ohrožení provozu obecně prospěšného zařízení
- § 287 šíření toxikomanie
- § 290 získání kontroly nad vzdušným dopravním prostředkem, civilním plavidlem a pevnou plošinou
- § 291 ohrožení bezpečnosti vzdušného dopravního prostředku a civilního plavidla
- § 309 vlastizrada
- § 310 rozvracení republiky
- § 311 teroristický útok
- § 312 teror
- § 312a účast na teroristické skupině
- § 312d financování terorismu
- § 312e podpora a propagace terorismu
- § 314 sabotáž
- § 316 vyzvědačství
- § 317 ohrožení utajované informace
- § 331 přijetí úplatku
- § 332 podplacení
- § 333 nepřímé úplatkářství
- § 345 křivé obvinění
- § 348 padělání a pozměnění veřejné listiny
- § 353 nebezpečné vyhrožování
- § 354 nebezpečné pronásledování
- § 355 hanobení národa, rasy, etnické nebo jiné skupiny osob
- § 356 podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod
- § 357 šíření poplašné zprávy
- § 361 účast na organizované zločinecké skupině
- § 364 podněcování k trestnému činu
- § 365 schvalování trestného činu
- § 400 genocidum
- § 401 útok proti lidskosti
- § 402 apartheid a diskriminace skupiny lidí
- § 403 založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka
- § 404 projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka
- § 405 popírání, zpochybňování, schvalování a ospravedlňování genocidia
- § 405a agrese
- § 406 příprava útočné války
- § 407 podněcování útočné války

5 Bezpečnostní pravidla

Záměrem této části není vytvořit duplicitu k vyhlášce o kybernetické bezpečnosti a stanovovat pravidla upravující informační bezpečnost uvnitř organizace zákazníka (např. vytváření systému informační bezpečnosti, klasifikace aktiv a hodnocení rizik, konkrétní technická opatření). Lze předpokládat, že zákazník podstatnou část z níže uvedených pravidel zahrne do smluvních ujednání mezi ním a poskytovatelem ve fázi výběru konkrétního poskytovatele cloudových služeb.

Obsah této části podstatně vychází z obsahu standardů zabývajících se bezpečností cloudových služeb, zejména z:

- C5:2020 od BSI (dále jen C5 a označení příslušného ID z tohoto standardu), dostupné z:

  https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/C5_NewRelease/C5_NewRelease_node.html;jsessionid=D78FD1A74D29B6D4100E89511243C0EB.1_cid500

- Úřední sdělení České národní banky ze dne 19. srpna 2016 k výkonu činnosti na finančním trhu – cloud computing (dále ČNB Cloudy), dostupné z:

  https://www.cnb.cz/export/sites/cnb/cs/legislativa/.galleries/Vestnik-CNB/2016/vestnik_2016_08_20816560.pdf

- Obecné pokyny k outsourcingu u poskytovatelů cloudových služeb, vydané Evropskou pojišťovací asociací (dále EIOPA), dostupné i v češtině z:

  https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en

- ISO/IEC 27017:2015 Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002

Tabulka č. 2 Bezpečnostní pravidla

ID BP	Stručný popis	Bezpečnostní pravidlo	Označení standardu	Bezpečnostní úroveň				Distribuční model			Komentář NÚKIB
				1	2	3	4	IaaS	PaaS	SaaS	
1		**Obecné podmínky pro cloudové služby**									
1.1	Informace o soudní příslušnosti	Zákazník zajistí, že mu materiální dodavatel nebo prodejce poskytne v popisu systému cloudové služby a smluvních ujednáních jasnou a srozumitelnou informaci o právu země, kterým se řídí smlouva a příslušnosti soudů, které rozhodují případné spory ze smlouvy. Je-li to možné je takovým právem právo České republiky a soudy České republiky.	C5 BC-01		X	X	X	X	X	X	
1.2	Informace o poloze zpracování dat	Zákazník zajistí, že mu materiální dodavatel nebo prodejce poskytne v popisu systému a smluvních ujednáních jasnou a srozumitelnou informaci o poloze systémových komponent, včetně těch zajišťovaných systematickými zpracovateli, ve kterých jsou nebo mohou být zákaznická data a provozní údaje zpracovávány, ukládány a zálohovány. Zákazník musí být schopen určit polohu zpracování a ukládání zákaznických dat a provozních údajů včetně záloh zákaznických dat a provozních údajů podle smluvně dostupných možností. Zákazník dále zajistí, že u zákaznických dat a provozních údajů zpracovávaných mimo území členského státu EU/EHP poskytne materiální dodavatel popis toho, jak bude chráněn ve smyslu čl. 45, 46 a 47 GDPR.	C5 BC-01		X	X	X	X	X	X	

1.3	Informace o zpracování dat mimo EU/EHP	Zákazník zajistí, že mu materiální dodavatel nebo prodejce poskytne jasnou, srozumitelnou a průběžně aktualizovanou informaci o důvodech, pro něž obvykle dochází nebo může docházet při využívání cloudové služby ke zpracování zákaznického obsahu mimo území členského státu EU/EHP, průměrnou dobu po kterou je nebo může být zákaznický obsah obvykle zpracováván mimo území členského státu EU/EHP a obvyklý rozsah zákaznického obsahu, který je nebo může být zpracováván mimo území členského státu EU/EHP.			X	X	X	X	X	X	
1.4	Trvalé uložení dat v EU/EHP	Zákazník zajistí, že zákaznická data a provozní údaje jsou trvale a nepřetržitě uloženy výlučně na území členských států EU/EHP.			X	X	X	X	X	X	Uvedené ustanovení nevylučuje uložení i na území mimo členské státy EU/EHP.
1.5	Omezení zpracování dat mimo EU/EHP	Zákazník zajistí, že zákaznická data a provozní údaje jsou zpracovávány na území členských států EU (EHP). Aniž je dotčeno pravidlo ID 1.4, v odůvodněných případech, po nezbytně nutnou dobu, v nezbytném rozsahu mohou být zákaznická data a provozní údaje zpracovávány i na území jiných států, které zajišťují odpovídající úroveň ochrany ve smyslu čl. 45 GDPR, nebo jinde pokud materiální dodavatel poskytl vhodné záruky ve smyslu čl. 46, 47 GDPR. Výjimky pro specifické situace dle čl. 49 GDPR nejsou dotčeny.			X	X	X	X	X	X	

1.6	Informace o dostupnosti během běžného provozu	Zákazník zajistí, že ve smlouvě s prodejcem a materiálním dodavatelem je srozumitelně, jasně a závazně uvedena informace o dostupnosti cloudové služby a právní následky při nedodržení uvedené dostupnosti. Pokud informace o dostupnosti vyjadřuje průměrné hodnoty, které nejsou závazné v jednotlivých případech, je nutné to jednoznačně uvést.	C5 BC-02	X	X	X	X	X	X	X	Standardním místem měření dostupnosti služby je perimetr datacentra, ze kterého je služba poskytována. Uvedené nebrání dohodě o mezi zákazníkem a materiálním dodavatelem nebo prodejcem.
1.7	Informace o zvládání provozních incidentů během běžného provozu	Zákazník zajistí, že ve smlouvě s prodejcem a materiálním dodavatelem je srozumitelně, jasně a závazně uvedena informace o kategoriích a prioritách provozních incidentů, cílový čas odezvy na provozní incident dle jednotlivých kategorií provozních incidentů (čas mezi oznámením provozního incidentu a zahájením jeho řešení prodejcem a materiálním dodavatelem), cílový čas vyřešení (čas do vyřešení provozního incidentu) a právní následky při nedodržení uvedeného cílového času odezvy a cílového času vyřešení. Pokud informace o cílovém času vyřešení provozního incidentu vyjadřují průměrné hodnoty, které nejsou závazné v jednotlivých případech, je nutné to jednoznačně uvést.	C5 BC-02		X	X	X	X	X	X	
1.8	Informace o údajích obnovy v případě nouzového provozu	Zákazník zajistí, že mu materiální dodavatel nebo prodejce sdělí na žádost jasně a srozumitelně ve vztahu k dané službě maximálně přípustný čas výpadku (RTO), maximálně tolerovatelné období ztráty dat (RPO), nezbytný čas pro spuštění nouzového provozu, nouzovou kapacitu ve vztahu k	C5 BC-03		X	X	X	X	X	X	

		běžnému provozu, čas obnovy do běžného provozu.									
1.9		Zákazník ověří, zda maximálně přípustný čas výpadku a maximálně tolerovatelné období ztráty dat na straně materiálního dodavatele odpovídá jeho vlastním požadavkům na vytváření záloh.	ISO 27017 12.3.1		X	X	X	X	X	X	
1.10	Informace o dostupnosti datového centra	Zákazník zajistí, že mu materiální dodavatel nebo prodejce v případě potřeby sdělí jasnou a srozumitelnou informaci o dostupnosti datacentra, včetně datacenter systematických zpracovatelů, ze kterého je služba poskytována. Dostupnost a čas výpadku nebo odstávky jsou uváděny za rok podle klasifikačních schémat průmyslových standardů.	C5 BC-04			X	X	X	X	X	
1.11	Informace o certifikátech a osvědčeních	Zákazník zajistí, že materiální dodavatel disponuje certifikátem ČSN EN ISO/IEC 27001 nebo ISO/IEC 27001 do jehož certifikovaného rozsahu náleží poskytovaná cloudová služba od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů IAF, který podepsal MLA.	C5 BC-06	X	X	X	X	X	X	X	
1.12		Zákazník zajistí, že materiální dodavatel disponuje certifikátem ČSN EN ISO/IEC 27001 nebo ISO/IEC 27001 do jehož certifikovaného rozsahu náleží poskytovaná cloudová služba jehož rozsah zahrnuje identifikaci normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017 a příslušné auditní zprávy od certifikačního orgánu, který byl akreditován			X	X	X	X	X	X	

		pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů IAF, který podepsal MLA									
1.1		Zákazník zajistí, že materiální dodavatel disponuje certifikátem ČSN EN ISO/IEC 27001 nebo ISO/IEC 27001 do jehož certifikovaného rozsahu náleží poskytovaná cloudová služba jehož rozsah zahrnuje identifikaci normy ČSN ISO/IEC 27018 nebo ISO/IEC 27018 a příslušné auditní zprávy od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů IAF, který podepsal MLA			X	X	X	X	X	X	
1.2	Dokládání ISO	Zákazník zajistí, že mu materiální dodavatel předloží aktuální certifikát ISO/IEC 27001 každých 15 kalendářních měsíců. Poskytovaná cloudová služba musí být uvedena v certifikovaném rozsahu na certifikátu vydaném certifikačním orgánem, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů IAF, který podepsal MLA.		X	X	X	X	X	X	X	

1.3		Zákazník zajistí, že mu materiální dodavatel předloží aktuální certifikát ISO/IEC 27001 do jehož certifikovaného rozsahu náleží poskytovaná cloudová služba jehož rozsah zahrnuje identifikaci normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017 a ČSN ISO/IEC 27018 nebo ISO/IEC 27018 každých 15 kalendářních měsíců. Poskytovaná cloudová služba musí být uvedena v certifikovaném rozsahu na certifikátu vydaném certifikačním orgánem, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů IAF, který podepsal MLA.			X	X	X	X	X	X	
1.4	Informace o plánovaných odstávkách	Zákazník zajistí, že ho materiální dodavatel bude s dostatečným předstihem informovat o plánovaných odstávkách poskytované cloudové služby.			X	X	X	X	X	X	
1.5	Jednostranné ukončení smlouvy	Zákazník zajistí, že smluvní ustanovení mu umožňují jednostranně ukončit smlouvu.	ČNB Cloudy, str. 4 přílohy		X	X	X	X	X	X	
1.6	Vlastnictví zákaznického obsahu	Zákazník zajistí, že neztratí vlastnická práva, která mu náleží, k zákaznickému obsahu, který vloží do cloudové služby.		X	X	X	X	X	X	X	
1.7	Vlastnictví softwaru	Zákazník zajistí, že je jednoznačně určeno vlastnictví programového kódu a programových licencí spojených s využíváním cloudové služby.	ISO27017 8.1.2	X	X	X	X	X	X	X	
1.8	Informace o změně vlastníka	Zákazník zajistí, že ho materiální dodavatel bude informovat o změně skutečného majitele, dle zákona upravujícího legalizaci výnosů z trestné činnosti a financování terorismu, tohoto materiálního dodavatele nebo o změně kontroly nad zásadními systémovými komponenty, dle klasifikace systémových komponent provedené dle	příloha 7, písm. i), bod 3 VKB			X	X	X	X	X	§ 4 odst. 4, zákon č. 253/2008 Sb.,

		ustanovení ID 5.2, využívanými tímto materiálním dodavatelem k poskytování cloudové služby.									
1.9	Právo odstoupit při změně vlastníka	Zákazník zajistí, že bude mít právo jednostranně odstoupit od smlouvy v případě změny skutečného majitele materiálního dodavatele nebo změny kontroly nad zásadními aktivy využívanými materiálním dodavatel k poskytování cloudové služby.				X	X	X	X	X	
2		**Organizace informační bezpečnosti (OIS)**									
2.1	ISMS, SoA	Zákazník zajistí, že materiální dodavatel dodržuje systém řízení bezpečnosti informací. Rozsah systému řízení bezpečnosti informací musí zahrnovat organizační jednotky materiálního dodavatele, lokality a procesy k poskytování služby. Opatření jsou dokumentována pro řízení, implementaci, údržbu a neustálé zlepšování cloudových služeb. Dokumentace obsahuje rozsah systému řízení, prohlášení o aplikovatelnosti (SoA) ve kterém jsou doložena, jaká bezpečnostní opatření byla vybrána pro potlačení bezpečnostních rizik a výsledky posledního interního či certifikačního auditu materiálního dodavatele.	C5 OIS-01	X	X	X	X	X	X	X	

2.2	Bezpečnostní politiky	Zákazník zajistí, že jeho vrcholové vedení akceptuje bezpečnostní politiky materiálního dodavatele, který je bude komunikovat interním a externím zaměstnancům a svým dodavatelům. Materiální dodavatel zavede na základě těchto bezpečnostních politik přiměřená bezpečnostní opatření. Politiky popisují význam bezpečnosti informací, bezpečnostní cíle, požadovanou bezpečnostní úroveň, nejvýznamnější aspekty bezpečnostní strategie k dosažení stanovených cílů a organizační strukturu materiálního dodavatele v rozsahu systému řízení bezpečnosti informací.	C5 OIS-02	X	X	X	X	X	X	X	
2.3	Vazby mezi činností MD a činností třetích stran	Zákazník zajistí, že vazby a závislosti mezi činností poskytování služby ze strany materiálního dodavatele a činností třetích stran jsou komunikovány a dokumentovány. To zahrnuje řešení zranitelností, kybernetických bezpečnostních incidentů a nesprávného fungování nasmlouvaných služeb.	C5 OIS-03		X	X	X	X	X	X	

2.4	Rozdělení úkolů a odpovědností	Zákazník zajistí, že rozdílné úkoly a odpovědnosti jsou rozděleny na základě posouzení rizik tak, aby se předešlo neautorizované a nechtěné změně nebo zneužití zpracovávaných, ukládaných a přenášených zákaznických dat v rámci poskytování cloudové služby. Posouzení rizik zahrnuje následující oblasti, pokud se vztahují na poskytování cloudové služby a spadají do oblasti odpovědnosti materiálního dodavatele cloudové služby: a) správa profilů, b) schvalování a přidělování přístupových oprávnění, c) vývoj, testování změn a provoz systémových komponent. Pokud rozdělení odpovědnosti a úkolů není možné z organizačních nebo technických důvodů, je nutné uplatnit opatření k monitorování aktivit, tak aby byly detekovány neautorizované a nechtěné změny a zneužití a následně přijaty odpovídají reakce.	C5 OIS-04		X	X	X	X	X	X	
2.5	Informovanost o hrozbách a zranitelnostech	Zákazník zajistí, že materiální dodavatel cloudových služeb využívá informace poskytované příslušnými úřady a zájmovými skupinami tak, aby byl informován o aktuálních hrozbách a zranitelnostech.	C5 OIS-05		X	X	X	X	X	X	

