NÚKIB

Průvodce požadavky bezpečnostní úrovně kritická

TLP:CLEAR

15. dubna 2026

Verze 1.0

Národní úřad
pro kybernetickou
a informační bezpečnost

Obsah

Seznam pojmů a zkratek

ČR	Česká republika
DIA	Digitální a informační agentura
EHP	Evropský hospodářský prostor
ESVO	Evropské sdružení volného obchodu
EU	Evropská unie
ISMS	systém řízení bezpečnosti informací
katalog	katalog cloud computingu
NÚKIB, Úřad	Národní úřad pro kybernetickou a informační bezpečnost
poskytovatel	poskytovatel služeb cloud computingu
vyhláška	vyhláška č. 505/2025 Sb., o některých požadavcích pro zápis do katalogu cloud computingu
vyhláška č. 316/2021 Sb.	vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu
zákazník	zákazník cloudových služeb
ZKB	zákon č. 264/2025 Sb., o kybernetické bezpečnosti
žádost	žádost o zápis nabídky cloud computingu do katalogu cloud computingu

1 Co se dozvím v tomto dokumentu?

Účelem tohoto dokumentu je nabídnout poskytovatelům služeb cloud computingu (dále jen „poskytovatelé“) praktickou pomůcku k orientaci v požadavcích nové vyhlášky č. 505/2025 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „vyhláška“), která nabyla účinnosti dne 1. 1. 2026. Dokument poskytovatele provází základními pojmy a postupy dokládání jednotlivých požadavků při přípravě žádosti o zápis nabídky cloud computingu do katalogu cloud computingu (dále jen „žádost“) a při následném pravidelném dokládání některých bezpečnostních požadavků po dobu evidence nabídky. Tento materiál si klade za cíl minimalizovat riziko interpretačních nejasností již od počátku účinnosti nové úpravy, usnadnit poskytovatelům přípravu úplné dokumentace a snížit tak administrativní a časovou zátěž při přípravě žádosti a celkového procesu zápisu služeb cloud computingu do katalogu cloud computingu (dále jen „katalog“). Dokument rovněž zohledňuje praktické dopady přechodného ustanovení dle § 10 vyhlášky, které do 1. 1. 2028 umožňuje ve vymezených případech dokládat splnění požadavků podle pravidel přechozí právní úpravy.

Pokud máte jakékoliv další otázky, napište nám na regulace@nukib.gov.cz.

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

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

2 Požadavky bezpečnostní úrovně Kritická

Pro lepší přehlednost a rychlou orientaci je v této kapitole uveden stručný výčet požadavků a úplné znění požadavků definovaných v příloze č. 4 vyhlášky pro bezpečnostní úroveň **kritická**.

Následující tabulka je koncipována jako přehledová matice, která obsahuje:

- **stručný popis požadavků** a
- **označení řádků požadavků a jejich bezpečnostní úroveň** (**nízká**, **střední**, **vysoká** a **kritická**)

Lokalita správy a dohledu	1.1	1.1	1.1	1.1
Zpracování zákaznických dat a specifických provozních údajů na území ČR (výjimka možná)				1.2
Povinnost odmítnout jakoukoli žádost cizího orgánu o zpřístupnění dat zákazníka				2.1
Písemný popis povinností vyplývající z legislativy zemí mimo EU/EHP (bez adequacy decision)	2.2	2.2	2.2	2.2
Oprávnění k provedení kontroly – DIA/NÚKIB	3.1	3.1	3.1	3.1
Plány kontinuity provozu a obnovy po havárii	4.1	4.1	4.1	4.1
Geografická redundance nebo odolnost datacenter	4.2	4.2	4.2	4.2
Synchronní replikace a garantovaná kapacita záložní lokality			4.3	4.3
Umístění datacenter				4.4
Nástroje pro detekci a zmírnění DDoS útoků	4.3	4.3	4.5	4.5

Vzdálená administrátorská konzole 24/7			4.6	4.6
Záznamy o přístupu k nezašifrovaným zákaznickým datům	5.1	5.1	5.1	5.1
Automatické (by default) šifrování - při všech síťových přenosech a v uložišti				5.2
Šifrování dle doporučení NÚKIB - při všech síťových přenosech a v uložišti			5.3	5.3
Certifikované HSM moduly a správa klíčů				5.4
Certifikace ISO/IEC 27001 a ISO/IEC 27017 a 27018			6.1	6.1
Auditní zpráva SOC 2 Type 2 nebo C5 Type 2			6.2	6.2
Nástroj pro sledování a vyhodnocování kybernetických událostí a zpřístupňování všech kybernetických událostí		7.1	7.1	7.1
Notifikace bezpečnostních incidentů a informování o přijatých opatřeních	7.2	7.2	7.2	7.2
Skenování zranitelností	8.1	8.1	8.1	8.1
Penetrační testování				8.2
Připojení do výměnného uzlu internetu (IXP) v ČR			9.1	9.1

2.1 Místo zpracování a uložení dat

Podstatným prvkem a zároveň rizikem při využívání služeb cloud computingu je skutečnost, že zákazník cloudových služeb (dále jen „zákazník“) předává svá data a informace poskytovateli, a může tak docházet k jejich správě, ukládání a zpracování v různých státech s odlišnými právními režimy.