2.6	Zásady, pokyny a postupy pro řízení rizik	Zákazník zajistí, že materiální dodavatel má zásady, pokyny a postupy pro řízení rizik, které jsou dokumentovány, sdělovány a poskytovány v těchto oblastech: a) identifikace rizik spojených se ztrátou důvěrnosti, integrity a dostupnosti informací v rámci ISMS a přiřazení osob odpovědných za konkrétní rizika, b) analýza rizik a pravděpodobnost výskytu rizika, c) vyhodnocení analýzy rizik na základě definovaných kritérií pro akceptování rizik a stanovení priorit jejich mitigace, d) řešení rizik prostřednictvím opatření, včetně schválení autorizace a přijetí zbytkových rizik ze strany osob odpovědných za rizika, e) dokumentace realizovaných činností, které umožňují konzistentní, platné a srovnatelné výsledky.	C5 OIS-06		X	X	X	X	X	X	
2.7	Provedení hodnocení rizik	Zákazník zajistí, že materiální dodavatel provádí proces hodnocení rizik podle potřeby, minimálně však jednou ročně. Při určování rizik se berou v úvahu následující aspekty, pokud se vztahují na poskytovanou cloudovou službu a jsou v oblasti odpovědnosti materiálního dodavatele cloudových služeb: a) zpracování, ukládání nebo přenos dat cloudových zákazníků při různých bezpečnostních úrovních, b) výskyt slabých míst a chyb v technických ochranných opatřeních pro oddělení sdílených zdrojů, c) útoky prostřednictvím přístupových bodů, včetně rozhraní přístupných z veřejných sítí, d) konfliktní úkoly a oblasti odpovědnosti,	C5 OIS-07		X	X	X	X	X	X	

		které nelze oddělit z organizačních nebo technických důvodů, e) závislosti na podpůrných organizacích.									
3		**Bezpečnostní politiky a pokyny (SP)**									
3.1	Dokumentace a komunikace politik	Zákazník zajistí, že politiky a pokyny jsou v souladu s politikou bezpečnosti informací, jsou dokumentovány v jednotné struktuře a jsou komunikovány interním a externím zaměstnancům materiálního dodavatele. Politiky a pokyny jsou verzovány a schvalovány vrcholným vedením materiálního dodavatele, případně jiným oprávněným a určeným orgánem. Politiky a pokyny by měly obsahovat alespoň následující aspekty: a) cíle, b) rozsah, c) role a jejich odpovědnosti, včetně požadovaných kvalifikací a pravidel zastupitelnosti, d) role a závislosti na dalších organizacích (zejména cloudových zákazníků a subdodavatelů), e) kroky ke zpracování bezpečnostní	C5 SP-01	X	X	X	X	X	X	X	

		strategie, f) příslušné právní a regulatorní požadavky.									
3.2	Přezkoumání politik	Zákazník zajistí, že politiky a pokyny bezpečnosti informací jsou přezkoumávány alespoň jednou ročně kvalifikovanými experty materiálního dodavatele. Tento přezkum bude obsahovat alespoň: a) organizační a technické změny v procedurách poskytování cloudových služeb, b) změny v právních a regulatorních požadavcích v prostředí materiálního dodavatele. Změny těchto politiky a pokynů musí být schváleny před jejich uvedením v platnost	C5 SP-02		X	X	X	X	X	X	
3.3	Výjimky z politik	Zákazník zajistí, že výjimky z politik a pokynů bezpečnosti informací i příslušných kontrol, projdou procesem řízení rizik, včetně schválení těchto výjimek a přijetí souvisejících rizik osobami za tyto rizika odpovědnými. Tyto schválení jsou dokumentována, časově omezena a jsou	C5 SP-03		X	X	X	X	X	X	

		přezkoumávána alespoň jednou ročně osobami odpovědnými za tyto rizika.									
4		**Personál (HR)**									
4.1	Ověření kvalifikace a důvěryhodnosti	Zákazník zajistí, že materiální dodavatel u svých interních a externích zaměstnanců, kteří přistupují k zákaznickým datům nebo k provozním údajům, před uzavřením zaměstnaneckého poměru (nebo ekvivalentu tohoto poměru): a) ověřuje osobní identitu dle občanského průkazu (nebo ekvivalentu), b) ověřuje CV zaměstnance, c) ověřuje dosažené vzdělání a akademické tituly zaměstnance, e) vyžaduje výpis z rejstříku trestů (nebo ekvivalent).	C5 HR-01	X	X	X	X	X	X	X	
4.2		Zákazník zajistí, že administrátoři a klíčoví interní a externí zaměstnanci materiálního dodavatele, kteří budou mít povahou své činnosti nutný přístup k zákaznickým datům nebo k provozním údajům, bude mít udělenou bezpečnostní prověrku minimálně na stupeň "D", důvěrné.					X	X	X	X	
4.3	Pravidla a podmínky zaměstnávání	Zákazník zajistí, že materiální dodavatel u svých interních a externích zaměstnanců vyžaduje soulad s aplikovatelnými bezpečnostními politikami týkajícími se bezpečnosti informací. Tento soulad musí být součástí podmínek zaměstnaneckého poměru (nebo jeho ekvivalentu).	C5 HR-02	X	X	X	X	X	X	X	

4.4		Zákazník zajistí, že materiální dodavatel prokazatelně seznámil své interní a externí zaměstnance s bezpečnostními politikami týkajícími se bezpečnosti informací a pokyny z nich vyplývajícími před tím, než je jim svěřen přístup k zákaznickým datům, zákaznickému nebo k provozním údajům nebo k systémovým komponentům, které materiální dodavatel využívá k poskytování cloudových služeb v produkčním prostředí.		X	X	X	X	X	X	X	
4.5	Bezpečnostní školení a program zvyšování bezpečnostního povědomí	Zákazník zajistí, že materiální dodavatel má zpracovaný školící program týkající se bezpečnosti a zvyšování bezpečnostního povědomí, pravidelně jej aktualizuje na základě změn v bezpečnostních politikách a informací o aktuálních hrozbách; tímto školícím programem pravidelně prochází všichni interní i externí zaměstnanci poskytovatele.	C5 HR-03	X	X	X	X	X	X	X	
4.6		Zákazník zajistí, že materiální dodavatel v pravidelných intervalech aktualizuje školící program s ohledem na změny v politikách, pokynech a současných poznatcích o hrozbách a tento program pokrývá minimálně následující aspekty: a) zacházení se systémovými komponenty používanými k poskytování služeb cloud computingu v produkčním prostředí v souladu s aplikovatelnými politikami a procedurami, b) zacházení se zákaznickými daty nebo s provozními údaji v souladu s aplikovatelnými politikami a pokyny, a v souladu s požadavky právního prostředí a regulátora, c) informace o současných hrozbách a	C5 HR-03	X	X	X	X	X	X	X	

		d) zásady správného chování v případě bezpečnostního incidentu.									
4.7	Disciplinární opatření	Zákazník zajistí, že materiální dodavatel v případě porušení politik, pokynů a aplikovatelných právních a regulatorních požadavků bude postupovat v souladu s definovanou politikou, která musí zahrnovat následující aspekty: a) ověření, zda k porušení došlo a b) zvážení povahy a závažnosti porušení a jeho dopadů.	C5 HR-04	X	X	X	X	X	X	X	
4.8	Odpovědnosti v případě změny či ukončení zaměstnaneckého vztahu	Zákazník zajistí, že materiální dodavatel prokazatelně informuje interní a externí zaměstnance o tom, které povinnosti vyplývající z politik a pokynů vztahujících se k informační bezpečnosti, jim přetrvávají v případě změny či ukončení zaměstnaneckého vztahu a po jak dlouhou dobu.	C5 HR-05	X	X	X	X	X	X	X	

4.9	Dohody o důvěrnosti	Zákazník zajistí, že materiální dodavatel uzavře s interními a externími zaměstnanci, dodavateli a externími poskytovateli služeb dohody o mlčenlivosti a důvěrnosti na základě požadavků identifikovaných materiálním dodavatelem za účelem ochrany dat, informací a poskytovaných služeb.	C5 HR-06	X	X	X	X	X	X	X	
4.10		Zákazník zajistí, že materiální dodavatel nechá tyto dohody akceptovat dodavateli a externími poskytovateli služeb v okamžiku uzavření smlouvy a v případě interních a externích zaměstnanců před tím, než jim bude udělen přístup k datům zákazníka.	C5 HR-06	X	X	X	X	X	X	X	
4.11		Zákazník zajistí, že materiální dodavatel má zdokumentované požadavky identifikované za účelem ochrany dat, informací a poskytovaných služeb a nejméně jednou ročně je reviduje; v případě, že revize ukáží nutnost požadavky aktualizovat, je nutné aktualizovat dohody o mlčenlivosti a důvěrnosti.	C5 HR-06	X	X	X	X	X	X	X	
4.12		Zákazník zajistí, že poskytovatel informuje interní zaměstnance, externí zaměstnance, dodavatele a externí poskytovatele služeb a získá potvrzení o souhlasu s aktualizovanými dohodami o mlčenlivosti a důvěrnosti.	C5 HR-06	X	X	X	X	X	X	X	

5		**Řízení systémových komponent (AM)**									
5.1	Seznam systémových komponent	Zákazník zajistí, že materiální dodavatel zavede postupy pro inventarizaci systémových komponent. Seznam je prováděn automaticky nebo určenými osobami nebo týmy, kteří jsou odpovědní za úplnost, přesnost, platnost a konzistentnost seznamu během celého životního cyklu systémových komponent. Systémové komponenty jsou evidovány spolu s informacemi potřebnými k jejich aplikaci na proces řízení rizik, včetně kroků, kterými je zajištěno zvládání rizik během celého jejich životního cyklu. Změny těchto informací jsou evidovány.	C5 AM-01	X	X	X	X	X	X	X	
5.2	Politiky pro používání a nakládání se systémovými komponenty	Zákazník zajistí, že politiky a pokyny materiálního dodavatele pro přijatelné použití a bezpečné nakládání se systémovými komponenty jsou dokumentovány, komunikovány a týkají se následujících aspektů: a) náležitosti inventarizace, b) klasifikace a označování na základě potřeby ochrany informací a opatření pro konkrétní úrovně ochrany, c) bezpečná konfigurace mechanismů pro zpracování chyb, provozních údajů, šifrování, ověřování a autorizaci, d) požadavky pro verzování softwaru, diskového obrazu a aplikace záplat, e) manipulace se systémovými komponentami, pro které již nejsou k dispozici opravné a bezpečnostní záplaty, f) omezení instalace softwaru nebo využívání služeb, g) ochrana před malwarem, h) dálková deaktivace, mazání nebo	C5 AM-02	X	X	X	X	X	X	X	

		blokování, i) fyzické dodání a přeprava, j) řešení kybernetických bezpečnostních incidentů a zranitelných míst, k) úplné a nezvratné smazání dat po vyřazení z provozu.									
5.3	Proces pro použití a implementaci hardwaru	Zákazník zajistí, že materiální dodavatel má schvalovací proces pro použití systémových komponent, které mají být uvedeny do provozu a jsou používány k poskytování cloudových služeb v produkčním prostředí, ve kterých jsou rizika vyplývající z jejich uvedení do provozu identifikována, analyzována a zmírněna. Schválení se uděluje pro ověření bezpečné konfigurace mechanismu pro zpracování chyb, provozních údajů, šifrování, ověřování a autorizaci podle zamýšleného použití a na základě příslušných politik.	C5 AM-03		X	X	X	X	X	X	

5.4	Proces pro vyřazení hardwaru	Zákazník zajistí, že vyřazení systémových komponent používaných k provozování systémových komponent podporujících produkční prostředí cloudových služeb v odpovědnosti materiálního dodavatele, vyžaduje schválení na základě příslušných politik. Vyřazení z provozu zahrnuje úplné a trvalé vymazání dat nebo řádné zničení média.	C5 AM-04		X	X	X	X	X	X	
5.5	Dodržování zásad a pokynu pro manipulaci se systémovými komponenty	Zákazník zajistí, že interní a externí zaměstnanci materiálního dodavatele se prokazatelně zavázali dodržovat zásady a pokyny pro přijatelné používání a nakládání se systémovými komponentami dříve, než mohou být použity za předpokladu, že materiální dodavatel zjistil, že ztráta nebo neoprávněný přístup může ohrozit bezpečnost informací cloudové služby. Veškerá předané systémové komponenty jsou prokazatelně vráceny materiálnímu dodavateli po ukončení pracovního poměru.	C5 AM-05		X	X	X	X	X	X	
5.6	Klasifikace a označení systémových komponent	Zákazník zajistí, že systémové komponenty jsou klasifikovány a pokud možno označeny. Klasifikace a označení systémových komponent odráží potřeby ochrany informací, které zpracovávají, ukládají nebo přenáší. Potřebu ochrany určuje jednotlivec nebo tým odpovědný za systémové komponenty na straně materiálního dodavatele podle jednotného schématu. Schéma určuje cíle ochrany podle důvěrnosti, integrity a dostupnosti.	C5 AM-06		X	X	X	X	X	X	

6		**Fyzická bezpečnost (PS)**									
6.1	Fyzická bezpečnost a požadavky na ochranu prostředí	Zákazník zajistí, že bezpečnostní požadavky budov a prostorů vztahujících se k poskytování cloudových služeb jsou založeny na bezpečnostních cílech, identifikovaných bezpečnostních požadavcích a posouzení rizik fyzické a environmentální bezpečnosti. Zákazník zajistí, že tyto bezpečnostní požadavky jsou zdokumentovány, komunikovány a poskytovány ve formě bezpečnostních politik a konceptů dle ustanovení ID 3.1.	C5 PS-01	X	X	X	X	X	X	X	
6.2		Zákazník zajistí, že materiální dodavatel zajišťuje alespoň jednoho záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra.	C5 PS-01	X	X	X	X	X	X	X	
6.3		Zákazník zajistí, že pokud materiální dodavatel využívá k poskytování cloudových služeb prostory nebo budovy provozované třetími stranami, mají zdokumentované, které bezpečnostní požadavky přenáší poskytovatel na tuto třetí stranu. Vhodné a efektivní ověření implementace bezpečnostních pravidel je provedeno v souladu s pravidly pro kontrolu a monitoring subdodavatelů (dle ID 13.4).	C5 PS-01	X	X	X	X	X	X	X	
6.4		Zákazník zajistí, že materiální dodavatel zajistí samostatný provoz zařízení poskytujících cloudové služby v případě výpadku dodávek energií alespoň na 48 hodin.	C5 PS-01 add			X	X	X	X	X	

6.5	Modely redundance	Zákazník zajistí, že materiální dodavatel umožňuje synchronní replikaci zákaznických dat a provozních údajů alespoň do jednoho záložního datového centra, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra.				X	X		X	X	
6.6		Zákazník zajistí, že materiální dodavatel zajistí alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra.				X	X	X			
6.7		Zákazník zajistí, že materiální dodavatel zajistí, že primární i záložní datacentrum, ze kterého jsou poskytovány služby, jsou v dostatečné vzdálenosti od relevantních naturogenních a antropogenních zdrojů rizik nebo je přijato adekvátní bezpečnostní opatření.				X	X	X	X	X	
6.8		Zákazník zajistí, že materiální dodavatel zajistí, že primární a záložní datové centrum se nacházejí v rozdílných distribučních oblastech elektřiny a ve vzdálenosti alespoň 10km od sebe navzájem.				X	X	X	X	X	
6.9		Zákazník zajistí, že model redundance, který používá materiální dodavatel, odpovídá požadavkům zákazníka na spolehlivost a dostupnost cloudových služeb.	C5 PS-02 cust			X	X	X	X	X	
6.10	Ochrana perimetru	Zákazník zajistí, že struktura prostor a budov sloužících k poskytování cloudových služeb je fyzicky pevná, ucelená a chráněná způsobem adekvátním k tomu, aby vyhovovala bezpečnostním požadavkům kladeným na materiálního dodavatele v ustanoveních ID 6.1.	C5 PS-03			X	X	X	X	X	

6.11		Zákazník zajistí, že materiální dodavatel prokazatelně zavedl v prostorách a objektech sloužících k poskytování cloudových služeb bezpečnostní opatření vhodná k tomu, aby zavčas detekoval a zabránil neoprávněnému či neautorizovanému přístupu, nebo k poškození a neoprávněným zásahům tak, aby nedošlo k narušení informační bezpečnosti cloudových služeb.	C5 PS-03 + § 17 VKB	X	X	X	X	X	X	X	
6.12		Zákazník zajistí, že materiální dodavatel zajistil bezpečnostní opatření na vstupu do prostor a budov sloužících k poskytování cloudových služeb, které minimálně zahrnují permanentně přítomný bezpečnostní personál (alespoň dva lidé), kamerový dohled a systém ochrany proti vloupání.	C5 PS-03 add			X	X	X	X	X	

6.13	Kontrola fyzického přístupu	Zákazník zajistí, že materiální dodavatel na vstupu do prostor a budov sloužících k poskytování cloudových služeb kontroluje fyzický přístup v souladu s ustanovením ID 6.1 tak, aby zabránil neautorizovanému přístupu. Kontrola přístupu je podporována systémem na kontrolu přístupu. Požadavky na systém na kontrolu přístupů jsou zdokumentovány, komunikovány, zahrnuty v bezpečnostní politice nebo konceptu dle ID 3.1 a pokrývají minimálně následující aspekty: a) Specifikaci procedury pro udělení a odejmutí přístupu založené na principu nejnižšího privilegia (least-privilige-principle) a na nutnosti potřeby znalostí pro výkon úkolu (need-to-know principle); b) Automatické odejmutí přístupových práv, pokud nebyla využita v období dvou měsíců; c) Automatické stažení přístupových práv, pokud nebyla využita v období šesti měsíců; d) Dvoufaktorová autentizace pro přístup do oblastí se systémovými komponentami, které zpracovávají data zákazníka; e) Individuální sledování, vizuální označení a dohled nad návštěvníky a externími pracovníky během jejich pohybu po prostorách a budovách; f) Existence a povaha zaznamenávání přístupu, která umožní materiálnímu dodavateli efektivní dohled a kontrolu nad tím, jestli pouze určený personál vstupuje do prostor a budov sloužících k poskytování cloudových služeb.	C5 PS-04		X	X	X	X	X	X	

6.14	Ochrana před požárem a kouřem	Zákazník zajistí, že materiální dodavatel zajistí u prostor a budov sloužících k poskytování cloudových služeb před kouřem a ohněm strukturálními, technickými a organizačními opatřeními, které splňují bezpečnostní požadavky dle ID 6.1 a zahrnují například následující aspekty: a) Strukturální opatření: - zřízení požárních sekcí s odolností proti požárům alespoň 90 minut ve všech strukturálních částech. b) Technická opatření: - Systém včasného hlášení požárů s funkcí automatické vypnutí elektrického proudu; monitorované oblasti jsou dostatečně rozdělené tak, aby se proporčně vyvážilo bránění šíření požáru a současně zůstala zachována dostupnost poskytovaných cloudových služeb. - Automatický hasící systém, případně systém pro omezení přísunu kyslíku. - Požární alarm s napojením na místní hasičské stanici. c) Organizační opatření: - Pravidelné inspekce zkoumající soulad skutečného stavu s požadavky na požární bezpečnost. - Pravidelná požární cvičení.	C5 PS-05		X	X	X	X	X	X	
6.15		Všechna kritéria z ID 6.14 jsou hlídána a monitorována a překročení stanovených limitů je hlášeno expertním pracovníkům materiálního dodavatele.	C5 PS-05 add			X	X	X	X	X	

6.16	Ochrana před přerušeními dodávek zapříčiněnými výpadky proudu a podobnými riziky	Zákazník zajistí, že materiální dodavatel má v souladu s ustanoveními ID 6.1 zdokumentované prostředky sloužící k tomu, aby bylo zabráněno selhání technických dodávek pro prostory a budovy sloužící k poskytování cloudových služeb minimálně v těchto oblastech: a) Provozní redundance zdrojů energií a chlazení b) Používání adekvátně velkých zdrojů nepřerušitelných dodávek energie a nouzových zdrojů energie vybudovaných tak, aby bylo zajištěno, že všechna data zůstanou nepoškozena v případě výpadku proudu. Jejich funkčnost je testována vhodnými způsoby a cvičeními minimálně jednou ročně. c) Údržba (servisní zásahy, inspekce, opravy) je prováděna v souladu s doporučeními výrobce zařízení. d) Ochrana zdrojů energie a telekomunikačních zdrojů proti přerušení, rušení, poškození a odposlouchávání. Ochrana je pravidelně kontrolována, minimálně jednou za dva roky a pokaždé, když má kvalifikovaný personál podezření na neautorizovanou manipulaci.	C5 PS-06			X	X	X	X	X	
6.17		Zdroje nepřerušitelných dodávek energie a nouzové zdroje energie jsou nastaveny tak, aby vyhovovaly požadavkům stanoveným v SLA. Připojení k telekomunikační síti je nastaveno s dostatečnou redundancí tak, aby její selhání nemělo dopad na poskytování služeb materiálním dodavatelem.	C5 PS-06 add			X	X	X	X	X	

6.18	Dohled nad provozními a environmentálními parametry	Zákazník zajistí, že materiální dodavatel monitoruje a kontroluje operační parametry technických prostředků a sledované parametry prostor a budov spojených s poskytováním cloudových služeb s ohledem na bezpečnostní požadavky dle ID 6.1. V případě, že je překročen rozsah sledovaných hodnot, příslušné oddělení je automaticky informováno, aby mohlo bez prodlení zahájit nezbytné kroky k návratu hodnot do přípustného rozsahu.	C5 PS-07			X	X	X	X	X	
7		**Provoz (OPS)**									
7.1	Plánování kapacit	Zákazník zajistí, že plánování kapacit a zdrojů (personální a IT zdroje), se řídí zavedeným postupem, aby se zamezilo možným omezením poskytovaných služeb. Postupy zahrnují předpovídání budoucích požadavků na kapacitu za účelem identifikace trendů využití zdrojů a správy vytížení systému.	C5 OPS-01		X	X	X	X	X	X	
7.2		Zákazník zajistí, že materiální dodavatelé přijmou vhodná opatření, aby zajistili, že budou nadále plnit požadavky dohodnuté se zákazníky cloudu na poskytování cloudových služeb v případě kapacitních překážek nebo výpadků týkajících se personálních a IT zdrojů, zejména těch, které se týkají vyhrazeného využití systémových komponent v souladu s příslušnými dohodami.	C5 OPS-01		X	X	X	X	X	X	
7.3	Monitorování kapacit	Zákazník zajistí, že jsou definovány technické a organizační procesy pro monitorování a poskytování cloudových služeb. Materiální dodavatel tak zajišťuje, že zdroje a služby jsou poskytovány v souladu se smluvními dohodami a že je zajištěno	C5 OPS-02		X	X	X	X	X	X	

		dodržování dohod o úrovni služeb (monitoring a evaluace SLA).									
7.4	Řízení systémových zdrojů	Zákazník zajistí, že v závislosti na schopnostech příslušného modelu služby mu materiální dodavatel poskytne nástroje pro řízení a monitorování systémových kapacit a bezpečnostních událostí. Zákazník jejich využití zahrne do bezpečnostní politiky a bude tyto nástroje využívat pro sběr a nepřetržité vyhodnocování provozních a bezpečnostních událostí.	C5 OPS-03, ISO17 CLD.12.4.5			X	X	X	X	X	
7.5	Koncept malware ochrany	Zákazník zajistí, že politiky a pokyny, kterými materiální dodavatel řídí ochranu před malwarem jsou dokumentovány, sdělovány a poskytovány s ohledem na následující aspekty: a) použití ochranných mechanismů specifických pro používaný systém; b) provozování ochranných programů na systémových součástech, za které odpovídá materiální dodavatel a které se používají k poskytování cloudových služeb v produkčním prostředí; c) provoz programů ochrany na koncových zařízeních zaměstnanců.	C5 OPS-04	X	X	X	X	X	X	X	
7.6	Podpora	Zákazník si dohodne, termíny a časy fungování systémů a podpory.			X	X	X	X	X	X	
7.7	Monitoring kvality	Zákazník si dohodne, ustanovení o monitoringu kvality služby.			X	X	X	X	X	X	

7.8	Implementace malware ochrany	Zákazník zajistí, že systémové komponenty spadající do odpovědnosti materiálního dodavatele cloudových služeb, které se používají k nasazení cloudové služby v produkčním prostředí, jsou nakonfigurovány s ochranou proti malwaru. Pokud to distribuční model neumožňuje nebo nejsou bezpečnostní produkty součástí služby, zajistí si tyto produkty zákazník sám a bude je využívat. Pokud jsou programy ochrany nastaveny na detekci podezřelého chování a odstranění škodlivého softwaru, jsou tyto programy ochrany aktualizovány alespoň denně.	C5 OPS-05 + add			X	X	X	X	X	
7.9	Zaznamenání logů	Zákazník zajistí definici svých požadavků na zaznamenávání bezpečnostních událostí a zajistí, že materiální dodavatel tyto požadavky splňuje.	ISO17 12.4.1		X	X	X	X	X	X	
7.10	Koncept ochrany a obnovy dat	Zákazník zajistí, že politiky a pokyny pro zálohování a obnovu dat jsou dokumentovány, komunikovány a poskytovány, pokud jde o následující aspekty: a) rozsah a četnost zálohování dat a doba uchovávání dat jsou v souladu se smluvními dohodami se zákazníky cloudu a s požadavky na provozní kontinuitu materiálního dodavatele, b) k šifrování dat jsou použity nejmodernější metody, c) přístup k zálohovaným datům a k provádění obnov mají pouze oprávněné osoby, d) zkoušky procesů obnovy.	C5 OPS-06	X	X	X	X	X	X	X	

7.11	Monitoring záloh a obnovy dat	Zákazník zajistí, že zálohování dat je monitorováno pomocí technických a organizačních opatření. Poruchy jsou vyšetřovány kvalifikovaným personálem a neprodleně odstraňovány, aby bylo zajištěno dodržování smluvních závazků vůči zákazníkům cloudu a materiálnímu dodavateli v ohledech týkajících se četnosti zálohování dat a doby jejich ukládání.	C5 OPS-07		X	X	X	X	X	X	
7.12	Pravidelná kontrola procesu obnovy a zálohování	Zákazník zajistí, že procesy obnovy se testují pravidelně, nejméně jednou ročně. Testy umožnují posoudit, zda jsou dodržovány smluvní dohody a specifikace pro maximální přípustné prostoje (RTO) a maximální přípustnou ztrátu dat (RPO). Odchylky od specifikací jsou hlášeny odpovědnému personálu nebo komponentám systému, aby bylo možno je okamžitě vyhodnotit a zahájit nezbytné kroky k nápravě.	C5 OPS-08		X	X	X	X	X	X	
7.13	Přenos a zálohování dat	Zákazník zajistí, že materiální dodavatel na základě hodnocení rizik přenáší data, určená k zálohování, do vzdáleného umístění nebo je přenáší na záložní médium. Pokud jsou data přenášena prostřednictvím sítě, probíhá záloha dat nebo přenos v zašifrované formě, který odpovídá doporučením NÚKIB v oblasti kryptografických prostředků.	C5 OPS-09			X	X	X	X	X	

7.14	Koncept sběr a monitoringu provozních údajů	Zákazník zajistí, že materiální dodavatel zavedl politiky a pokyny, kterými se řídí sběr a monitoring provozních údajů a na systémových komponentech v oblasti jeho odpovědnosti. Tyto zásady a pokyny jsou dokumentovány, sdělovány a poskytovány s ohledem na následující aspekty: a) definice bezpečnostních událostí, které by mohly vést k narušení pravidel pro ochranu, b) specifikace pro aktivaci, zastavení a pozastavení sběru provozních údajů, c) informace týkající se účelu a doby uchovávání provozních údajů, d) definice rolí a odpovědnosti za nastavení a monitorování provozních údajů, e) synchronizace času systémových komponent, f) shoda s právními a regulatorními požadavky.	C5 OPS-10	X	X	X	X	X	X	X	
7.15		Zákazník zajistí, že materiální dodavatel uchovává provozní údaje alespoň 12 měsíců, po jejich vytvoření.			X	X	X	X	X	X	

7.16	Bezpečné nakládání se zákaznickými daty bez zákaznického obsahu	Zákazník zajistí, že zásady a pokyny pro bezpečné nakládání se zákaznickými daty bez zákaznického obsahu jsou dokumentovány, sdělovány a poskytovány s ohledem na následující aspekty: a) zákaznická data bez zákaznického obsahu se shromažďují a používají výhradně pro účely fakturace, řešení provozních incidentů a řízení kybernetických bezpečnostních incidentů, b) anonymizovat zákaznická data bez zákaznického obsahu tak, aby nebylo možné vyvodit žádné závěry o cloudovém zákazníkovi nebo uživateli, c) žádné komerční využití, d) skladování na pevně stanovené období přiměřeně spojené s účely sběru, e) okamžité vymazání, pokud jsou splněny účely sbírky a další skladování již není nutné, f) poskytování cloudovým zákazníkům podle smluvních dohod.	C5 OPS-11		X	X	X	X	X	X	
7.17	Přístup, úložiště a odstranění zákaznických dat bez zákaznického obsahu	Zákazník zajistí, že požadavky na sběr provozních dat a monitorování bezpečnostních událostí a na bezpečné nakládání se zákaznickými daty bez zákaznického obsahu jsou prováděny technicky podporovanými postupy s ohledem na tato omezení: a) přístup pouze oprávněným uživatelům a systémům, b) pozastavení po stanovenou dobu, c) smazání dat, pokud pozastavení již není pro potřeby sběru dat nadále potřeba.	C5 OPS-12		X	X	X	X	X	X	

7.18	Identifikace bezpečnostních událostí	Zákazník zajistí, že provozní údaje jsou automaticky monitorovány pro případné bezpečnostní události, které mohou narušit cíle ochrany v souladu s požadavky na sběr provozních údajů a monitorování. To také zahrnuje detekci vztahů mezi bezpečnostními událostmi. Identifikované události jsou automaticky hlášeny příslušným oddělením pro rychle vyhodnocení a vhodnou reakci.	C5 OPS-13		X	X	X	X	X	X	
7.19	Ukládání logů	Zákazník zajistí, že materiální dodavatel cloudových služeb uchovává vygenerované provozní údaje a uchovává je ve vhodné, neměnné a agregované formě, bez ohledu na jejich zdroj, aby bylo možné centrální autorizované vyhodnocení dat. Data protokolu jsou vymazána, pokud již nejsou požadována pro účel, pro který byla shromážděna.	C5 OPS-14		X	X	X	X	X	X	
7.20	Identifikace přístupů pro forenzní analýzu	Zákazník zajistí, že vygenerované provozní údaje umožňují jednoznačnou identifikaci přístupů uživatelů k provedení forenzní analýzy v případě kybernetického bezpečnostního incidentu.	C5 OPS-15		X	X	X	X	X	X	
7.21	Nastavení přístupů k logům	Zákazník zajistí, že přístup ke komponentám systému pro protokolování a monitorování v oblasti odpovědnosti materiálního dodavatele cloudových služeb je omezen na oprávněné uživatele.	C5 OPS-16		X	X	X	X	X	X	
7.22	Dostupnost systémů pro logování a monitoring	Zákazník zajistí, že materiální dodavatel monitoruje systémové komponenty v souvislosti se sběrem a monitorováním provozních údajů v oblasti jeho odpovědnosti. Poruchy jsou automaticky a neprodleně hlášeny odpovědným útvarům materiálního dodavatele, aby mohly být	C5 OPS-17		X	X	X	X	X	X	

		chyby vyhodnoceny a učiněna potřebná opatření.									
7.23	Zvládání zranitelností, poruch a chyb	Zákazník zajistí, že materiální dodavatel provede včasnou identifikaci a řešení zranitelností systémových komponent používaných k poskytování cloudové služby. Tyto pokyny a instrukce obsahují specifikace týkající se následujících aspektů: a) pravidelná identifikace zranitelných míst, b) posouzení závažnosti identifikovaných zranitelných míst, c) stanovení priorit a provádění akcí k rychlé nápravě nebo zmírnění identifikovaných zranitelných míst na základě závažnosti a podle definovaných časových os.	C5 OPS-18		X	X	X	X	X	X	
7.24	Penetrační testování	Zákazník zajistí, že materiální dodavatel cloudových služeb provádí alespoň jednou ročně penetrační testy prováděné kvalifikovanými interními zaměstnanci nebo dodavatelsky. Penetrační testy se provádějí podle zdokumentované metodiky zkoušek a zahrnují systémové komponenty relevantní pro poskytování cloudové služby v oblasti odpovědnosti materiálního dodavatele cloudových služeb, které byly jako takové identifikovány v analýze rizik.	C5 OPS-19			X	X	X	X	X	

7.25	Analýza a vyhodnocování zranitelností a bezpečnostních incidentů	Zákazník zajistí, že materiální dodavatel pravidelně měří, analyzuje a vyhodnocuje postupy, kterými se zachází se zranitelnostmi a kybernetickými bezpečnostními incidenty, aby ověřil jejich vhodnost a účinnost. Výsledky jsou vyhodnoceny alespoň jednou za čtvrt roku odpovědnými odděleními materiálního dodavatele, aby byly podniknuty nezbytné kroky pro funkčnost neustálého zlepšování a byla ověřena jejich účinnost.	C5 OPS-20		X	X	X	X	X	X	
7.26	Informovanost zákazníků v případě provozních incidentů	Zákazník zajistí, že materiální dodavatel cloudových služeb pravidelně informuje zákazníky cloudu o stavu provozních incidentů, které je ovlivňují, nebo je-li to vhodné a nutné, zapojí zákazníka do řešení a to způsobem, která je v souladu se smluvními podmínkami. Ihned po vyřešení incidentu je zákazník informován o přijatých opatřeních, podle smluvních dohod.	C5 OPS-21		X	X	X	X	X	X	
7.27	Testování a dokumentace známých zranitelností	Zákazník zajistí, že systémové komponenty v oblasti odpovědnosti materiálního dodavatele cloudových služeb jsou automaticky kontrolovány na známé zranitelnosti alespoň jednou měsíčně v souladu s politikami pro řešení zranitelností, závažnost je posuzována v souladu s definovanými kritérii a opatření pro včasnou nápravu nebo zmírnění jsou zahájena v definovaných časových oknech.	C5 OPS-22			X	X	X	X	X	
7.28	Hardening systému	Zákazník zajistí, že komponenty systému v produkčním prostředí jsou nastaveny podle obecně uznávaných průmyslových standardů. Požadavky na hardening pro každou součást systému jsou dokumentovány.	C5 OPS-23		X	X	X	X	X	X	

7.29	Rozdělení prostředí v cloudu	Zákazník zajistí, že zákaznická data uložená a zpracovaná na sdílených virtuálních a fyzických zdrojích jsou bezpečně a přísně oddělena, tak aby byla zajištěna důvěrnost a integrita těchto dat.	C5 OPS-24		X	X	X	X	X	X	
8		**Správa identit a řízení přístupu (IDM)**									
8.1		Zákazník zajistí, že materiální dodavatel umožní využívat pro přístup do správy cloud computingu vícefaktorovou autentizaci s nejméně dvěma různými typy faktorů.			X	X	X	X	X	X	
8.2		Zákazník zajistí, že využívá pro přístup do správy cloud computingu vícefaktorovou autentizaci s nejméně dvěma různými typy faktorů.			X	X	X	X	X	X	

8.3	Politika uživatelských účtů a přístupových práv	Zákazník zajistí, že v rámci materiálního dodavatele je uplatňován koncept rolí a práv zahrnující: • Přiřazení jedinečných uživatelských jmen; • Udělování a úpravy uživatelských účtů a přístupových práv na základě zásady nejnižšího privilegia (least privilege principle) a zásady nutnosti vědět (need to know principle); • Oddělení povinností mezi provozními a monitorovacími funkcemi („oddělení povinností“); • Oddělení povinností mezi správou, schvalováním a přiřazováním uživatelských účtů a přístupových práv; • Schválení oprávněné osoby nebo systémů k udělení nebo úpravě uživatelských účtů a přístupových práv před přístupem k datům cloudového zákazníka nebo systémových komponentů použitých k poskytování cloudové služby; • Pravidelná kontrola přidělených uživatelských účtů a přístupových práv; • Blokování a odebrání přístupových účtů v případě nečinnosti; • Odstranění nebo úprava přístupových práv v případě změn odpovědnosti za práci na základě času nebo události;	C5 IDM-01	X	X	X	X	X	X	X	

		• Dvoufázové nebo vícefaktorové ověřování pro uživatele s privilegovaným přístupem; • Požadavky na schvalování a dokumentaci správy uživatelských účtů a přístupových práv.									