2.1.1 Řádek 1.1 Lokalita správy a dohledu

Řádek 1.1	Poskytovatel uvádí informace o všech státech, z jejichž území dochází k výkonu správy a dohledu nad službou cloud computingu.

Do formuláře žádosti uveďte všechny státy, ve kterých dochází ke správě a dohledu nad službou, kterou chcete zapsat.

Dokládá se:

- písemným popisem.

2.1.2 Řádek 1.2 Zpracování zákaznických dat a specifických provozních údajů na území ČR (výjimka možná)

Řádek 1.2	Zákaznická data a specifické provozní údaje jsou zpracovávány na území České republiky. Aniž je dotčen požadavek uvedený na řádku 4.4 této přílohy, mimo území České republiky mohou být zákaznická data a specifické provozní údaje zpracovávány pouze v odůvodněných případech, po nezbytně nutnou dobu a v nezbytném rozsahu, pokud poskytovatel popíše, jak budou zákaznická data chráněna před narušením bezpečnosti informací. Poskytovatel vždy uvádí úplný výčet datových center a jejich lokace po úroveň katastrálního území nebo obce, ve kterých jsou zpracovávána zákaznická data a specifické provozní údaje, a dále v případě, že služba cloud computingu A) umožňuje splnění požadavku na zpracovávání zákaznických dat a specifických provozních údajů pouze na území České republiky, jasně označuje takovou službu cloud computingu a deklaruje závazek zpracovávání zákaznických dat a specifických provozních údajů pouze na území České republiky, B) neumožňuje splnění požadavku na zpracovávání zákaznických dat a specifických provozních údajů pouze na území České republiky, jasně označuje takovou službu cloud computingu a uvádí výčet států, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat a specifických provozních údajů, údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat a specifických provozních údajů na území příslušných států, a dále údaj o tom, zda jsou nebo nejsou zákaznická data a specifické provozní údaje pseudonymizovány v případě tohoto zpracování; dále vyžaduje souhlas zákazníka pro případy zpracování zákaznických dat a specifických provozních údajů mimo území České republiky, který je vyjádřen v samostatném dokumentu, který obsahuje výčet států, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat a specifických provozních údajů, údaj o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat a specifických provozních údajů na území příslušných států, a dále údaj o tom,

	zda jsou nebo nejsou zákaznická data a specifické provozní údaje pseudonymizovány v případě tohoto zpracování, nebo C) neumožňuje splnění požadavku na zpracovávání zákaznických dat a specifických provozních údajů pouze na území České republiky, jasně označuje takovou službu cloud computingu a uvádí výčet států, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat a specifických provozních údajů, údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat a specifických provozních údajů na území příslušných států, a dále údaj o tom, zda jsou nebo nejsou zákaznická data a specifické provozní údaje pseudonymizovány v případě tohoto zpracování; dále vyžaduje souhlas zákazníka v každém jednotlivém případě zpracování zákaznických dat a specifických provozních údajů mimo území České republiky.

Data a informace s nejzávažnějšími dopady v případě narušení jejich bezpečnosti, tedy data a informace v informačních systémech nebo jejich částech zařazených do kritické bezpečnostní úrovně, by neměla vůbec opouštět území České republiky (dále jen „ČR“). Za tímto účelem budou moci být taková data zpracovávána pouze v cloud computingu státního poskytovatele cloud computingu, jak stanoví zákon č. 365/2000 Sb., o informačních systémech veřejné správy.

Zpracování mimo ČR však nelze zakázat zcela, a proto se ponechává možnost vyžádat si od zákazníka souhlas s předáním a zpracováním zákaznických dat a specifických provozních údajů i mimo ČR. Souhlas musí být výslovný, tedy nikoliv skrytý v rámci ostatních smluvních ustanovení, ale dostatečně odsazený a zdůrazněný od ostatního textu smlouvy, popř. musí tvořit zcela samostatný dokument.

Souhlas může být udělen jako generální před zahájením využívání cloud computingu, nebo v každém jednotlivém případě. V případě generálního souhlasu musí být tento nezbytně písemný. V případě jednotlivých souhlasů musí být obecný rámec písemný, přičemž vyslovení s dílčím zpracováním mimo území ČR se může realizovat skrze prostředky pro komunikaci na dálku.

Výchozím požadavkem tohoto řádku tedy je, aby zákaznická data a specifické provozní údaje byly zpracovávány na území ČR. Mimo území ČR mohou být zákaznická data a specifické provozní údaje zpracovávány pouze v odůvodněných případech, po nezbytně nutnou dobu a v nezbytném rozsahu, pokud popíšete, jak budou zákaznická data chráněna před narušením bezpečnosti informací.

Ať zapisovaná služba zpracovává zákaznická data a specifické provozní údaje kdekoli, vždy uveďte úplný seznam data center a jejich lokace po úroveň katastrálního území nebo obce, kde jsou zpracovávána zákaznická data a specifické provozní údaje.

Mohou nastat následující situace:

A) služba výchozí požadavek **splňuje** – tuto službu jasně označte a deklarujte závazek zpracovávat zákaznická data a specifické provozní údaje pouze na území ČR **nebo**

B) služba výchozí požadavek **nesplňuje** a pro zpracování zákaznických dat a specifických provozních údajů mimo území ČR je vyžadován **generální souhlas zákazníka** – tuto službu jasně označte a dále uveďte:

   i. výčet států, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat a specifických provozních údajů,
   ii. údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat a specifických provozních údajů na území příslušných států,
   iii. údaj o tom, zda jsou nebo nejsou zákaznická data a specifické provozní údaje pseudonymizovány v případě tohoto zpracování

   a rovněž doložte, že pro případy zpracování zákaznických dat a specifických provozních údajů mimo území ČR vyžadujete od zákazníka **souhlas**, který

   i. je vyjádřen v samostatném dokumentu,
   ii. obsahuje výčet států, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat a specifických provozních údajů,
   iii. obsahuje údaj o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat a specifických provozních údajů na území příslušných států,
   iv. údaj o tom, zda jsou nebo nejsou zákaznická data a specifické provozní údaje pseudonymizovány v případě tohoto zpracování, **nebo**

C) služba výchozí požadavek **nesplňuje** a pro zpracování zákaznických dat a specifických provozních údajů mimo území ČR je vyžadován **souhlas zákazníka v každém jednotlivém případě** – tuto službu jasně označte a dále uveďte:

   i. výčet států, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat a specifických provozních údajů,
   ii. údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat a specifických provozních údajů na území příslušných států,
   iii. údaj o tom, zda jsou nebo nejsou zákaznická data a specifické provozní údaje pseudonymizovány v případě tohoto zpracování

   a rovněž doložte, že pro zpracování zákaznických dat a specifických provozních údajů mimo území ČR vyžadujete od zákazníka **souhlas v každém jednotlivém případě zpracování** zákaznických dat a specifických provozních údajů mimo území ČR.

Jak vyplývá z výše uvedeného, rozdíl mezi variantami B a C je ve formě vyžádání souhlasu se zpracováním zákaznických dat a specifických provozních údajů mimo ČR. Varianta B vyjadřuje generální souhlas zákazníka a varianta C vyjadřuje souhlas se zpracováním zákaznických dat a specifických provozních údajů mimo území ČR pro každý jednotlivý případ.

Dokládá se:

- částí auditní zprávy **a současně**
- částí smluvní dokumentace.

2.2 Žádosti o zpřístupnění a předání dat

2.2.1 Řádek 2.1 Odmítnutí žádostí o zpřístupnění dat zákazníka

Řádek 2.1	Poskytovatel v případě, že obdrží žádost cizozemských orgánů o zpřístupnění nebo předání zákaznických dat nebo specifických provozních údajů, tuto žádost odmítne a data nevydá a nezpřístupní.

Tento požadavek má za cíl poskytnout zákazníkovi jistotu, že jeho data nebudou zpřístupněna státním orgánům odlišných od státního orgánu ČR. Protože však v režimu kritické bezpečnostní úrovně musí být data trvale uložena výhradně na území ČR v rámci státního poskytovatele cloud computingu, nedostáváte se pod jurisdikci cizích států. Znamená to, že pokud obdržíte žádost cizozemského orgánu (zejména zpravodajských služeb nebo orgánů činných v trestním řízení cizích států) o zpřístupnění nebo předání zákaznických dat či specifických provozních údajů, jste oprávněni a zároveň povinni takovou žádost odmítnout a odkázat jej na příslušný orgán rozhodující o zpřístupnění dat v rámci justiční spolupráce.

Dokládá se:

- čestným prohlášením **nebo**
- smluvní dokumentací **nebo**
- částí další dokumentace **nebo**
- částí auditní zprávy.

2.2.2 Řádek 2.2 Písemný popis povinností

Řádek 2.2	Poskytovatel jasně a srozumitelně uvádí své povinnosti vyplývající z právních řádů států odlišných od členských států Evropské unie nebo odlišných od členských států Evropského hospodářského prostoru nebo u těch států, u kterých Evropská komise nerozhodla o udělení rozhodnutí o odpovídající ochraně (adequacy decision) podle článku 45 obecného nařízení o ochraně osobních údajů, na jejichž území se nalézá datové centrum nebo jiná infrastruktura, ve které dochází ke zpracování zákaznických dat nebo specifických provozních údajů podle řádku 1.2 této přílohy týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů. Tento popis musí být v takové kvalitě, aby z něj bylo možné zákazníkem posoudit vhodnost právního řádu s ohledem na zpracovávání zákaznických dat a specifických provozních údajů. Proto poskytovatel provede popis povinností obsahující informace o tom, který cizozemský orgán veřejné moci, jehož činnost spočívá v prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, zpravodajská služba, nebo jiný orgán s obdobným předmětem činnosti nebo obdobnými pravomocemi, může žádat o zpřístupnění a předání dat, za jakých podmínek může tento orgán žádat o zpřístupnění a předání dat a na jak dlouho, na jaká data se daná povinnost vztahuje a zda je možné žádost o zpřístupnění nebo předání dat přezkoumat nezávislým soudem.