8.4	Přidělování a změny v přístupových právech a uživatelských účtech	Zákazník zajistí, že specifikované postupy pro přidělování a úpravy uživatelských účtů a přístupových práv pro interní a externí zaměstnance materiálního dodavatele, jakož i pro systémové komponenty zapojené do automatizovaných autorizačních procesů materiálního dodavatele, zajišťují soulad s konceptem role a práv a politikou pro správu uživatelských účtů a přístupových práv.	C5 IDM-02	X	X	X	X	X	X	X	
8.5	Uzamčení a odebrání uživatelských účtu v případě neaktivity nebo vícenásobného chybného pokusu o přihlášení	Zákazník zajistí, že uživatelské účty interních a externích zaměstnanců materiálního dodavatele a systémových komponent zapojených do automatizovaných autorizačních procesů materiálního dodavatele jsou automaticky uzamčeny, pokud nebyly použity po dobu dvou měsíců. K odblokování těchto účtů je nutný souhlas autorizovaného personálu nebo systémových komponent. Uzamčené uživatelské účty jsou automaticky zrušeny po šesti měsících. Po zrušení musí být postup pro udělování uživatelských účtů a přístupových práv (srov. ID 8.4) opakován.	C5 IDM-03	X	X	X	X	X	X	X	
8.6	Odebrání nebo přizpůsobení přístupových práv v případě změny pracovních povinností nebo zařazení	Zákazník zajistí, že pokud se změní pracovní povinnosti interních nebo externích zaměstnanců materiálního dodavatele nebo úkoly systémových komponent zapojených do automatizovaných autorizačních procesů materiálního dodavatele, jsou jejich přístupová práva okamžitě zrušena. Privilegovaná přístupová práva jsou upravena nebo zrušena do 48 hodin od účinnosti změny. Všechna ostatní přístupová práva jsou upravena nebo zrušena do 14 dnů. Po zrušení musí být	C5 IDM-04	X	X	X	X	X	X	X	

		postup pro udělování uživatelských účtů a přístupových práv (srov. ID 8.4) opakován.									
8.7	Pravidelný přezkum přístupových práv	Zákazník zajistí, že přístupová práva interních a externích zaměstnanců materiálního dodavatele a systémových komponent, které hrají roli v automatizovaných procesech autorizace materiálního dodavatele, jsou přezkoumávána nejméně jednou ročně, aby se zajistilo, že stále odpovídají skutečné oblasti použití. Kontrolu provádějí pověřené osoby z organizačních jednotek materiálního dodavatele, které mohou posoudit vhodnost přidělených přístupových práv na základě jejich znalosti oblastí úkolů zaměstnanců nebo systémových komponent. Zjištěné odchylky budou řešeny neprodleně, nejpozději však do 7 dnů od jejich zjištění, vhodnou úpravou nebo odebráním přístupových práv.	C5 IDM-05	X	X	X	X	X	X	X	
8.8		Zákazník zajistí, že privilegovaná přístupová práva jsou přezkoumávána každých šest měsíců dle výše uvedeného postupu.	C5 IDM-05 add			X	X	X	X	X	

8.9	Privilegovaná přístupová práva	Zákazník zajistí, že privilegovaná přístupová práva jsou personalizována, časově omezena podle posouzení rizik a přiřazována podle potřeby pro provádění úkolů („zásada potřeby vědět“). Činnosti uživatelů s privilegovanými přístupovými právy se zaznamenávají, aby se zjistilo jakékoli zneužití privilegovaného přístupu v podezřelých případech. Zaznamenané informace jsou automaticky sledovány pro definované události, které mohou znamenat zneužití. Při zjištění takové události jsou odpovědní pracovníci automaticky informováni, aby mohli okamžitě posoudit, zda došlo k zneužití a přijmout odpovídající opatření.	C5 IDM-06	X	X	X	X	X	X	X	
8.10	Přístup k datům zákazníka	Zákazník zajistí, že je informován materiálním dodavatelem, kdykoli interní nebo externí zaměstnanci poskytovatele cloudových služeb čtou nebo zapisují zákaznická data nebo provozní údaje zpracované, uložené nebo přenášené v cloudové službě nebo k nim přistupují bez předchozího souhlasu zákazníka. Informace jsou poskytovány vždy, když provozní údaje nebo zákaznická data cloudového zákazníka nejsou nebo nebyly šifrovány, šifrování je / bylo zakázáno pro přístup k datům, nebo smluvní dohody takové informace výslovně nevylučují. Informace obsahují příčinu, čas, trvání, typ a rozsah přístupu. Tyto informace jsou dostatečně podrobné, aby umožnili odborníkům v oboru zákazníka posoudit rizika přístupu. Informace jsou poskytovány v souladu se smluvními dohodami nebo do 72 hodin po přístupu.	C5 IDM-07	X	X	X	X	X	X	X	

8.11		Zákazník zajistí, že v případě, že by měl externí či interní zaměstnanec materiálního dodavatele přistoupit k zákaznickým datům nebo provozním údajům, která nejsou šifrovány, vyžádá si nejprve souhlas zákazníka. Pro udělení tohoto souhlasu musí být zákazník informován o účelu přístupu, době trvání, času, typu a rozsahu přístupu, tak aby byl schopen vyhodnotit rizika spojená s tímto přístupem.	C5 IDM-07 add				X	X	X	X	
8.12	Důvěrnost a autenticita informací	Zákazník zajistí, že přidělení autentizačních informací pro přístup ke komponentám systému použitým k poskytování cloudové služby interním a externím uživatelům materiálního dodavatele a systémových komponent, které jsou zapojeny do automatizovaných autorizačních procesů materiálního dodavatele, se provádí řádným způsobem, který zajišťuje důvěrnost informací. Pokud jsou hesla použita jako autentizační informace, je jejich důvěrnost zajištěna následujícími postupy, pokud je to technicky možné: • Uživatelé si mohou vytvořit heslo sami, nebo musí změnit počáteční heslo při prvním přihlášení k systémové součásti. Počáteční heslo ztratí platnost po maximálně 14 dnech. • Při vytváření hesel je nutné dodržet požadavky na hesla stanovené zákazníkem, pokud je to technicky možné. • Uživatel je informován o změně nebo resetování hesla. • Úložiště na straně serveru používá kryptograficky silné hashovací funkce. Odchylky jsou vyhodnoceny pomocí analýzy	C5 IDM-08	X	X	X	X	X	X	X	

		rizik a jsou z nich vyvozena zmírňující opatření.									
8.13	Ověřovací mechanismy	Zákazník zajistí, že systémové komponenty v oblasti odpovědnosti materiálního, které se používají k poskytování cloudových služeb, ověřují uživatele interních a externích zaměstnanců materiálního dodavatele a systémové komponenty, které jsou zapojeny do automatizovaných autorizačních procesů materiálního dodavatele. Přístup k produkčnímu prostředí vyžaduje dvoufázové nebo vícefaktorové ověření. V rámci produkčního prostředí probíhá ověřování uživatelů pomocí hesel, digitálně podepsaných certifikátů nebo postupů, které dosahují přinejmenším rovnocenné úrovně zabezpečení.	C5 IDM-09	X	X	X	X	X	X	X	

9		**Správa klíčů a šifrování (CRY)**									
9.1	Politika pro používání šifrovacích procedur a správu klíčů	Zákazník zajistí, že materiální dodavatel má v souladu s touto vyhláškou zavedené a zdokumentované politiky a pokyny týkající se technických a organizačních pojistek pro šifrovací procedury a správu šifrovacích klíčů, které se dotýkají minimálně těchto oblastí: a) Používání silných šifrovacích postupů a bezpečných síťových protokolů zohledňujících nejnovější poznatky a postupy v dané oblasti. b) Šifrování, které je na základě risk-based analýzy přizpůsobeno povaze dat, komunikačním kanálům, typu, síle a kvalitě šifrování. c) Požadavky na zabezpečení generování, uchovávání, vyzvednutí, distribuci, stažení a výmaz šifrovacích klíčů. d) Zvážení relevantních právních a regulatorních závazků a požadavků.	C5 CRY-01	X	X	X	X	X	X	X	
9.2	Šifrování při přenosu dat	Zákazník zajistí, že materiální dodavatel zavedl procesy a technická opatření se silným šifrováním a autentizací pro přenos dat zákazníka po veřejných sítích.	C5 CRY-02	X	X	X	X	X	X	X	
9.3	Šifrování citlivých dat při uchovávání	Zákazník zajistí, že materiální dodavatel zavedl postupy a technické záruky pro šifrování dat zákazníků cloudu během skladování. Soukromé klíče používané pro šifrování jsou známy pouze zákazníkům cloudu v souladu s příslušnými zákonnými a regulačními povinnostmi a požadavky. Výjimky se řídí zadaným postupem. Postupy používání soukromých klíčů, včetně jakýchkoli výjimek, musí být smluvně dohodnuty se zákazníkem cloudu. Toto kritérium se nevztahuje na data, která nelze	C5 CRY-03	X	X	X	X	X	X	X	

		z funkčních důvodů šifrovat kvůli poskytování cloudové služby.									

9.4	Správa bezpečnostních klíčů	Zákazník zajistí, že postupy a technické záruky pro bezpečné řízení klíčů v oblasti odpovědnosti materiálního dodavatele zahrnují alespoň následující aspekty: • Generování klíčů pro různé kryptografické systémy a aplikace; • vydávání a získávání certifikátů veřejného klíče; • Poskytování a aktivace klíčů; • Bezpečné ukládání klíčů (oddělení systému správy klíčů od úrovně aplikací a middlewaru) včetně popisu toho, jak oprávnění uživatelé získávají přístup; • Změna nebo aktualizace kryptografických klíčů včetně politik definujících, za jakých podmínek a jakým způsobem mají být změny a / nebo aktualizace provedeny; • Zacházení s ohroženými klíči; • Stažení a vymazání klíčů; a • Jsou-li použity předem sdílené klíče, specifická ustanovení týkající se bezpečného použití tohoto postupu jsou specifikována samostatně.	C5 CRY-04	X	X	X	X	X	X	X	
10		**Zabezpečení komunikace**									
10.1		Zákazník zajistí reálné (fyzické) zdvojení připojení k poskytovateli cloud computingových služeb.				X	X	X	X	X	

10.2	Technické prostředky	Zákazník zajistí, že poskytovatel zavedl technické záruky, které jsou vhodné k rychlému odhalení a reakci na síťové útoky na základě nepravidelných vzorců příchozího nebo odchozího provozu a / nebo distribuované útoky typu Denial-of-Service (DDoS).	C5 COS-01	X	X	X	X	X	X	X	
10.3		Zákazník zajistí, že bude pravidelně vyhodnocovat informace a podklady týkající se síťových útoků dodaných poskytovatelem.			X	X	X	X	X	X	
10.4	Technické prostředky	Zákazník zajistí pro části cloudové služby v rámci své odpovědnosti (např. virtuální stroje v rámci řešení IaaS), aby detekovali a reagovali na síťové útoky založené na anomálních vzorech příchozího a odchozího provozu (např. MAC spoofing a ARP poisoning) útoky) a / nebo distribuované odmítnutí služby (DDoS) včas.	C5 COS-01 add			X	X	X	X	X	
10.5		Zákazník definuje své požadavky na oddělení v sítích tak, aby bylo ve sdíleném prostředí cloudových služeb dosaženo izolace nájemce, a ověří, že poskytovatel cloudových služeb tyto požadavky splňuje.	ISO17 13.1.3		X	X	X	X	X	X	
10.6	Bezpečnostní požadavky pro připojení v síti	Zákazník zjistí, jaké podmínky platí pro navázání spojení v síti poskytovatele cloudových služeb, konkrétně : a) v jakých případech mají být bezpečnostní zóny odděleny a ve kterých případech musí být zákazníci cloudu logicky nebo fyzicky odděleni; b) jaké komunikační vztahy a které síťové a aplikační protokoly jsou v každém případě povoleny; c) jak je datový přenos pro správu a monitorování oddělen od každého na úrovni sítě;	C5 COS-02		X	X	X	X	X	X	

		d) která interní komunikace mezi místy je povolena a; e) která síťová komunikace je povolena									
10.7	Monitorování připojení v síti	Zákazník zajistí, že se bude rozlišovat mezi důvěryhodnými a nedůvěryhodnými sítěmi. Na základě posouzení rizik jsou tyto sítě rozděleny do různých bezpečnostních zón pro interní a externí síťové oblasti (a případně DMZ). Fyzická a virtualizovaná síťová prostředí jsou navržena a nakonfigurována tak, aby omezovala a monitorovala navázané připojení k důvěryhodným nebo nedůvěryhodným sítím podle definovaných bezpečnostních požadavků.	C5 COS-03		X	X	X	X	X	X	
10.8	Monitorování připojení v síti	Zákazník zajistí (pomocí vhodných ovládacích prvků), že virtuální sítě v cloudové službě, jsou navrženy, nakonfigurovány a dokumentovány v souladu s jejich požadavky na zabezpečení sítě (např. Logickou segmentací organizačních jednotek cloudového zákazníka).	C5 COS-03 add		X	X	X	X	X	X	
10.9	Připojení mezi sítěmi	Zákazník zajistí, že každé rozhraní sítě je řízeno bezpečnostními branami. Autorizace přístupu do systému pro přístup mezi sítěmi	C5 COS-04	X	X	X	X	X	X	X	

		je založena na posouzení bezpečnosti na základě požadavků zákazníků cloudu.									
10.10	Připojení mezi sítěmi	Zákazník zajišťuje, že přístup je řízen podle jeho potřeb ochrany pomocí bezpečnostních bran na perimetrech virtuálních sítí v cloudové službě, za kterou jsou odpovědní.	C5 COS-04 add		X	X	X	X	X	X	
10.11	Sítě pro správu a provoz	Zákazník zajistí, že existují samostatné sítě pro administrativní správu a provoz. Tyto sítě jsou logicky nebo fyzicky odděleny od zákaznické sítě cloudu a jsou chráněny před neoprávněným přístupem pomocí vícefakotorové autentizace. Sítě využívané poskytovatelem cloudových služeb k migraci nebo vytváření virtuálních počítačů jsou také fyzicky nebo logicky odděleny od ostatních sítí.	C5 COS-05		X	X	X	X	X	X	
10.12	Oddělení datového provozu ve sdílených sítích	Zákazník zajistí, že jeho datový provoz ve společně používaných síťových prostředích je na síťové úrovni oddělen podle dokumentovaného konceptu tak, aby byla zajištěna důvěrnost a integrita přenášených dat.	C5 COS-06	X	X	X	X	X	X	X	
10.13	Dokumentace síťové topologie	Zákazník zajistí, aby dokumentace logické struktury sítě a používání k poskytování nebo provozování cloudové služby je sledovatelná a aktuální, aby se předešlo administrativním chybám během živého provozu a aby se zajistila včasná obnova v případě poruchy, v souladu se smluvními podmínkami. Dokumentace ukazuje, jak jsou přiděleny podsítě a jak je síť rozdělena na zóny a segmenty. Kromě toho jsou uvedena geografická umístění, v nichž jsou uložena data zákazníků cloudu.	C5 COS-07	X	X	X	X	X	X	X	

10.14	Politiky datových přenosů	Zákazník zajistí, že data (zákaznický obsah) přenášená do cloudové služby jsou chráněna proti neoprávněnému zásahu, kopírování, úpravě, přesměrování nebo vymazání v souladu s politikou bezpečnosti informací.	C5 COS-08	X	X	X	X	X	X	X	
10.15		Zákazník zajistí síťovou dostupnost v požadované kapacitě u svého dodavatele síťových služeb s ohledem na síťovou dostupnost nasmlouvaných cloudových služeb.	Eiopa G. 12	X	X	X	X	X	X	X	
11		**Přenositelnost, propojení a exit strategie (PI)**									
11.1		Zákazníci cloudu zajistí vhodnými opatřeními, že zákaznická data a provozní údaje včetně logů, ke kterým mají smluvní vztah, jsou požadována od materiálního dodavatele na konci smlouvy nebo přístupná přes definovaná rozhraní (typ a rozsah dat odpovídají smluvním dohodám, které byly uzavřeny před používání cloudové služby) a že jsou uložena v souladu se zákonnými požadavky použitelnými na tato data.		X	X	X	X	X	X	X	
11.2	Exit strategie	Zákazník vytvoří exit strategii, jejíž požadavky budou přeneseny do smluvního vztahu o poskytování služeb cloud computingu s materiálním dodavatelem		X	X	X	X	X	X	X	

11.3		Zákazník při tvorbě exit strategie pro potřeby smluvního vztahu s materiálním dodavatelem zajistí, že pokrývá zejména tyto aspekty: a) cíle, kterých má exit strategie dosáhnout b) definici spouštěčů exit strategie c) analýzu dopadů zaměřenou na náklady a lidské síly potřebné k úspěšné exit strategii d) rozdělení rolí a zodpovědností při průběhu exit strategie a transferu systémů (k jiným materiálním dodavatelům) e) definici parametrů úspěchu při provádění exit strategie f) ustanovení o smluvních pokutách při neúspěšné exit strategii		X	X	X	X	X	X	X	

11.4		Zákazník zajistí, vypracování plánů pro ukončení poskytování služby cloud computingu (exit strategii) s ohledem na to, aby byla co nejméně omezena dostupnost a kvalita služby. Obsahem exit strategie bude zejména: a) okolnosti, za kterých může dojít k aktivaci exit strategie - jednostranné rozhodnutí zákazníka o odstoupení od smlouvy - insolvence, rozpad, nebo ukončení činnosti materiálního dodavatele - výmaz poskytované služby z katalogu cloud computingu - nesoulad smlouvy s právními či regulatorními požadavky - uplynutí doby, na kterou byla smlouva uzavřena - hrubé porušení SLA poskytovatelem či materiálním dodavatelem - neshoda s materiálním dodavatelem při jednáních o změně smlouvy - významná změna kontroly nad materiálním dodavatelem - významná změna kontroly nad zásadními aktivy využívanými materiálními dodavateli k poskytování služby - významná změna u dodavatelů, subdodavatelů a třetích stran relevantních pro poskytování služby materiálním dodavatelem - jiná významná změna na straně materiálního dodavatele relevantní k poskytování služby b) určení typu záloh nutných pro úspěšné zvládnutí exit strategie c) vytipování možných variant řešení		X	X	X	X	X	X	X	

		migrace d) odhad nákladů migrace a srovnávací analýza se současným stavem e) podrobnosti o předání dat a provozních údajů zákazníkovi f) závazek materiálního dodavatele spolupracovat při předání dat se zákazníkem a budoucím materiálním dodavatelem, který převezme správu dat g) závazek materiálního dodavatele stanovit přechodné období po ukončení smluvního vztahu, během kterého nebude narušeno využívání služby h) lhůty pro ukončení exit strategie									
11.5		Zákazník zajistí, že má materiální dodavatel povinnost uhradit zákazníkovi náklady spojené s migrací v případě, že je aktivování		X	X	X	X	X	X	X	

		exit strategie způsobeno hrubým porušením smluvního vztahu									
11.6	Dokumentace bezpečnosti vstupů a výstupů	Zákazník zajistí, že materiální dodavatel umožní dostupnost cloudových služeb skrze jiné cloudové služby případně IT systémy zákazníka skrze zdokumentované rozhraní příchozích a odchozích dat. Zákazník dále zajistí, že materiální dodavatel má tato rozhraní jasně zdokumentovaná tak, aby z nich mohl zákazník, nebo expertní zaměstnanec zákazníka, získat data.	C5 PI-01	X	X	X	X	X	X	X	
11.7		Zákazník zajistí, že materiální dodavatel vede datovou komunikaci skrze standardizované komunikační protokoly, které zajišťují důvěrnost a integritu přenášených informací s ohledem na stanovenou úroveň ochrany; komunikace přes nedůvěryhodné sítě musí být šifrovaná podle ID 9.2.	C5 PI-01	X	X	X	X	X	X	X	
11.8		Zákazník zajistí, že materiální dodavatel poskytne dokumentaci rozhraní, jejíž typ a rozsah umožní zákazníkovým zaměstnancům s požadovanou úrovní kvalifikace tato rozhraní využívat k jejich účelu; dokumentace a informace v ní obsažené jsou materiálním dodavatelem udržované v takovém stavu, že jsou aplikovatelné na tu verzi cloudových služeb, která je určena pro užívání.	C5 PI-01	X	X	X	X	X	X	X	