Předtím, než zákazník začne využívat vaši cloudovou službu, měl by mít možnost vyhodnotit rizika spojená se zpracováním dat ve vaší infrastruktuře. Aby mohl posoudit právní prostředí, ve kterém budou data zpracovávána, musíte vy jako poskytovatel podat srozumitelný popis povinností, které pro vás vyplývají z právních řádů států mimo EU, mimo Evropský hospodářský prostor nebo u těch států, pro které Evropská komise nerozhodla o odpovídající ochraně.[1] Tento popis se týká států, na jejichž území máte datová centra nebo jinou infrastrukturu, kde zpracováváte zákaznická data či specifické provozní údaje. Zákazník musí mít k dispozici dostatek informací, aby mohl posoudit, jak právní řád daného státu ovlivňuje bezpečnost a ochranu dat a vyhodnotit rizika spojená s možnými zásahy cizích státních orgánů.

V rámci popisu uveďte, které orgány dané země mohou žádat o zpřístupnění nebo předání dat, jaké mají pravomoci, za jakých podmínek mohou takovou žádost podat, na jak dlouho mohou k datům získat přístup, jakého okruhu dat se jejich oprávnění týká a také zda existuje možnost nezávislého soudního přezkumu takové žádosti.

Dokládá se:

- písemným popisem.

[1] Jedná se o *adequacy decision* podle článku 45 obecného nařízení o ochraně osobních údajů, které je dostupné zde: Nařízení - 2016/679 - EN - GDPR - EUR-Lex

2.3 Oprávnění k provedení kontroly

V případě opakujících se kybernetických bezpečnostních incidentů poskytovatele nebo zjištění rozporu s poskytovatelem deklarovanými parametry v rámci služby cloud computingu můžete být jednou za rok kontrolováni Digitální a informační agenturou (dále jen „DIA“) nebo Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „Úřad“ nebo také „NÚKIB“). Kontrola může podle kontrolního řádu probíhat na všech místech a zařízeních souvisejících s poskytováním služby cloud computingu.

Splnění tohoto požadavku ověřuje DIA nebo Úřad z úřední činnosti samotným výkonem kontroly. Jako poskytovatel nemusíte splnění požadavku prokazovat.

2.4 Zajištění poskytování služby cloud computingu

Kategorie požadavků obsažená v řádku 4 příloh č. 1 až 4 k vyhlášce upravuje oblast **zajištění poskytování služby cloud computingu**. Cílem této skupiny požadavků je ověřit, že poskytovatel disponuje technickými a procesními mechanismy, které minimalizují riziko výpadku služby a zajišťují její obnovu v případě incidentu. Požadavky řádku 4 se soustředí zejména na plány kontinuity provozu (BCP), plány obnovy (DRP), geografickou redundanci datových center a technickou připravenost infrastruktury pro řešení krizových situací.

2.4.1 Řádek 4.1 Plány kontinuity provozu a obnovy po havárii

Řádek 4.1	Poskytovatel má vyhotoven a udržuje plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu.

Požadavek tohoto řádku má ověřit, že jakožto poskytovatel disponujete funkčním, pravidelně testovaným a aktualizovaným systémem zajištění kontinuity provozu a obnovy po havárii. Plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu jsou nástroje sloužící k zajištění dostupnosti. Zákazník musí být schopen posoudit, jak bude s jemu poskytovanou službou cloud computingu zacházeno poskytovatelem v případě nenadálé či krizové situace. Na základě tohoto posouzení si zákazník vypracuje vlastní plány zajišťující provoz služby cloud computingu z pohledu provozu celého informačního systému veřejné správy. Aby byl zákazník schopen uvedeného posouzení, je třeba, aby měl poskytovatel takové plány vůbec vytvořeny.

Ačkoliv spolu oba dokumenty úzce souvisejí a tvoří jeden celek pro řízení kontinuity, každý se zaměřuje na jinou fázi krizového stavu:

- **plán zajištění kontinuity provozu (BCP – Business Continuity Plan)** se zaměřuje na to, jak udržet klíčové aspekty služby v chodu **během** incidentu. Zejména řeší procesy, lidské zdroje, alternativní komunikační kanály a náhradní způsoby fungování tak, aby zákazník pociťoval co nejmenší dopad.

- **plán na obnovu po havárii (DRP – Disaster Recovery Plan)** je techničtěji zaměřen a řeší, jak obnovit IT infrastrukturu a data do plně funkčního stavu **po** havárii. Zejména obsahuje konkrétní kroky pro obnovu serverů z archivních kopií, zprovoznění záložních datových center a ověření integrity dat. DRP rovněž typicky obsahuje informaci o maximální přijatelné době obnovy (RTO – Recovery Time Objective) a maximální přijatelné ztrátě (RPO – Recovery Point Objective) pro danou službu, pokud tyto informace nejsou již obsaženy v jiných dokumentech (typicky SLA).

Tyto dokumenty musí být dostatečně konkrétní a musí pokrývat scénáře narušení bezpečnosti a dostupnosti služby. Pokud plány obsahují vysoce citlivé technické údaje (např. konkrétní IP adresy, jména pracovníků nebo detailní konfigurace), které nechcete zveřejňovat, lze tyto údaje v nezbytné míře začernit. Dokument však i po těchto úpravách musí zůstat srozumitelný a musí z něj být patrné, že procesy jsou reálně nastaveny.