11.9	Smluvní dohody o poskytování dat	Zákazník zajistí, že ve smlouvě s materiálním dodavatelem budou upraveny minimálně tyto oblasti týkající se ukončení smluvního vztahu do té míry, do jakých se dají aplikovat na cloudové služby: a) Typ, rozsah a formát dat, které poskytovatel poskytuje zákazníkovi; b) Definici časového rámce, během kterého poskytovatel předá a zpřístupní data zákazníkovi; c) Definici přesného dne, kdy poskytovatel znemožní zákazníkovi přístup k datům a vymaže je; d) Zodpovědnost a závazek poskytovatele spolupracovat při poskytnutí dat zákazníkovi. Definice jsou založené na potřebách kvalifikovaných zaměstnanců potenciálního zákazníka kteří posuzují vhodnost cloudových služeb s ohledem na závislost na materiálním dodavateli a s ohledem na právní a regulatorní požadavky.	C5 PI-02	X	X	X	X	X	X	X	
11.10		Návrh uvedených ustanovení (ID 11.9) je založen na zákonných a regulatorních požadavcích v prostředí materiálního dodavatele. Zákazník zajistí, že materiální dodavatel tyto požadavky pravidelně (nejméně jednou ročně) identifikuje, zkoumá jejich aktuálnost a případně navrhuje odpovídajícím způsobem ustanovení upravit.	C5 PI-02 add	X	X	X	X	X	X	X	
11.11	Bezpečný výmaz dat	Zákazník zajistí, že výmaz dat materiálním dodavatelem po ukončení smluvního vztahu je v souladu se smluvními ujednáními a relevantními právními a regulatorními požadavky.	C5 PI-03	X	X	X	X	X	X	X	

11.12		Zákazník zajistí, že materiální dodavatel vymaže zákaznická data a provozní údaje, a to jak v cloudovém prostředí zákazníka, tak v zálohách.	C5 PI-03	X	X	X	X	X	X	X	
11.13		Zákazník zajistí, že materiální dodavatel vymaže data způsobem znemožňujícím obnovení forenzními metodami.	C5 PI-03	X	X	X	X	X	X	X	
12		**Nákup, vývoj a úprava informačních systémů**									
12.1	Politiky pro vývoj a akvizici	Zákazník zajistí, že politiky a pokyny s technickými a organizačními opatřeními pro bezpečný vývoj cloudové služby jsou dokumentovány, komunikovány a poskytovány v souladu s bezpečnostními zásadami a pokyny. Politiky a pokyny jsou postaveny na základě uznávaných standardů a metod s ohledem na následující aspekty: a) Bezpečnost při vývoji softwaru (požadavky, návrh, implementace, testování a ověřování); b) Bezpečnost při zavádění softwaru (včetně nepřetržitého dodávání); c) Bezpečnost v provozu (reakce na zjištěné chyby a zranitelnosti).	C5 DEV-01		X	X	X			X	

12.2	Outsourcing vývoje	Zákazník zajistí, že v případě externího vývoje cloudové služby (nebo jednotlivých systémových komponent), jsou mezi poskytovatelem cloudových služeb a dodavatelem externího vývoje smluvně dohodnuty specifikace týkající se následujících aspektů: a) Bezpečnost při vývoji softwaru (požadavky, návrh, implementace, testy a ověření) v souladu s uznávanými standardy a metodami; b) Přijmutí/akceptace testů kvality poskytovaných služeb v souladu s dohodnutými funkčními a nefunkčními požadavky; c) Poskytnutí důkazu o tom, že bylo provedeno dostatečné bezpečnostní ověření, aby se vyloučila existence známých zranitelností.	C5 DEV-02		X	X	X	X	X	X	

12.3	Politiky pro změny	Zákazník zajistí, že politiky a pokyny s technickými a organizačními zabezpečeními pro správu změn systémových komponent cloudové služby v rámci nasazení softwaru jsou dokumentovány, komunikovány a poskytovány podle bezpečnostních zásad a pokynů s ohledem na následující aspekty: a) Kritéria pro posuzování rizik, kategorizace a stanovení priorit změn a související požadavky na typ a rozsah zkoušek, které mají být provedeny, a nezbytná schválení pro vývoj/nasazení v produkčním prostředí jsou schváleny oprávněnými osobami nebo systémovými komponenty. b) Požadavky na provedení a dokumentaci testování; c) Požadavky na oddělení povinností během vývoje, testování a vydávání změn; d) Požadavky na správné informování zákazníků cloudu o typu a rozsahu změn a následných povinností spolupráce v souladu se smluvními dohodami; e) Požadavky na dokumentaci změn v systémové, provozní a uživatelské dokumentaci; f) Požadavky na implementaci a dokumentaci nouzových změn, které musí splňovat stejnou úroveň zabezpečení jako běžné změny.	C5 DEV-03		X	X	X	X	X	X	

12.4	Bezpečnostní školení týkající se vývoje a nepřetržitého dodávání	Zákazník zajistí, že poskytovatel cloudových služeb poskytuje vzdělávací program pro pravidelné, cílové skupinově orientované bezpečnostní školení a informovanost interních a externích zaměstnanců o standardech a metodách bezpečného vývoje a poskytování softwaru a o tom, jak používat nástroje používané pro tento účel. Program je pravidelně přezkoumáván a aktualizován s ohledem na použité politiky a pokyny, přiřazené role a odpovědnosti a použité nástroje.	C5 DEV-04	X	X	X	X	X	X	X	
12.5	Hodnocení rizik, kategorizace a stanovení priorit	Zákazník zajistí, že v souladu s platnými zásadami (politiky pro změny informačních systémů), jsou změny podrobeny posouzení rizik s ohledem na možné dopady na dotčené součásti systému a podle toho jsou kategorizovány a stanoveny priority.	C5 DEV-05	X	X	X	X	X	X	X	
12.6	Testování změn	Zákazník zajistí, že změny cloudové služby jsou podrobeny příslušnému testování během softwarového vývoje a nasazení. Typ a rozsah testování odpovídají posouzení rizik. Testy jsou prováděny příslušně kvalifikovanými pracovníky poskytovatele nebo automatizovanými testovacími postupy, které odpovídají nejmodernějším metodám. Zákazníci jsou do testu zapojení v souladu se smluvními dohodami. Závažnost chyb a zranitelností zjištěných v testech, které jsou relevantní pro rozhodnutí o nasazení, je stanovena podle definovaných kritérií a jsou zahájeny akce pro včasnou nápravu nebo jejich zmírnění.	C5 DEV-06	X	X	X	X	X	X	X	

12.7	Logování změn	Zákazník zajistí, že systémové komponenty a nástroje pro správu zdrojových kódů a nasazení softwaru, které se používají k provádění změn systémových komponent cloudové služby v produkčním prostředí, podléhají koncepci rolí a práv podle Politiky uživatelských účtů a přístupových práv, a mechanismů autorizace. Musí být nakonfigurovány tak, aby byly zaznamenány všechny změny, a lze je tedy vysledovat zpět k jednotlivcům nebo systémovým komponentám, které je provádějí.	C5 DEV-07	X	X	X	X	X	X	X	
12.8	Řízení verzí	Zákazník zajistí, že postupy řízení verzí jsou nastaveny tak, aby sledovaly závislosti jednotlivých změn a obnovovaly postižené součástí systému zpět do jejich předchozího stavu v důsledku chyb nebo identifikovaných zranitelností.	C5 DEV-08		X	X	X	X	X	X	
12.9		Zákazník zajistí, že materiální poskytovatel má proces řízení změn.		X	X	X	X	X	X	X	
12.10	Schvalování změn	Zákazník zajistí, že pouze oprávnění pracovníci nebo systémové komponenty poskytovatele cloudových služeb schvalují změny v cloudové službě na základě definovaných kritérií (např. výsledky testů a požadovaná oprávnění) před tím, než jsou poskytnuty zákazníkům cloudu v produkčním prostředí. Zákazníci cloudu se na změnách podílejí podle smluvních dohod.	C5 DEV-09		X	X	X	X	X	X	

12.11	Oddělení prostředí	Zákazník zajistí, že produkční prostředí je fyzicky nebo logicky odděleno od testovacích nebo vývojových prostředí, aby se zabránilo neautorizovanému přístupu k zákaznickým datům, šíření malwaru nebo změnám systémových komponent. Data obsažena v produkčních prostředích se nepoužívají v testovacích nebo vývojových prostředích, aby nedošlo k ohrožení jejich důvěrnosti.	C5 DEV-10		X	X	X	X	X	X	
12.12		Zákazník zajistí, že materiální poskytovatel cloudových služeb bude povinen s dostatečným předstihem (předem schváleným) informovat orgán veřejné moci o plánované významné změně v poskytování služby a jejích dopadech.		X	X	X	X	X	X	X	
12.13		Zákazník zajistí možnost odstoupit od smlouvy v souvislosti s významnou změnou.		X	X	X	X	X	X	X	dle VKB, příloha č. 7 k vyhlášce č. 82/2018 Sb. písmeno n)
13		**Řízení dodavatelů (SSO)**									
13.1		Zákazník zajistí, že materiální dodavatel s dostatečným předstihem informuje zákazníka před plánovanou podstatnou změnou subdodavatele nebo subdodávky, dodávky služeb nebo změny třetí strany relevantní pro poskytování cloudových služeb, která může ovlivnit schopnost materiálního dodavatele plnit jeho smluvní povinnosti.		X	X	X	X	X	X	X	

13.2		Zákazník specifikuje, které ze služeb cloudu computingu nemůže materiální dodavatel zajistit skrze subdodavatele (systematické zpracovatele).	Eiopa G. 13			X	X	X	X	X	
13.3		Zákazník zajistí, že materiální dodavatel informuje zákazníka s dostatečným předstihem o významné změně v subdodavatelích (sub-outsourcovaných služeb), tak, aby zákazník mohl provést analýzu rizik; materiální dodavatel umožní podat námitky proti takovýmto změnám a umožní zákazníkovi ukončit smluvní vztah.	Eiopa G. 13	X	X	X	X	X	X	X	

13.4	Politiky a pokyny pro kontrolu a monitoring třetích stran	Zákazník zajistí, že materiální dodavatel má v souladu s ustanoveními v ID 3.1 zdokumentované politiky a pokyny pro kontrolu a monitoring třetích stran, jejichž dodávky a služby přispívají k poskytování cloudových služeb a tyto třetí strany jsou s nimi prokazatelně seznámeny; tyto politiky a pokyny pokrývají minimálně oblasti: a) Požadavky na proces posuzování rizik spojených s pořizováním služeb od třetích stran; b) Požadavky na klasifikaci třetích stran založené na posouzení rizik ze strany poskytovatele a zhodnocení, jestli je třetí strana subdodavatelem; c) Požadavky na bezpečnost informací pro případ zpracování, uchovávání nebo přenos informací třetími stranami založené na uznávaných technických standardech; d) Požadavky na školení zaměstnanců o informační bezpečnosti; e) Relevantní právní a regulatorní požadavky; f) Požadavky na vypořádání se se zranitelnostmi, bezpečnostními incidenty a poruchami; g) Specifikace smluvních podmínek pro tyto požadavky; h) Specifikace pro kontrolu dodržování těchto požadavků; i) Specifikace pro aplikaci těchto požadavků na poskytovatele služeb využívaných třetími stranami do té míry, do jaké tito poskytovatelé služeb přispívají k poskytnutí cloudové služby zákazníkovi.	C5 SSO-01	X	X	X	X	X	X	X	

13.5	Analýza rizik poskytovatelů služeb a dodavatelů	Zákazník zajistí, že materiální dodavatel provádí posouzení rizik při využívání služeb dalších dodavatelů a subdodavatelů podle politik a pokynů pro kontrolu a monitoring třetích stran před tím, než jsou tyto třetí strany zapojeny do poskytování cloudových služeb zákazníkovi. Aktuálnost posouzení rizik je pravidelně, minimálně jednou ročně, přezkoumána kvalifikovaným personálem materiálního dodavatele během využívání služby.	C5 SSO-02	X	X	X	X	X	X	X	
13.6		Zákazník zajistí, že materiálním dodavatelem prováděné posouzení rizik zahrnuje identifikaci, analýzu, zhodnocení, zvládání a dokumentaci rizik s ohledem na následující aspekty: a) Potřebná úroveň ochrany zajišťující dostupnost, důvěrnost a integritu informací zpracovávaných, uchovávaných nebo přenášených třetími stranami; b) Dopady narušení ochrany a bezpečnostních incidentů na poskytování cloudových služeb; c) Závislost materiálního dodavatele na službách třetí strany s ohledem na rozsah, komplexnost a unikátnost pořizovaných služeb se zvážením možných alternativ.	C5 SSO-02	X	X	X	X	X	X	X	

13.7	Databáze systematických zpracovatelů a dodavatelů	Zákazník zajistí, že materiální dodavatel vede a udržuje databázi třetích stran, které přispívají k poskytování cloudových služeb zákazníkovi. Tato databáze obsahuje minimálně následující údaje: a) Název společnosti; b) Sídlo společnosti; c) Umístění zpracovávání a uchovávání dat; d) Kontaktní zodpovědná osoba třetí strany; e) Kontaktní zodpovědná osoba poskytovatele; f) Popis služby; g) Klasifikace založená na analýze rizik; h) Počátek využívání služby; a i) Důkaz souladu se smluvními požadavky. Materiální dodavatel informace v databázi minimálně jednou ročně přezkoumá s ohledem na jejich kompletnost, přesnost a pravdivost.	C5 SSO-03	X	X	X	X	X	X	X	
13.8	Monitoring shody s požadavky	Zákazník zajistí, že materiální dodavatel kontroluje shodu s požadavky na informační bezpečnost a aplikovatelné právní a regulatorní požadavky v souladu s politikami a pokyny týkajícími se kontroly a monitoringu třetích stran. Monitoring zahrnuje pravidelné revize níže uvedených podkladů v rozsahu, v jakém je poskytnutí těchto podkladů třetí stranou v souladu se smluvními podmínkami: a) Zprávy o kvalitě poskytovaných služeb; b) Certifikáty řídících systémů, soulad s mezinárodně uznávanými standardy; c) Nezávislé auditní zprávy třetí strany o vhodnosti a operační efektivitě jejích vnitřních kontrolních systémů zaměřených na poskytování služby; a	C5 SSO-04	X	X	X	X	X	X	X	

		d) Záznamy třetí strany o zvládání zranitelností, bezpečnostních incidentů a poruch.									
13.9		Zákazník zajistí, že materiální dodavatel provádí kontrolu s frekvencí odpovídající zařazení třetí strany do kategorie založené na posouzení rizik provedeném materiálním dodavatelem podle ustanovení ID 13.5. Výsledky kontroly jsou zahrnovány do procedury řízení rizik. Identifikované porušení a neshody jsou analyzovány, zhodnoceny a ošetřeny v souladu s procesem řízení rizik.	C5 SSO-04	X	X	X	X	X	X	X	
13.10		Zákazník skrze vhodné kontrolní mechanismy zajistí, že zůstává po celou dobu informován o třetích stranách a subdodavatelích zapojených do poskytování cloudové služby a na základě informovanosti a zjištěných potřebách zpracovávaných a uchovávaných dat vložených do cloudové služby zvažuje, jestli je potřeba podnikat další kroky ke kontrole a monitorování těchto třetích stran a subdodavatelů.	C5 SSO-04 comp	X	X	X	X	X	X	X	