Dokládá se:

- plánem zajištění kontinuity provozu a plánem na obnovu po havárii **nebo**
- auditní zprávou podle § 7 odst. 1 vyhlášky.

2.4.2 Řádek 4.2 Geografická redundance nebo odolnost datacenter

Řádek 4.2	Poskytovatel vždy zajišťuje primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, a uvádí úplný výčet datových center, ze kterých je služba cloud computingu poskytována, a jejich lokace po úroveň katastrálního území nebo obce a dále zajišťuje, že A) tato datová centra jsou v dostatečné vzdálenosti od přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací, nebo že je přijato adekvátní bezpečnostní opatření, nebo B) se tato datová centra nacházejí ve vzájemné vzdálenosti nejméně 50 km a u obou datových center je navržena a aplikována fyzická ochrana proti přírodním katastrofám, úmyslnému útoku nebo haváriím.

Tento požadavek je zaměřen na ochranu fyzické infrastruktury datových center, ze kterých je poskytována služba cloud computingu tak, aby byla chráněna před vnějšími vlivy a byla tak zachována dostatečná dostupnost služby cloud computingu. Cílem tohoto požadavku je eliminovat riziko vzniku tzv. jediného bodu selhání (Single Point of Failure) na úrovni datového centra. Je třeba mít jistotu, že i v případě výpadku primární lokality jste schopni zajistit kontinuitu služby z lokality jiné.

Tento požadavek lze rozdělit do více částí. První je obecná část požadavku, která vyžaduje potvrzení existence primárního a alespoň jednoho datového centra kapacitně dostatečného k převzetí služby a výčet všech datových center včetně jejich přesné lokace. V druhé (zvláštní) části požadavku jsou poskytovateli dány dvě možnosti, kterými může doložit zajištění geografické odolnosti. Níže je požadavek rozebrán podrobněji.

Obecná část požadavku

Základní podmínkou obecného požadavku je zajištění **primárního a alespoň jednoho záložního datového centra**. Vyhláška striktně vyžaduje, aby záložní datové centrum bylo **kapacitně dostatečné** k plnému převzetí provozu za datové centrum primární. Za primární a záložní datové centrum lze považovat dvě redundantní datová centra, kdy z obou z nich je poskytovatel schopen zajistit funkčnost služby cloud computingu.

Dále je nutné **identifikovat všechna datová centra,** která se podílejí na poskytování dané služby. Výčet tedy nesmí obsahovat pouze primární a záložní datové centrum, ale veškeré lokality, kde dochází k běhu služby nebo uložení dat. Vyhláška vyžaduje uvádět lokaci všech datových center **minimálně na úroveň obce nebo katastrálního území**. Pro účely zápisu tedy není dostačující uvést pouze kraj nebo jiné obecné označení lokality. Tato úroveň detailu slouží k tomu, aby mohla být objektivně posouzena rizikovost dané oblasti (např. povodňová území, seizmické zóny).

Zvláštní část požadavku

V druhé části tohoto požadavku je nutné prokázat, že zvolené lokality jsou od sebe dostatečně geograficky odděleny, aby nebyly ohroženy stejným zdrojem rizika. Volíte si zde jednu ze dvou následujících variant:

Varianta A

Tato varianta je určena pro situace, kdy mezi datovými centry navzájem není dostatečný vzdálenostní odstup, a proto je třeba využít individuální posouzení lokality a vzdálenosti od přírodních zdrojů rizik a rizik vyvolaných činností člověka. V rámci této varianty musíte prokázat jednu z následujících skutečností:

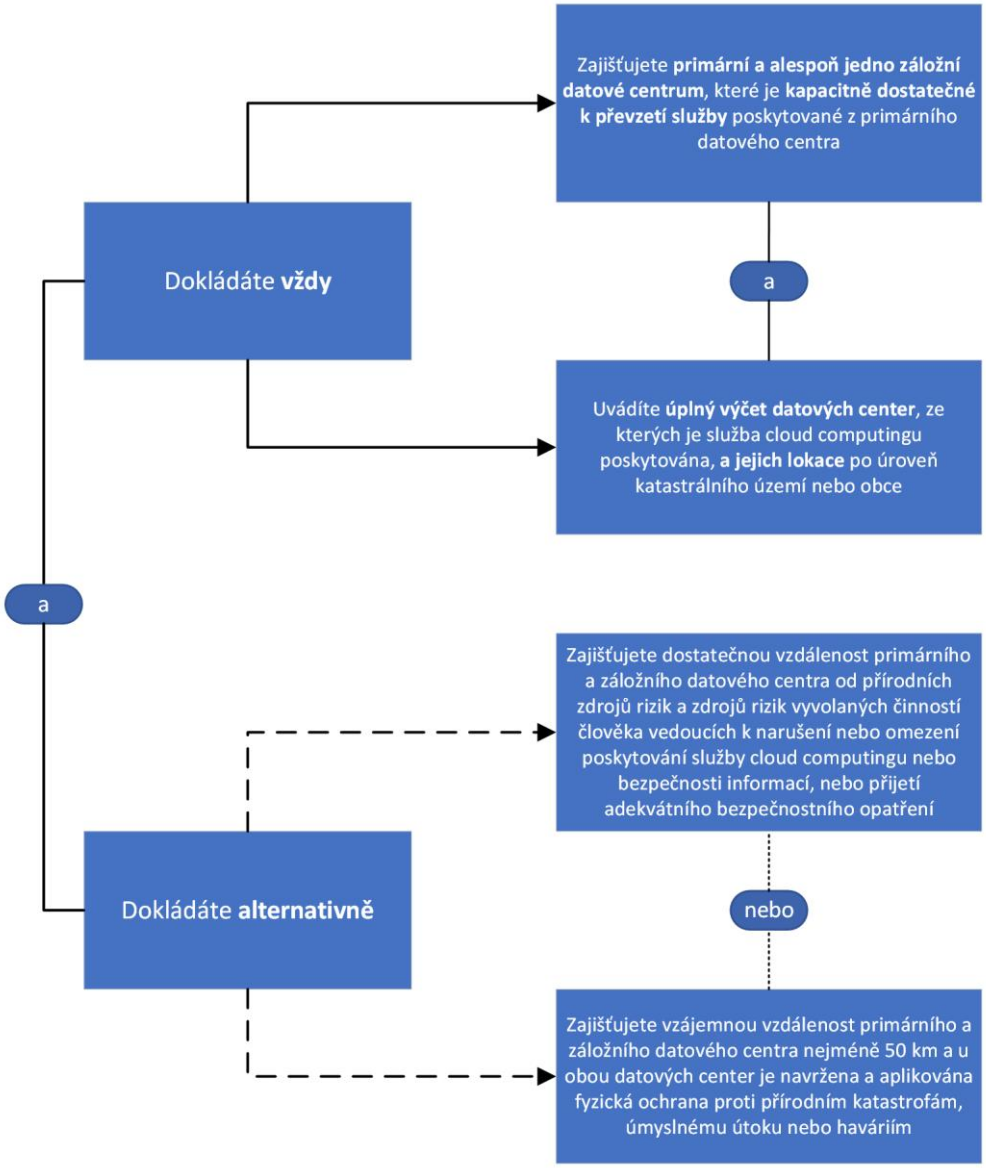
- **dostatečná vzdálenost od přírodních zdrojů rizik a rizik vyvolaných aktivitou člověka** vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací **nebo**
- **přijetí adekvátních bezpečnostních opatření,** kdy je třeba prokázat, že byť se datová centra nacházejí v blízkosti potenciálního zdroje rizika, byla přijata taková technická nebo organizační opatření, která toto konkrétní riziko eliminují.

Varianta B

Tato varianta využívá pevně stanovený minimální rozestup mezi datovými centry, kdy lze s rostoucí vzájemnou vzdáleností předpokládat snižující se pravděpodobnost jejich vystavení stejným zdrojům rizik. V rámci této varianty musíte prokázat následující skutečnosti:

- **datová centra se nacházejí ve vzájemné vzdálenosti nejméně 50 km vzdušnou čarou** a
- **u obou datových center je navržena a aplikována fyzická ochrana** proti přírodním katastrofám, úmyslnému útoku nebo haváriím.

Pro úspěšné splnění požadavku je tedy třeba vždy doložit splnění všech náležitostí části obecné, tedy potvrdit existenci primárního a alespoň jednoho datového centra kapacitně dostatečného k převzetí služby a doložit výčet všech datových center včetně jejich přesné lokace. Dále musí být splněna jedna z variant A nebo B v druhé části požadavku. Ve formuláři žádosti jasně uveďte, jakou z variant splňujete, a u všech podkladů se držte obecného postupu pro dokládání požadavků popsaného v úvodním dokumentu tohoto průvodce.



Dokládá se:

- částí smluvní dokumentace **nebo**
- částí další dokumentace **nebo**
- částí auditní zprávy **a současně**
- zprávou nebo jiným dokladem o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka, který obsahuje náležitosti uvedené v příloze č. 7 vyhlášky, ze kterého vyplývá splnění požadavku podle varianty A, **nebo**
- částí auditní zprávy, ze které vyplývá splnění požadavku podle varianty B.

2.4.3 Řádek 4.3 Synchronní replikace a garantovaná kapacita záložní lokality

Řádek 4.3	Poskytovatel umožňuje synchronní replikaci dat alespoň do jednoho záložního datového centra, které je kapacitně dostatečné k převzetí služby cloud computingu poskytované z primárního datového centra.

Tento požadavek má za cíl ověřit, že jako poskytovatel služby cloud computingu disponujete alespoň jedním záložním datovým centrem, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra a že jste schopen zákazníkovi nabídnou funkci synchronní (okamžité, real-time) replikace dat do tohoto kapacitně dostatečného záložního datového centra.

Synchronní replikací dat se rozumí zápis dat v reálném čase současně do primárního i záložního datového centra. Jejím účelem je, aby v případě potřeby bylo možné přenést poskytování služby cloud computingu z primárního do záložního datového centra, a byla tak zachována kontinuita poskytování služby cloud computingu.