13.11	Exit strategie materiálního poskytovatele	Zákazník zajistí, že materiální dodavatel má vypracovanou a zdokumentovanou exit strategii pro ty poskytované služby, kde hodnocení rizik poskytovatelů služeb a dodavatelů s ohledem na rozsah, komplexnost a jedinečnost poskytované služby dosahuje úrovně velmi vysoké závislosti.	C5 SSO-05		X	X	X	X	X	X	
13.12		Zákazník zajistí, že materiálním dodavatelem zpracovaná exit strategie je v souladu s plánem kontinuity a zahrnuje minimálně následující aspekty: a) Analýzu potenciálních nákladů, dopadů, zdrojů a časové náročnosti potřebných k tranzici cloudové služby k alternativnímu poskytovateli; b) Určení a přidělení rolí, odpovědností a dostatečných zdrojů úspěšnému provedení tranzice; c) Definování kritérií úspěchu při provádění tranzice; d) Definování ukazatelů výkonu poskytované služby, jejichž nenaplnění iniciuje zahájení exit strategie.	C5 SSO-05		X	X	X	X	X	X	
14		**Správa kybernetických bezpečnostních incidentů (SIM)**									
14.1		Zákazník zajistí, že materiální dodavatel musí pravidelně informovat orgán veřejné moci o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy;		X	X	X	X	X	X	X	
14.2		Zákazník zajistí, že materiální dodavatel zaznamenává události, které ohrozily nebo narušily bezpečnost informačních systémů, a umožňuje zákazníkovi získání všech informací, které se týkají událostí, které	ČNB Cloudy, str. 3 přílohy	X	X	X	X	X	X	X	

		ohrozily nebo narušily bezpečnost zákaznických dat a provozních údajů.									
14.3		Zákazník zajistí, že dojde-li při zpracování zákaznických dat a provozních údajů, mimo rámec servisních úkonů a mimo rámec řízených přístupů, ke zpřístupnění dat zákazníka internímu nebo externímu zaměstnanci materiálního dodavatele nebo jiné osobě pro něj činné (řetězový outsourcing), materiální dodavatel mu neprodleně ohlásí toto zpřístupnění jako bezpečnostní incident.	ČNB Cloudy, str. 4 přílohy	X	X	X	X	X	X	X	
14.4		Zákazník zajistí, že ho materiální dodavatel stanoveným způsobem neprodleně informuje o vzniku kybernetického bezpečnostního incidentu nebo potvrzeného narušení bezpečnosti, kterým je zákazník postižen	exp. skupina 20. 03. 2020	X	X	X	X	X	X	X	
14.5	Politika řízení bezpečnostních incidentů	Zákazník zajistí, že má materiální dodavatel vypracované, zdokumentované a komunikované politiky a pokyny s technickými a bezpečnostními pojistkami, které jsou poskytovány v souladu s ID 3.1 tak, aby byla zajištěna rychlá, efektivní a řádná reakce na všechny známé bezpečnostní incidenty. Materiální dodavatel vypracuje návody pro klasifikaci, prioritizaci a eskalaci bezpečnostních incidentů a vytvoří rozhraní do řízení incidentů a řízení kontinuity. Materiální dodavatel dále zřídí Computer Emergency Response Team (CERT/CSIRT), který přispívá ke koordinovanému řešení	C5 SIM-01			X	X	X	X	X	

		bezpečnostních incidentů. Materiální dodavatel vhodným a včasným způsobem informuje zákazníka o bezpečnostním incidentu, který se jej týká.									
14.6		Zákazník zajistí, že materiální dodavatel vypracuje instrukce zabezpečující sběr dat z podezřelých systému přesvědčivým způsobem v případě bezpečnostního incidentu. Dále má zpracované plány pro případ typizovaných bezpečnostních incidentů a hodnotící metody na takové úrovni, aby získané informace neztratily důkazní hodnotu v případném následném zákonném posouzením.	C5 SIM-01 add			X	X	X	X	X	
14.7	Zpracovávání bezpečnostních incidentů	Zákazník zajistí, že materiální dodavatel, případně ve spolupráci s externími odborníky, klasifikuje, určí priority a provádí analýzy příčin událostí, které by mohly představovat bezpečnostní incident.	C5 SIM-02	X	X	X	X	X	X	X	
14.8		Zákazník zajistí, že materiální dodavatel provádí simulaci postupů spojených se zvládáním bezpečnostních incidentů a útoků alespoň jednou ročně prostřednictvím vhodných testů a cvičení (např. cvičení Blue Team x Red Team).	C5 SIM-02 add		X	X	X	X	X	X	

14.9	Dokumentace a hlášení bezpečnostních incidentů	Zákazník zajistí, že materiální dodavatel po zpracování bezpečnostních incidentů zdokumentuje jeho řešení a v souladu se smluvními podmínkami a zpráva ji zašle dotčeným zákazníků na vědomí, případně potvrzení zvoleného řešení.	C5 SIM-03	X	X	X	X	X	X	X	
14.10	Povinnost uživatelů nahlásit bezpečnostní incident	Zákazník zajistí, že materiální dodavatel informuje zaměstnance a další relevantní obchodní partnery o jejich povinnostech v oblasti bezpečnostních incidentů. V případě potřeby souhlasí, nebo jsou smluvně zavázáni okamžitě informovat materiálního dodavatele o všech bezpečnostních incidentech přímo se dotýkajících služby poskytování cloudu materiálním dodavatelem.	C5 SIM-04	X	X	X	X	X	X	X	
14.11	Zhodnocení a proces zlepšování	Zákazník zajistí, že materiální dodavatel má zavedené mechanismy k měření a monitorování typu a rozsahu bezpečnostních incidentů a k hlášení bezpečnostních incidentů relevantním úřadům. Informace získané z těchto hodnocení jsou využívány k identifikaci opakujících se bezpečnostních incidentů a určení oblastí potřebujících další ochranu.	C5 SIM-05	X	X	X	X	X	X	X	
15		**Řízení kontinuity činností**									
15.1		Zákazník zajistí, že v jeho pohotovostních plánech je zahrnut i případ neočekávaného ukončení činností poskytovatele služby cloud computingu, případ omezení přístupu k vlastnímu zákaznickému obsahu a přesun zákaznických dat (včetně logů - provozních údajů) zpět nebo k jinému poskytovateli outsourcingu.	ČNB Cloudy, str. 4 přílohy	X	X	X	X	X	X	X	

15.2	Odpovědnost vrcholového managementu	Zákazník zajistí, že vrcholový management materiálního dodavatele je jmenován jako vlastník procesu řízení kontinuity činností a procesu řízení krizových situací. Odpovídá za zavedení procesu v rámci organizace a za zajištění souladu s politikami a pokyny. Musí zajistit, aby byly k dispozici dostatečné zdroje pro efektivní činnost těchto procesů.	C5 BCM-01	X	X	X	X	X	X	X	
15.3	Politiky a pokyny pro analýzu dopadů	Zákazník zajistí, aby politiky a pokyny k určení dopadu jakékoli poruchy cloudové služby byly zdokumentovány, sdělovány a zpřístupněny v souladu s bezpečnostní politikou. Následující aspekty jsou považovány za minimum: a) Možné scénáře založené na analýze rizik; b) Identifikace kritických produktů a služeb; c) Identifikace závislostí, včetně procesů a požadovaných zdrojů, aplikací, obchodních partnerů a třetích stran; d) Hrozby zachycení pro kritické produkty a služby e) Identifikace dopadů vyplývajících z plánovaných a neplánovaných poruch a změn v průběhu času; f) Určení maximální přípustné doby výpadku služby; g) Stanovení priorit v procesu obnovy; h) Stanovení časových cílů pro obnovení kritických produktů a služeb v rámci RTO; i) Stanovení časových cílů do kterých musí být obnovena ztracená data v rámci RPO; j) Odhad zdrojů potřebných k efektivní činnosti procesu obnovy.	C5 BCM-02	X	X	X	X	X	X	X	

15.4	Plánování kontinuity činností	Zákazník zajistí, že na základě analýzy dopadů na podnikání bude zaveden, zdokumentován a vynucován jednotný rámec pro plánování provozní kontinuity. Plánování je založeno na zavedených standardech. Plány kontinuity činností a pohotovostní plány budou zohledňovat následující aspekty: a) Definovat účel a rozsah s ohledem na příslušné závislosti; b) Přístupnost a srozumitelnost plánů pro osoby, které mají podle něj jednat; c) Určení alespoň jedné osoby odpovědné za přezkoumání, aktualizaci a schválení; d) Definovat komunikační kanály, role a odpovědnosti včetně upozornění zákazníka; e) Postupy obnovy, dočasná řešení a referenční informace (s ohledem na stanovení priorit při obnově komponent a služeb infrastruktury a sladění se zákazníky); f) Metody pro realizaci plánů; g) Proces neustálého zlepšování; h) Prostředí pro řízení bezpečnostních incidentů.	C5 BCM-03	X	X	X	X	X	X	X	
15.5	Ověření, aktualizace a testování plánů kontinuity činností	Zákazník zajistí, že analýza dopadu na podnikání, plány kontinuity činností a havarijní plány jsou pravidelně přezkoumávány, aktualizovány a testovány (nejméně jednou ročně), nebo po významných organizačních nebo environmentálních změnách. Testy těchto plánů zahrnují zúčastněné zákazníky a příslušné třetí strany. Testy jsou zdokumentovány a výsledky jsou brány v úvahu pro budoucí opatření na zajištění kontinuity provozu.	C5 BCM-04	X	X	X	X	X	X	X	

15.6		Zákazník zajistí, že testy havarijních plánů mohou na vyžádání a po předchozí oboustranné domluvě probíhat za jeho účasti/dohledu při jejich průběhu.				X	X	X	X	X	
16		**Soulad s předpisy a audit (COM)**									
16.1	Identifikace požadavků	Zákazník zajistí, že materiální dodavatel jednoznačně identifikuje, dokumentuje a udržuje aktuální veškeré relevantní zákonné, předpisové a smluvní požadavky kladené na materiálního dodavatele a týkající se informační bezpečnosti cloudové služby a postupy materiálního dodavatele pro splnění těchto požadavků.	C5 COM-01		X	X	X	X	X	X	
16.2	Politika provádění auditů	Zákazník zajistí, že zásady a pokyny materiálního dodavatele pro plánování a provádění auditů jsou dokumentovány, komunikovány a zpřístupňovány a týkají se následujících aspektů: • Omezení přístupu k systémových komponentám pouze pro čtení v souladu s dohodnutým plánem auditu a podle potřeby k provádění činností; • Činnosti, které mohou mít za následek poruchu cloudové služby nebo porušení smluvních požadavků, jsou prováděny během plánovaných oken údržby nebo mimo období špiček; a • Protokolování a monitorování činností.	C5 COM-02, §3 písm. f) VKB, příl. 5 odst. 1.1 písm. e), 1.6 písm. d VKB		X	X	X	X	X	X	

16.3	Interní audit	Zákazník zajistí, že osoby s odpovídající odborností v rámci materiálního dodavatele prostřednictvím interních auditů kontrolují v pravidelných intervalech, nejméně jednou za dva roky, soulad systému řízení bezpečnosti informací s příslušnými a použitelnými právními, regulačními, dobrovolně převzatými nebo smluvními požadavky, jakož i dodržování politik a pokynů v rozsahu jejich působnosti. Zjištěné zranitelnosti a odchylky podléhají posouzení rizik v souladu s postupem řízení rizik a následná opatření jsou definována a sledována.	C5 COM-03, §16 odst. VKB, § 3 písm. f), g), i) VKB	X	X			X	X	X	
16.4	Interní audit	Zákazník zajistí, že osoby s odpovídající odborností v rámci materiálního dodavatele prostřednictvím interních auditů kontrolují v pravidelných intervalech, nejméně jednou ročně, soulad systému řízení bezpečnosti informací s příslušnými a použitelnými právními, regulačními, dobrovolně převzatými nebo smluvními požadavky, jakož i dodržování politik a pokynů v rozsahu jejich působnosti. Zjištěné zranitelnosti a odchylky podléhají posouzení rizik v souladu s postupem řízení rizik a následná opatření jsou definována a sledována.	C5 COM-03, §16 odst. VKB, § 3 písm. f), g), i) VKB			X	X	X	X	X	

16.5	Přezkum výsledků vedením	Zákazník zajistí, že vrcholové vedení materiálního dodavatele cloudových služeb je pravidelně informováno o výkonosti informační bezpečnosti v rámci systému řízení bezpečnosti informací, aby byla zajištěna jeho trvalá vhodnost, přiměřenost a účinnost. Informace jsou zahrnuty do přezkumu systému řízení bezpečnosti informací, které provádí vrcholové vedení materiálního dodavatele nejméně jednou za dva roky.		X	X			X	X	X	
16.6	Přezkum výsledků vedením	Zákazník zajistí, že vrcholové vedení materiálního dodavatele cloudových služeb je pravidelně informováno o výkonosti informační bezpečnosti v rámci systému řízení bezpečnosti informací, aby byla zajištěna jeho trvalá vhodnost, přiměřenost a účinnost. Informace jsou zahrnuty do přezkumu systému řízení bezpečnosti informací, které provádí vrcholové vedení materiálního dodavatele nejméně jednou ročně.				X	X	X	X	X	
16.7	Právo auditu NÚKIB, MV	Zákazník zajistí, že prodejce a materiální dodavatel umožní Ministerstvu vnitra nebo Národnímu úřadu pro kybernetickou a informační bezpečnost zdarma ve vztahu k dané cloudové službě provedení kontroly ve smyslu zákona o kontrole na všech místech, souvisejících s poskytováním dané cloudové služby a zároveň poskytnou veškerou součinnost, kterou si tyto orgány vyžádají.		X	X	X	X	X	X	X	

17		**Žádosti cizích státních orgánů o zpřístupnění nebo předání dat (INQ)**									
17.1	Informace o nakládání s žádostmi státních orgánů na zpřístupnění dat	Zákazník zajistí, že v popisu služby je jasně a srozumitelně uvedena informace o tom, jak materiální dodavatel nebo prodejce řeší žádosti ze strany cizích státních orgánů na zpřístupnění nebo předání zákaznických dat nebo provozních údajů. Informace obsahuje postup na ověření oprávněnosti (legálnosti) takové žádosti, postup zapojení a informování dotčeného zákazníka o takové žádosti, popis možností dotčeného zákazníka takovou žádost rozporovat a popis toho, zda je materiální dodavatel schopen rozšifrovat zašifrovaná zákaznická data a provozní údaje v případě takové žádosti a jak je tato schopnost materiálním dodavatelem využívána ke zpřístupnění nebo předání zákaznických dat nebo provozních údajů.	C5 BC-05		X	X	X	X	X	X	
17.2	Právní posouzení žádostí o předání nebo zpřístupnění	Zákazník zajistí, že v případě žádosti cizích státních orgánů vůči materiálnímu dodavateli nebo prodejci o zpřístupnění nebo předání zákaznických dat nebo provozních údajů, bude taková žádost podléhat právnímu posouzení odpovídajícími odborníky materiálního dodavatele nebo prodejce. Posouzení zohlední, zda má žádost státního orgánu proveditelný a platný právní základ, zda rozsah zákaznického obsahu, který je žádán zpřístupnit nebo předat, je přiměřený účelu žádosti a jaké další kroky je třeba podniknout. Zákazník zajistí, že o provedeném posouzení materiální dodavatel provede záznam, který uchová alespoň 10 let pro účely kontroly.	C5 INQ-01		X	X	X	X	X	X	

17.3	Posouzení rizika předání nebo zpřístupnění zákaznického obsahu státním orgánům	Zákazník v rámci řízení rizik vyhodnotí rizika pro bezpečnost informací vyplývající z možných žádostí cizích státních orgánů o zpřístupnění nebo předání zákaznických dat a provozních údajů a s tím i souvisejícím předáním nebo zpřístupněním jeho zákaznických dat nebo provozních údajů, přitom zohlední dostupné informace o jurisdikci míst zpracování zákaznických dat a provozních údajů (ID 1.2). O vyhodnocení rizik provede zákazník záznam. Cloudovou službu může zákazník využívat, pouze pokud bylo toto riziko vyhodnoceno jako přijatelné.	C5 INQ-01 add, BC-05	X	X	X	X	X	X	X	
17.4	Vyrozumění zákazníka o žádosti o předání nebo zpřístupnění	Zákazník zajistí, že ho materiální dodavatel nebo prodejce informuje bez zbytečného odkladu o žádosti cizích státních orgánů o zpřístupnění nebo předání zákaznických dat nebo provozních údajů, ledaže příslušný právní základ, na kterém je státní orgán zřízen nebo na kterém stojí žádost o předání nebo zpřístupnění zákaznických dat nebo provozních údajů, to zakazuje. V takovém případě zákazník zajistí, že ho materiální dodavatel informuje poté, co vyprší platnost právního zákazu, např. po vypršení období mlčenlivosti nařízeného zákonem nebo soudem.	C5 INQ-02	X	X	X	X	X	X	X	
17.5	Předání nebo zpřístupnění po kladném vyhodnocení	Zákazník zajistí, že zpřístupnění nebo předání zákaznického obsahu na základě žádosti cizích státních orgánů materiálním dodavatelem nebo prodejcem podléhá podmínce, že právní posouzení materiálním dodavatelem nebo prodejcem ukázalo, že žádost má proveditelný a platný právní základ a na tomto základě musí být žádosti vyhověno.	C5 INQ-03	X	X	X	X	X	X	X	

17.6	Postup pro předání nebo zpřístupnění dat	Zákazník zajistí, že postupy materiálního dodavatele nebo prodejce pro nastavování přístupu nebo předávání zákaznického obsahu na základě žádosti cizího státního orgánu zajistí, že cizí státní orgány budou mít přístup pouze k datům, která jsou nutná pro zajištění účelu, pro který je žádost podávaná. Pokud není možné jednoznačné vymezení zákaznického obsahu, materiální dodavatel nebo prodejce data anonymizuje nebo pseudonymizuje, tak aby cizí státní orgán mohl data přiřadit pouze k tomu zákazníkovi, který je předmětem žádosti o předání nebo zpřístupnění zákaznického obsahu.	C5 INQ-04	X	X	X	X	X	X	X	
17.7	Poskytnutí dat v souladu s MLAT	Zákazník zajistí, že materiální dodavatel žádost státního orgánu třetí země (stát mimo členský stát EU/EHP) uzná a zákaznická data a provozní údaje poskytne nebo zpřístupní, pouze pokud žádost vychází z mezinárodní dohody, například úmluvy o vzájemné právní pomoci, která je v platnosti mezi třetí zemí a EU nebo členským státem EU (viz čl. 48 GDPR). Výjimky pro specifické situace dle č. 49 GDPR tímto nejsou dotčeny.		X	X	X	X	X	X	X	
17.8	Zabránění obcházení MLAT	Zákazník zajistí, že materiální dodavatel neumožní předání zákaznických dat a provozních údajů z EU do třetí země za účelem poskytnutí nebo zpřístupnění zákaznických dat a provozních údajů státním orgánům třetí země na základě jejich žádosti o zpřístupnění nebo předání zákaznických dat a provozních údajů. Výjimky pro specifické situace dle č. 49 GDPR tímto nejsou dotčeny.			X	X	X	X	X	X	