Z hlediska systematiky vyhlášky se v tomto případě jedná o **požadavek na dostupnost funkce**, nikoliv na její automatické zajištění. Postačí tedy prokázat, že služba funkcionalitu synchronní replikace dat umožňuje. Její aktivace je však ponechána na zákazníkovi.

Dokládá se:

- částí smluvní dokumentace **nebo**
- částí další dokumentace **nebo**
- částí auditní zprávy.

2.4.4 Řádek 4.4 Umístění datacenter

Řádek 4.4	Poskytovatel uvádí úplný výčet datových center, ze kterých je služba cloud computingu poskytována, a jejich lokace po úroveň katastrálního území nebo obce a dále zajišťuje, že primární i všechna záložní datová centra, ze kterých je poskytována služba cloud computingu, se nacházejí v České republice, vyjma případů výslovného písemného svolení zákazníka s ukládáním zákazníkem zašifrovaných zákaznických dat ve stavu neaktivních dat na území jiného členského státu Evropské unie a členského státu Evropského sdružení volného obchodu.

Ve službách cloud computingu zařazených do bezpečnostní úrovni kritická jsou zpracovávána nejcitlivější data státu, z tohoto důvodu byl zaveden požadavek na to, aby datová centra, z nichž je služba cloud computingu poskytována, se všechna nacházela na území ČR. Cílem je eliminovat rizika spojená např. s neočekávanými geopolitickými změnami v cizích jurisdikcích, které by mohly mít negativní dopad na dostupnost a provoz datových center.

Z hlediska systematiky vyhlášky se v tomto případě jedná o **požadavek na zajištění,** nikoliv na dostupnost pro zákaznika. Jako poskytovatel tedy musíte prokázat, že vaše infrastruktura toto kritérium **automaticky a trvale splňuje.**

Aby byl požadavek tohoto řádku splněn, musíte doložit úplný výčet datových center, ze kterých bude služba cloud computingu poskytována, včetně jejich lokace po úroveň katastrálního území nebo obce. Všechna tato datová centra se přitom musí nacházet na území ČR.

Výjimku představují situace, kdy zákazník udělí výslovný písemný souhlas s uložením zákaznických dat ve stavu neaktivních dat v datovém centru umístěném na území jiného členského státu EU nebo ESVO. V tomto případě však musí být veškerá zákaznická data ve stavu neaktivních dat zašifrována.

Dokládá se:

- částí auditní zprávy.

2.4.5 Řádek 4.5 Nástroje pro detekci a zmírnění DDoS útoků

Řádek 4.5	Poskytovatel je schopen poskytovat nástroj nebo službu pro detekci a zmírnění útoků typu odepření služby (DoS/DDoS) jak na síťové, tak aplikační úrovni. Poskytovatel se zavazuje, že předá zákaznická data a specifické provozní údaje cizozemskému orgánu pouze, pokud z právního posouzení vyšlo, že žádost cizozemského orgánu má proveditelný, aplikovatelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat nebo specifických provozních údajů je přiměřený účelu žádosti. O podkladech sloužících k přezkoumání zákonnosti žádosti poskytovatel provede záznam, který uchová alespoň 5 let pro účely kontroly nebo ho prokazatelně předá zákazníkovi.

Požadavek tohoto řádku se zaměřuje na schopnost poskytnout zákazníkům ochranu proti útokům typu odepření služby (DoS/DDoS). Pro jeho správné doložení je klíčové pochopit, že se jedná

o **požadavek na dostupnost funkce**, nikoliv na její automatické zajištění. Stačí tedy prokázat, že v rámci poskytované služby **nabízíte nástroje**, které **detekci a zmírnění (mitigaci)** těchto útoků umožňují. Aktivace je pak na zákazníkovi.

Z doložených podkladů tedy musí být jasně patrné, že služba nabízí nástroje pro detekci a zmírnění útoků DoS/DDoS a že je tato ochrana k dispozici jak na síťové, tak aplikační úrovni.

Dokládá se:

- částí smluvní dokumentace **nebo**
- částí další dokumentace **nebo**
- částí auditní zprávy.

2.4.6 Řádek 4.6 Vzdálená administrátorská konzole 24/7

Řádek 4.6	Poskytovatel umožňuje obsluhu služby cloud computingu pomocí administrátorské konzole vzdáleně přístupné zákazníkovi v nepřetržitém režimu.

Tento požadavek je zaměřen na umožnění zákazníkovi danou službou cloud computingu spravovat na dálku v nepřetržitém režimu. Z hlediska systematiky vyhlášky se jedná o **požadavek na dostupnost funkce**. Poskytovatel tedy musí prokázat, že takový nástroj nabízí a umožňuje jeho využití, přičemž konkrétní způsob nasazení a rozsah oprávnění je předmětem ujednání mezi poskytovatelem a zákazníkem.