18		**Bezpečnost a zabezpečení produktu**									
18.1	Pokyny a doporučení pro zákazníky cloudu	Zákazník zajistí, že materiální poskytovatel poskytuje zákazníkům cloudu pokyny a doporučení pro bezpečné používání poskytované cloudové služby. Informace v něm obsažené mají za cíl pomoci zákazníkovi cloudu v bezpečné konfiguraci, instalaci a použití cloudové služby. Typ a rozsah poskytovaných informací bude založen na potřebách zákazníka, který si stanoví požadavky na zabezpečení informací a jejich implementaci. Informace v pokynech a doporučeních pro bezpečné používání cloudové služby se týkají, kde je to aplikovatelné, následujících aspektů: a) Pokyny pro bezpečnou konfiguraci; b) Informační zdroje o známých zranitelnostech a mechanismech aktualizací; c) Mechanismy zpracování chyb a jejich logování; d) Mechanismy ověřování; e) Zavedení konceptu rolí a práv; f) Služby a funkce pro správu cloudové služby privilegovanými uživateli.	C5 PSS-01	X	X	X	X	X	X	X	

18.2	Identifikace zranitelností	Zákazník zajistí, že materiální poskytovatel cloudových služeb používá vhodná opatření ke kontrole zranitelností cloudové služby, které mohly být začleněny do služby během procesu jejího vývoje. Postupy pro identifikaci takových zranitelných míst jsou součástí procesu vývoje a v závislosti na posouzení rizik zahrnují následující činnosti: a) Statické testování zabezpečení aplikací; b) Dynamické testování zabezpečení aplikací; c) Kontrola kódu odborníky poskytovatele cloudových služeb; d) Získání informací o potvrzených zranitelnostech v softwarových knihovnách poskytovaných třetími stranami a používaných v jejich vlastních cloudových službách. Závažnost identifikovaných zranitelných míst je posuzována podle definovaných kritérií a jsou přijímána opatření k jejich okamžitému odstranění nebo zmírnění.	C5 PSS-02		X	X	X	X	X	X	
18.3	Registr známých zranitelností	Zákazník zajistí, že se materiální poskytovatel cloudových služeb odkazuje na (nebo provozuje denně aktualizovaný) online registr známých zranitelností, které ovlivňují poskytovatele a seznam systémových komponentů, které musí cloudoví zákazníci instalovat, poskytovat nebo sami provozovat na jejich vlastní odpovědnost. Online registr je snadno přístupný každému cloudovému zákazníkovi. Informace v nich obsažené tvoří vhodný základ pro posouzení rizik a možná následná opatření ze strany uživatelů cloudu. U každé chyby zabezpečení je uvedeno, zda jsou k dispozici aktualizace	C5 PSS-03		X	X	X	X	X	X	

		softwaru, kdy budou spuštěny a zda budou nasazeny poskytovatelem, zákazníkem, nebo oběma společně.									
18.4	Zpracování chyb a mechanismy logování	Zákazník zajistí, že poskytovaná cloudová služba je vybavena mechanismy zpracování chyb a logováním. Ty umožňují uživatelům cloudu získat informace týkající se stavu zabezpečení a poskytovaných dat, služeb nebo funkcí. Informace jsou dostatečně podrobné, aby umožnily uživatelům cloudu zkontrolovat následující aspekty (pokud jsou aplikovatelné pro cloudovou službu): a) K jakým datům, službám nebo funkcím, které má uživatel k dispozici, byl umožněn přístup, komu a kdy; b) Poruchy během zpracování automatických nebo ručních akcí; c) Změny konfiguračních parametrů souvisejících s bezpečností, mechanismy zpracování chyb a logování, autentizace uživatele, autorizace akce, kryptografie a zabezpečení komunikace. Logy jsou chráněny před neoprávněným přístupem a změnami a zákazník cloudu je může smazat. Pokud je zákazník cloudu odpovědný za aktivaci nebo typ a rozsah logování, musí poskytovatel poskytnout vhodné prostředky pro jejich sběr.	C5 PSS-04	X	X	X	X	X	X	X	

18.5	Mechanismy ověřování	Zákazník zajistí, že materiální poskytovatel cloudových služeb dává k dispozici mechanismy ověřování, které mohou vynutit vícefaktorovou autentizaci pro uživatele, IT komponenty nebo aplikace v oblasti odpovědnosti cloudových uživatelů. Tyto mechanismy ověřování jsou nastaveny na všech přístupových bodech, které umožňují uživatelům, IT komponentám nebo aplikacím přístup do cloudové služby. Pro privilegované uživatele, IT komponenty nebo aplikace jsou tyto mechanismy ověřování vynucovány.	C5 PSS-05	X	X	X	X	X	X	X	
18.6	Systém správy relací	Zákazník zajistí, že k ochraně důvěrnosti, dostupnosti a integrity během interakcí s cloudovou službou se používá vhodný systém správy relací, který odpovídá moderním standardům a je chráněn před známými zranitelnostmi. Jsou implementovány mechanismy, které znehodnocují relaci poté, co byla identifikována jako neaktivní. Nečinnost může být detekována měřením času. V tomto případě může být časový interval nakonfigurován poskytovatelem cloudových služeb nebo, pokud je to technicky možné, zákazníkem cloudu.	C5 PSS-06	X	X	X	X	X	X	X	
18.7	Řízení hesel	Zákazník zajistí, že pokud jsou hesla použita pro autentizaci, platí následující pravidla: a) Uživatelé mohou prvotně vytvořit heslo sami nebo při prvním přihlášení do cloudové služby. Pokud použijí počáteční heslo, musí jej změnit. Počáteční heslo ztratí platnost po maximálně 14 dnech; b) Při vytváření hesel je technicky vynuceno dodržování délky a složitosti, dle požadavků poskytovatele nebo zákazníka;	C5 PSS-07	X	X	X	X	X	X	X	

		c) Uživatel je informován o změně nebo resetování hesla;									
18.8	Koncept rolí a práv	Zákazník zajistí, že materiální poskytovatel cloudových služeb poskytuje uživatelům cloudu koncept rolí a práv pro správu přístupů. Popisuje profily práv pro funkce poskytované cloudovou službou. Profilování oprávnění je vhodné pro to, aby uživatelé mohli spravovat přístupová oprávnění v souladu s principem nejnižších privilegií a implementovat zásadu rozdělení pravomocí mezi provozními a kontrolními funkcemi.	C5 PSS-08	X	X	X	X	X	X	X	
18.9	Mechanismy řízení přístupu	Zákazník zajistí, že přístup k funkcím poskytovaným cloudovou službou je omezen řízením přístupu, který ověřuje, zda uživatelé, komponenty IT nebo aplikace jsou oprávnění provádět určité akce. Poskytovatel cloudové služby ověřuje funkčnost autorizačních mechanismů před tím, než jsou uživatelům cloudu zpřístupněny nové funkce, a v případě změn autorizačních mechanismů existujících funkcí. Závažnost identifikovaných zranitelností je hodnocena podle definovaných kritérií založených na standardizovaných metrikách CVSS (Common Vulnerability Scoring System) a jsou iniciována opatření pro včasné vyřešení nebo zmírnění. Chyby zabezpečení, které	C5 PSS-09	X	X	X	X	X	X	X	

		nebyly opraveny, jsou uvedeny v online registru známých chyb zabezpečení.									
18.10	Softwarově definované síťování	Zákazník zajistí, že pokud cloud služba nabízí funkce pro softwarově definované síťování (SDN), je důvěrnost dat uživatele cloudu zajištěna vhodnými SDN postupy. Poskytovatel cloudových služeb ověřuje funkčnost prostředků SDN před poskytnutím nových funkcí SDN uživatelům cloudu nebo úpravou stávajících funkcí SDN. Identifikované vady jsou posuzovány a opravovány způsobem orientovaným na rizika (risk-based approach).	C5 PSS-10		X	X	X	X	X	X	

18.11	Obrazy virtuálních zařízení a kontejnerů	Zákazník zajistí, že pokud provozuje virtuální zařízení nebo kontejnery, musí poskytovatel cloudových služeb zajistit následující aspekty: a) Zákazník cloudu může omezit výběr obrazu/image virtuálních zařízení nebo kontejnerů podle svých specifikací, takže uživatelé tohoto cloudového zákazníka mohou spustit pouze obraz/image nebo kontejnery vydané podle těchto omezení; b) Pokud poskytovatel cloudových služeb poskytne zákazníkovi cloudu obrazy/image virtuálních zařízení nebo kontejnerů, poskytovatel cloudových služeb náležitě informuje zákazníka cloudu o změnách provedených v předchozí verzi; c) Obrazy/image poskytnuté materiálním poskytovatelem prochází hardeningem dle obecně uznávaných standardů.	C5 PSS-11	X	X	X	X	X	X	X	

6 Stanovení bezpečnostních úrovní informačních systémů

Obsah této části zcela vychází ze Souhrnné analytické zprávy k projektu Příprava vybudování eGovernment cloudu, konkrétně z přílohy č. 4.

6.1 Základní východiska

Hodnocení důležitosti informačních systémů veřejné správy se v souladu s touto metodikou hodnotí pomocí určení kritických dopadů narušení dostupnosti, důvěrnosti a integrity dat nebo ICT služby, na kterých je funkčnost hodnoceného IS závislá. Primárně se hodnotí celý IS.

Pro určení dopadů narušení bezpečnosti je vytvořena hodnotící škála neboli vodítka hodnocení, která obsahují 10 oblastí (obecné scénáře) a 4 úrovně závažnosti dopadů (viz níže). Použití jednotné škály (vodítek hodnocení) pro hodnocení různých informačních systémů, by mělo zajistit jednotný způsob posouzení závažnosti dopadů narušení bezpečnosti a zároveň umožnit srovnání výsledků v rámci veřejné správy.

6.2 Princip hodnocení dopadů

Stanovení požadavků na úroveň bezpečnostních opatření využívaných cloudových služeb je založeno primárně na identifikaci požadavků na bezpečnost a spolehlivost celého IS.

Určení bezpečnostních parametrů IS vychází z identifikace kritických scénářů, které by mohly nastat v případě narušení dostupnosti zpracovávaných dat, jejich ztráty, narušení důvěrnosti a integrity dat. Kritické scénáře se pak mapují na scénáře uvedené ve vodítkách hodnocení.

6.2.1 Hodnocení následků nedostupnosti

Hodnocení následků nedostupnosti vychází z předpokladu, že nedochází ke ztrátě dat, jen k jejich dočasné nedostupnosti způsobené výpadkem informačního systému. Následky vyplývající z nedostupnosti dat se mohou lišit v závislosti na délce nedostupnosti IS. Pro stanovení okamžiku, kdy se poprvé projeví dopady z nedostupnosti a jak se v čase vyvíjí, se hodnocení provádí v následujících časových intervalech.

- nedostupnost 15 min.
- nedostupnost 1 hod.
- nedostupnost 4 hod.
- nedostupnost 8 hod.
- nedostupnost 16 hod.
- nedostupnost 1 den
- nedostupnost 2 dny
- nedostupnost 1 týden
- nedostupnost 14 dní
- nedostupnost 1 měsíc a více

Určení dopadů v jednotlivých časových intervalech napomáhá identifikovat okamžik, kdy se již výpadek IS stává pro správce IS neakceptovatelný. Je tak určující pro stanovení hodnoty RTO (recovery time objective), neboli času dokdy má být obnovena dostupnost služby po havárii.

Při hodnocení dopadů nedostupnosti je zároveň doporučeno zohlednit možnosti správce IS přejít na alternativní postupy zpracování dat – mimo systém, přičemž je ale třeba zohlednit sekundární dopady (např. zvýšené náklady), které zvolené alternativní zpracování může přinést.

Hodnocení narušení bezpečnosti dat a informací na základě interview s respondenty		Dostupnost									
Respondent	**Kategorie dat a informací (agenda)**	Nedostupnost 15 min.	Nedostupnost 1h	Nedostupnost 4h	Nedostupnost 8h	Nedostupnost 16 hod.	Nedostupnost 1den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více
doplnit jméno respondenta	doplnit název AIS / kategorie dat a informací										
	Bezpečnost a zdraví osob										
	Ochrana osobních údajů										
	Zákonné a smluvní povinnosti										
	Trestně-právní řízení										
	Veřejný pořádek										
	Mezinárodní vztahy										
	Řízení a provoz organizace			1	1	1	1	1	2	2	2
	Ztráta důvěryhodnosti										
	Finanční ztráty									1	1
	Zajišťování nezbytných služeb										

Poznámka: U některých IS se dopady nedostupnosti projeví v řádu minut až hodin, u jiných až v horizontu dní (obvykle pokud není daná agenda časově kritická, popř. lze její výkon zajistit mimo daný IS). Dopady nedostupnosti mohou u některých systémů růst lineárně, u některých bude dosaženo maxima např. po týdnu nedostupnosti a následně se již nezvětšuje (zůstává konstantní), protože se podařilo činnosti zajistit alternativním způsobem. Hlavní zásadou, kterou je třeba dodržovat, je že dopad v čase nemůže klesat.

6.2.2 Hodnocení následků ztráty dat

Tento dopad zkoumá následky, který by mohly vzniknout v případě ztráty dat. Pro určení optimálního požadavku na frekvenci zálohování dat se hodnocení provádí pro následující časové intervaly.

- Ztráta dat od zálohy (1 hod.)
- Ztráta dat od zálohy (4 hod.)
- Ztráta dat od zálohy (8 hod.)
- Ztráta dat od zálohy (16 hod.)
- Ztráta dat od zálohy (24 hod.)

Výsledek hodnocení totální ztráty dat ze systému může vyústit v požadavek na umístění záloh v geograficky oddělené lokalitě.

- Úplná ztráta dat

6.2.3 Hodnocení následků narušení důvěrnosti dat

Tento dopad je zkoumán z hlediska:

- prozrazení v rámci organizace – prozrazení zaměstnancům (lidem pracujícím pro organizaci, kteří však nemají oprávnění pro přístup k datům),
- prozrazení smluvním partnerům – prozrazení smluvním poskytovatelům služeb (zaměstnancům třetí strany, kteří mohou mít oprávněný přístup k systému nebo síti, ale nikoli k datům – například organizace provozující outsourcované informační služby),
- prozrazení vně organizace – únik informací na veřejnost.

Hodnocení narušení bezpečnosti dat a informací na základě interview s respondenty		Důvěrnost		
Respondent	**Kategorie dat a informací (agenda)**	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci
doplnit jméno respondenta	doplnit název AIS / kategorie dat a informací			
	Bezpečnost a zdraví osob			3
	Ochrana osobních údajů		2	3
	Zákonné a smluvní povinnosti			
	Trestně-právní řízení			
	Veřejný pořádek			
	Mezinárodní vztahy			
	Řízení a provoz organizace			
	Ztráta důvěryhodnosti	1		
	Finanční ztráty		2	3
	Zajišťování nezbytných služeb			

6.2.4 Hodnocení následků narušení integrity dat

Otázky zkoumané při vyšetřování tohoto dopadu se liší podle účelu hodnoceného informačního systému. Neodhalená změna nebo chyba v datech může způsobit zásadní dopady, organizace funguje na základě špatných dat. Dopad je zkoumán z hlediska:

- chyby malého rozsahu – neúmyslné modifikace dat, např. chyby při vkládání dat uživatelem, duplikace vstupu,
- chyby velké rozsahu – narušení správnosti a úplnosti informací velkého rozsahu, např. chyby v kódu informačního systému, porušení integrity dat vlivem technické selhání,
- úmyslné modifikace – úmyslná změna provedená uživatelem nebo správcem systému.

Hodnocení narušení bezpečnosti dat a informací na základě interview s respondenty		Integrita		
Respondent	**Kategorie dat a informací (agenda)**	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu	Úmyslná modifikace
doplnit jméno respondenta	doplnit název AIS / kategorie dat a informací			
	Bezpečnost a zdraví osob	1	3	4
	Ochrana osobních údajů		1	2
	Zákonné a smluvní povinnosti			
	Trestně-právní řízení			
	Veřejný pořádek			
	Mezinárodní vztahy			
	Řízení a provoz organizace			
	Ztráta důvěryhodnosti		1	2
	Finanční ztráty		1	2
	Zajišťování nezbytných služeb			

6.3 Postup hodnocení dopadů

Osvědčenou metodou hodnocení dopadů je řízené interview s věcným správcem (garantem) daného informačního systému, případně ve spolupráci s bezpečnostním ředitelem. Interview je vedeno zkušeným analytikem, který je znalý metodiky a postupů kvalitativního a kvantitativního hodnocení dopadů. Obvyklá délka interview na jeden IS je 90 až 120 minut. V případě potřeby se interview po dohodě s věcným správcem doplní o další sezení.

6.3.1 Průběh interview na hodnocení dopadů

V rámci interview jsou garanti dotazováni na nastínění realistického scénáře nejhoršího případu, který by mohl vyplývat z následujících dopadů:

- **nedostupnost** informačního systému (nedostupnost zpracovávaných informací),
- **ztráta** dat od poslední zálohy, úplná ztráta dat a informací,
- narušení **důvěrnosti** dat a informací (neoprávněné prozrazení a únik informací),
- narušení **integrity** dat a informací (vlivem neúmyslné modifikace (chyby), úmyslné modifikace dat a systémové chyby).

Interview zpravidla probíhají podle následujícího scénáře:

1) Získání základních informací o hodnoceném informačním systému: účel a rozsah zpracovávaných informací, relevantní legislativa a regulatorní požadavky, kritické termíny, úřední hodiny, lhůty apod.
2) Vysvětlení způsobu a postupu hodnocení dopadů. Zejména je potřeba zdůraznit dále uvedené zásady.

3) Kritické scénáře (scénáře nejhorší možného dopadu) popsané garantem se porovnají s obecnými vodítky pro hodnocení dopadů (viz níže Vodítka pro hodnocení dopadů). Pro určení závažnosti dopadů je použita stupnice o čtyřech úrovních dopadu (1-nízký, 2-střední, 3-vysoký, 4-kritický). *Poznámka: V případě, že se na danou situaci dá uplatnit více než jeden scénář současně (např. ohrožení bezpečnosti osob, ztráta důvěryhodnosti, finanční ztráta) se dopady nesčítají. Vždy se bere se v rámci vyhodnocení a stanovení požadavků na IS v potaz nejvyšší dosažená úroveň dopadu pro každý z parametrů bezpečnosti, viz příklad uvedený na obrázku níže.*
4) Po zpracování výsledků interview je vhodné zaslat výstup z hodnocení garantovi k revizi a odsouhlasení provedeného hodnocení.

Hodnocení narušení bezpečnosti dat a informací na základě interview s respondenty		Dostupnost										Ztráta						Důvěrnost			Integrita		
Respondent	**Kategorie dat a informací (agenda)**	Nedostupnost 15 min.	Nedostupnost 1h	Nedostupnost 4h	Nedostupnost 8h	Nedostupnost 16 hod.	Nedostupnost 1den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více	Ztráta dat od zálohy (1hod.)	Ztráta dat od zálohy (4hod.)	Ztráta dat od zálohy (8hod.)	Ztráta dat od zálohy (16hod.)	Ztráta dat od zálohy (24hod.)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu	Úmyslná modifikace
doplnit jméno respondenta	doplnit název AIS / kategorie dat a informací																						
	Bezpečnost a zdraví osob											1	1	1	1	1	2			3	1	3	4
	Ochrana osobních údajů		1	2	2	2	2	3	3	3	3						1		2	3		1	2
	Zákonné a smluvní povinnosti																						
	Trestně-právní řízení																						
	Veřejný pořádek																						
	Mezinárodní vztahy																						
	Řízení a provoz organizace			1	1	1	1	1	2	2	2												
	Ztráta důvěryhodnosti			2	2	2	3	3	4	4	4						1	1				1	2
	Finanční ztráty									1	1			1	1	1	3		2	3		1	2
	Zajišťování nezbytných služeb																						

6.3.2 Zásady, které je třeba při hodnocení dodržovat

Podstatou hodnocení dopadů je určit důležitost informačního systému neboli stanovit skutečné požadavky na zajištění zpracovávaných dat z hlediska požadavků na jejich dostupnost, důvěrnost a integritu. Pro maximální objektivitu hodnocení je potřeba se držet následujících zásad:

- Při hodnocení dopadů se nezkoumají možné příčiny (hrozby) narušení bezpečnosti.
- Neurčuje se pravděpodobnost výskytu jednotlivých scénářů narušení dostupnosti, důvěrnosti, integrity. Pokud je dopad podle scénáře, byť jen minimálně pravděpodobný, bere se v potaz, a stanoví se možné dopady dle scénářů vodítek hodnocení.
- Vždy se posuzují nejhorší možné scénáře. Kritické scénáře popisují nejhorší možné, ale stále ještě pravděpodobné dopady, které by mohly nastat v důsledku realizace různých hrozeb (kybernetické hrozby, fyzické hrozby, technické závady atd.). *Např. výpadek systému v neděli dopoledne může být nezajímavý, v pondělí dopoledne již může způsobit negativní dopad na služby občanům.*

Při hodnocení dopadů je důležité neuvažovat existující bezpečnostní opatření, aby se předešlo případným mylným předpokladům o jejich účinnosti a zejména pak zkreslení závažnosti dopadů.

6.4 Stanovení požadavků na bezpečnostní úroveň na základě výsledků hodnocení

Provedené hodnocení dopadů dává základ pro určení požadavků na bezpečnostní opatření. Například požadovanou úroveň redundance s ohledem na možné dopady nedostupnosti,

požadavek na použití kryptografických prostředků na ochranu dat v případě vysokých dopadů v oblasti důvěrnosti a zajištění integrity dat při přenosu. Od takto stanovených požadavků se pak odvíjí volba cloudové služby (bezpečnostní úroveň v rámci eGC), která je schopna požadované bezpečnostní parametry garantovat.

6.4.1 Odvození požadavků na dostupnost služby

Při rozhodování o požadované úrovni bezpečnosti eGC bude pro většinu správců IS klíčovým kritériem požadavek na dostupnost. Na základě výsledků hodnocení v následku narušení dostupnosti lze odvodit základní požadavky na SLA služby, jak je uvedeno na obrázku níže.

Příklad: Pro IS, který v následcích nedostupnosti dosáhne maximálně na střední úroveň dopadu a to až po 1 týdnu, bude dostačující SLA s garancí kumulovaného výpadku 8 hod. na měsíční bázi, tedy nejnižší úroveň eGC z hlediska dostupnosti.

Bezpečnostní úroveň	Základní požadavky na SLA cloudové služby			Dopady narušení dostupnosti									
	Dostupnost	Provozní doba pod SLA	Přípustná doba kumulovaných výpadků, s měsíčním vyhodnocováním	Nedostupnost 15 min.	Nedostupnost 1 h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 16 hod.	Nedostupnost 1 den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více
nízká (KeCG)	96,16%	Provozní doba pod SLA: minimálně určených 10 hodin v pracovní dny. Nezapočítávají se dny pracovního volna a dny pracovního klidu stanovené pro ČR. Např. r. 2018 má 250 pracovní dní , na bázi 10 hod. pod SLA denně, což dává max. měsíční výpadek 8,3 hod. při dostupnosti 96% (vztaženo na dobu pod SLA).	Max. 8 hod., avšak pouze v rámci definované pracovní doby	1							2	2	2
střední (KeCG)	99,45%	Provozní doba pod SLA: 24x7 (připravenost pro služby související s úplným el. podáním). Avšak určité služby SaaS, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu. To znamená, že el. podání bude obvykle fungovat nepřetržitě, ale reakce poskytovatele na nahlášené incidenty je omezena.	Max. 4 hod. na bázi 24x7	1			2	2	2	3	3	3	3
vysoká (KeCG)	99,90%	Provozní doba pod SLA: 24x7 (připravenost pro služby úplného el. podání, a pro ISVS pod ZoKB). Určité služby SaaS, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu.	Max. 43 min. na bázi 24x7	1	3	3	3	3	3	4	4	4	4
kritická (SeGC)	99,99%	Plně fault-tolerantní systém s geo-redundancí a replikací transakčních dat. Smluvní penále při výpadku dostupnosti služby delší než celkem 52 minut za rok (odpovídá 99,99%). Cloudové služby v této úrovni dopadu budou mít smluvně dané max. doby RPO / RTO.	Jednotlivý výpadek max. 15 min. Max. kumulovaný roční výpadek 52 min. (odpovídá 99,99%)	1-2	3-4								

Dosažení vyšší úrovně dopadů po delší době výpadku neznamená automaticky nutnost zařazení IS do vyšší bezpečnostní úrovně eGC. Správce IS může vyhodnotit rezervu dostupnosti v SLA jako akceptovatelné riziko na základě předchozích statistik, že např. u SLA dostupnosti "vysoká" je velmi malá pravděpodobnost, že výpadek dosáhne reálně doby 1 týdne a tím úrovně dopadů

"kritická". Každý správce IS musí vyhodnotit míru akceptovatelného rizika oproti zvýšeným nákladům, spojeným s pořízením služby kvalifikované pro vyšší úroveň dopadů.

6.4.2 Odvození požadavků na frekvenci vytváření a způsob uložení záloh dat

Pro časové intervaly, kde se dopady mění z hodnoty 1 na 2, popř. z hodnoty dopadu 2 na 3, je doporučeno vyjasnit výši nákladů, které mají zákazníci eGC s dodatečnou rekonstrukcí dat z jiných zdrojů (např. papírové formuláře) oproti nákladům spojeným s vyšší frekvencí vytváření záloh dat.

V případech, kdy jsou dopady z totální ztráty dat v elektronické podobě neakceptovatelné, je potřeby zvážit úroveň eGC, která nabízí geo-redundantní uložení dat.

Bezpečnostní úroveň	Ztráta dat					
	Ztráta dat od zálohy (1hod.)	Ztráta dat od zálohy (4hod.)	Ztráta dat od zálohy (8hod.)	Ztráta dat od zálohy (16hod.)	Ztráta dat od zálohy (24hod.)	Úplná ztráta dat
nízká (KeCG)	Pro časové intervaly, kde se dopady mění z hodnoty 1 na 2, popř. z hodnoty dopadu 2 na 3 je doporučeno vyjasnit výši nákladů, které mají OVM s dodatečnou rekonstrukcí dat z jiných zdrojů (např. papírové formuláře) oproti nákladům spojeným s vyšší frekvencí vytváření záloh dat.					1
střední (KeCG)						2
vysoká (KeCG)						3
kritická (SeGC)						4

6.4.3 Stanovení požadavků na důvěrnost dat

Výběr požadované bezpečnostní úrovně eGC z hlediska požadavků na zajištění důvěrnosti dat bude zpravidla podřízen požadavkům na dostupnost. V případech, kdy je v parametru důvěrnost dosaženo vyšší úrovně dopadu než v oblasti dostupnosti, je bezpečnostní úroveň eGC volena na základě dosažené hodnoty dopadu v parametru důvěrnost. Pokud se tedy ještě neuplatní dopady za integritu dat, viz dále.

V případech, kdy je u hodnoceného IS vyžadována ochrana právními předpisy, je nutné toto při výběru úrovně eGC zohlednit. Je-li tedy z nějakého důvodu ICT služba hodnocena dopadem ze ztráty důvěrnosti úrovní nižší než 3, je i přesto potřeba zvážit její zařazení do vyšší bezpečnostní úrovně eGC, minimálně do úrovně „vysoká“.

Poznámka: Bezpečnostní úrovně eGC jsou odstupňovány podle nabízených bezpečnostních funkcí zajišťujících důvěrnost uložených a přenášených dat. Pro úroveň dopadu „nízká“ nejsou kladené speciální požadavky na zajištění důvěrnosti a integrity dat. Naopak pro úroveň dopadu „vysoká“ a „kritická“ je nezbytné zajistit garanci šifrování uložených a přenášených dat, popř. také vyžadovat exkluzivní kontrolu nad šifrovacími klíči.

Bezpečnostní úroveň	Úrovně důvěrnosti		
	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci
nízká (KeCG)	1 Nízké požadavky na důvěrnost dat dle matice dopadů.		
střední (KeCG)	2 Střední požadavky na důvěrnost dat dle matice dopadů. V případech, kdy je vyžadována ochrana právními předpisy je nutné zvážit úroveň eGC "vysoká".		
vysoká (KeCG)	3 Vysoké požadavky na důvěrnost dat dle matice dopadů, popř. je ochrana vyžadována právními předpisy.		
kritická (SeGC)	4 Kritické požadavky na důvěrnost dat dle matice dopadů.		

6.4.4 Stanovení požadavků na integritu dat

Obdobně jako v oblasti důvěrnost platí i pro integritu dat, že výběr požadované bezpečnostní úrovně eGC bude zpravidla podřízen požadavkům na dostupnost IS. Tam, kde je v parametru integrita dosaženo vyšší úrovně dopadu než v oblasti dostupnosti, popř. též důvěrnosti, je bezpečnostní úroveň eGC volena na základě dosažené hodnoty dopadu v oblasti integrity dat.

Bezpečnostní úroveň	Úrovně integrity		
	Neúmyslná modifikace (chyba)	Systémová chyba	Úmyslná modifikace
nízká (KeCG)	1 Nízké požadavky na integritu dat dle matice dopadů.		
střední (KeCG)	2 Střední požadavky na integritu dat dle matice dopadů.		
vysoká (KeCG)	3 Vysoké požadavky na integritu dat dle matice dopadů.		
kritická (SeGC)	4 Kritické požadavky na integritu dat dle matice dopadů.		

Služby v rámci jednotlivých úrovní eGC musí být nabízeny tak, aby mohly zajistit všechny parametry (dostupnost, důvěrnost, integrita) v dané úrovni dopadu. *Příklad: Pokud je IS v parametru dostupnost hodnocen úrovní 3-vysoká, v důvěrnosti 2-střední, v integritě 1-nízká, je zařazena do úrovně bezpečnosti eGC „vysoká“.* V případě, že by nabízené služby (v oblasti integrity a důvěrnosti) zákazník v některém aspektu plně nevyužil, může s poskytovatelem jednat o modifikaci služby a získání slevy.

6.5 Závěr

Výsledky z provedeného hodnocení dopadů jsou pro správce IS vodítkem, jakou úroveň bezpečnostních opatření by měl interně zajistit, popř. vyžadovat v případě využití služeb eGC. Zároveň by tyto výsledky měly správci pomoci při rozhodování, zda a za jakých podmínek může informační systém migrovat do eGC a jakou úroveň bezpečnosti eGC služeb požadovat.

6.6 Vodítka pro hodnocení dopadů

Pro posouzení závažnosti dopadů způsobených narušením dostupnosti informačního systému veřejné správy, narušením důvěrnosti a integrity zpracovávaných dat jsou stanoveny následující oblasti dopadů.

A. Bezpečnost a zdraví osob
B. Ochrana osobních údajů
C. Zákonné a smluvní povinnosti
D. Trestně-právní řízení

E. Veřejný pořádek
F. Mezinárodní vztahy
G. Řízení a provoz organizace
H. Ztráta důvěryhodnosti
I. Finanční ztráty
J. Zajišťování nezbytných služeb

Závažnost dopadů je v každé z kategorií rozdělena do 4 úrovní dopadů (nízký, střední, vysoký a kritický). Matice dopadů je vytvořena tak, aby si úrovně (závažnosti) dopadů v jednotlivých kategoriích navzájem odpovídaly (byly přiměřeně korelovatelné). V případě, že je pro konkrétní případ hodnocení bezpečnosti dat poplatných více kategorií dopadů (např. je relevantní *Narušení bezpečnosti a zdraví osob* a *Ochrana osobních údajů*) použije se pro výsledné stanovení závažnosti dopadu nejvyšší dosažená hodnota v každém jednotlivém hodnoceném parametru bezpečnosti.

Pro další výklad a příklady použití jednotlivých oblastí dopadů se odkazujeme na Metodiku k vodítkům pro hodnocení dopadů v1.2 z března 2018 (publikovaná na webu NÚKIB viz https://www.govcert.cz/cs/kyberneticky-zakon/podpurne-materialy/).

Vodítka pro určení závažnosti dopadů narušení bezpečnosti informací (převzato z publikované metodiky NÚKIB v1.2 z března 2018)

Regulace odpovídající úrovni dopadu	Úroveň dopadu	Vodítka (oblasti) pro určení závažnosti dopadů narušení bezpečnosti informací (dostupnost, důvěrnost, integrita)									
		A. Bezpečnost a zdraví osob	B. Ochrana osobních údajů	C. Zákonné a smluvní povinnosti	D. Trestně-právní řízení	E. Veřejný pořádek	F. Mezinárodní vztahy	G. Řízení a provoz organizace	H. Ztráta důvěryhodnosti	I. Finanční ztráty	J. Zajišťování nezbytných služeb
Ostatní, ISVS, GDPR, ZKB - VIS, ISZS, ZKB - KII, ISZS	1 nízká	*žádné vodítko*	Může způsobit porušení etických, nikoli však právních předpisů vedoucí k negativním osobním dopadům na jednotlivce nebo skupinu osob.	Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	*žádné vodítko*	*žádné vodítko*	*žádné vodítko*	Naruší řádné řízení nebo fungování části nebo celé organizace.	Může negativně ovlivnit vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání.	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	*žádné vodítko*
	2 střední	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) jedné nebo několika osob.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2 % celkového ročního obratu - viz čl. 83/4 GDPR).	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody.	Může vytvořit podmínky pro páchání trestné činnosti nebo může ztížit její vyšetřování.	Může zapříčinit rozsahem, formou nebo místem omezené protesty (lokální nepokoje).	Může vytvářet negativní obraz ČR v jednom teritoriu, popř. v jednom státě.	Může omezit provádění důležitých činností organizace.	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá.	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05 % a 2 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit závažné omezení či narušení nezbytných služeb pro malé množství osob.
	3 vysoká *	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na velkou skupinu osob (pokuta až 20 mil. EUR nebo 4 % celkového ročního obratu - viz čl. 83/5 GDPR).	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	Může vést k narušení vyšetřování trestné činnosti nebo soudní řízení (méně závažná kriminalita, krátkodobě, v jednotlivých případech).	Může zapříčinit rozsahem, formou nebo místem omezené protesty na úrovni významné části správního území obce s rozšířenou působností, jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	Může vytvářet negativní obraz ČR ve světě.	Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.	Může přímo nebo nepřímo vést ke ztrátám vyšším než 2 % a nižším či rovným 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).Pozn. v případě PZS je hranice ztráty stanovena na 0,25 % HDP.	Může způsobit závažné omezení, narušení či nedostupnost nezbytných služeb pro více než 25 000 osob (v rámci kategorie provozovatelů základních služeb se může lišit dle právní úpravy pro jednotlivá odvětví viz vyhláška č. 437/2017 Sb.).
	4 kritická **	Může vést k přímému ohrožení či ztrátě života skupiny osob.	*žádné vodítko*	*žádné vodítko*	Může vést k závažnému, dlouhodobému narušení schopnosti vyšetřovat trestnou činnost, popřípadě zpochybnění soudních řízení a rozhodnutí (závažná kriminalita, celkové zpochybnění systému).	Může zapříčinit hromadné nepokoje, např. generální stávku, nebo jinak závažně narušit veřejný pořádek s celostátními dopady.	Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobit nevýhodu pro zájmy ČR.	Může závažně a dlouhodobě ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti.	Závažně a dlouhodobě ovlivní vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti.	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).Pozn. v případě KII je hranice ztráty stanovena na 0,5% HDP.	Může způsobit rozsáhlé omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
31. 7. 2020	1.0	Odb. regulace	Vytvoření dokumentu