Aby byl požadavek považován za splněný, musí vámi nabízený nástroj zákazníkovi splňovat následující atributy:

- **obsluha služby pomocí administrátorské konzole:** tímto nástrojem se rozumí management portál, grafické uživatelské rozhraní (GUI), rozhraní pro programování aplikací (API) nebo nástroje příkazového řádku (CLI), které umožňují aktivní správu a konfiguraci instancí služby. Tento nástroj nesmí sloužit pouze k pasivnímu nahlížení na stav služby, ale musí zákazníkovi umožňovat pružně reagovat na jakékoliv nutné události a provozní jevy (např. změna konfigurace, správa uživatelských oprávnění nebo škálování zdrojů) spojené s poskytováním služby cloud computingu.
- **dálková přístupnost:** administrátorská konzole musí být navržena tak, aby umožňovala plnohodnotnou správu služby prostřednictvím vzdáleného přístupu. Tato dálková přístupnost eliminuje nutnost fyzické přítomnosti personálu zákazníka v prostorách datových center poskytovatele a zajišťuje operativnost správy z pracoviště orgánu veřejné správy.
- **nepřetržitý režim:** garance, že zákazník může provést bezpečnostní nebo provozní zásahy v jakémkoliv okamžiku, což je nezbytné pro zachování kontinuity provozu informačních systémů veřejné správy i mimo běžnou pracovní dobu.

Aby byl požadavek tohoto řádku splněn, musíte tedy doložit, že jste jako poskytovatel služby cloud computingu schopen nabídnout zákazníkovi funkcionalitu umožňující obsluhu služby cloud computingu pomocí administrátorské konzole, která je zákazníkovi přístupna vzdáleně a v nepřetržitém režimu.

Dokládá se:

- částí smluvní dokumentace **nebo**
- částí další dokumentace.

2.5 Nakládání s daty

Šifrování v cloudových službách představuje bezpečnostní mechanismus, který chrání citlivá data uložená nebo přenášená v rámci cloudové infrastruktury. Data jsou převáděna do podoby, kterou lze číst pouze s odpovídajícím kryptografickým klíčem.

Mnoho poskytovatelů umožňuje také správu vlastních klíčů (tzv. BYOK – Bring Your Own Key), což zákazníkům poskytuje vyšší míru kontroly nad ochranou dat. Celkově je šifrování jedním ze základních prvků, který posiluje důvěru v cloudová řešení a podporuje bezpečný provoz cloudových služeb.

2.5.1 Řádek 5.1 Záznamy o přístupu k nezašifrovaným zákaznickým datům

Řádek 5.1	Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo v daném případě bez přechozího svolení zákazníka. Tento záznam musí obsahovat alespoň důvod, čas, trvání, typ a rozsah přístupu a dostatek dalších údajů potřebných k tomu, aby mohl zákazník vyhodnotit rizikovost tohoto přístupu. Poskytovatel umožňuje zákazníkovi přístup k tomuto záznamu, a za tím účelem jej uchovává alespoň po dobu 7 dní. Poskytovatel nemusí umožňovat přístup k záznamu v případě, že interní a externí pracovníci přistupují k nezašifrovanému zákaznickému obsahu na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat a vyrozumění zákazníka o této žádosti není možné v souladu s bodem 2.1 této přílohy. Pokud poskytovatel nemá zaveden proces pro přístup jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům bez předchozího svolení zákazníka, tento požadavek se neuplatní. Každý přístup k nezašifrovaným zákaznickým datům, ke kterému dojde bez předchozího svolení zákazníka, se pak považuje za narušení bezpečnosti informací dle řádku 7.2 této přílohy a poskytovatel postupuje v souladu s tímto požadavkem.

Požadavek míří na situace, kdy jako poskytovatel přistoupíte k zákaznickým datům z legitimních, smlouvou předvídaných, důvodů, např. servisní zásah v konkrétním případě bez předchozího souhlasu zákazníka. V takovém případě pak nepůjde o neoprávněný, nýbrž oprávněný přístup a požadavek má za cíl zajistit zákazníkovi (správci těchto dat) transparentnost takových přístupů.

Oproti úpravě ve vyhlášce č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „vyhláška č. 316/2021 Sb.“), nyní vyhláška připouští variantu neexistence zavedeného procesu pro přístup interních nebo externích zaměstnanců k nezašifrovaným datům zákazníka.

Pokud nemáte zavedený proces pro přístup svých interních a externích pracovníků k nezašifrovaným zákaznickým datům bez předchozího svolení zákazníka, považuje se každý takový přístup za narušení bezpečnosti informací. Není tedy možné situaci vyhodnocovat jako běžný provozní úkon, ale musíte ji hodnotit jako kybernetický bezpečnostní incident a v souladu s požadavkem řádku 7.2 notifikovat zákazníka. Absence procesu tedy neosvobozuje od povinností, naopak vede k přísnější klasifikaci každého neoprávněného přístupu.

Dokládá se:

- částí smluvní dokumentace **nebo**
- částí další dokumentace **nebo**
- částí auditní zprávy.

2.5.2 Řádek 5.2 Automatické (by default) šifrování při všech síťových přenosech a v úložišti

Řádek 5.2	Poskytovatel vždy chrání zákaznický obsah šifrováním při všech síťových přenosech a v úložištích ve službě cloud computingu.

Doložte, že vždy chráníte zákaznický obsah šifrováním při všech síťových přenosech a v úložištích ve službě cloud computingu.

Za přenos při všech síťových přenosech se považuje veškerá komunikace, která probíhá v rámci vaší vlastní infrastruktury[2] a mimo ni[3].

Šifrováním v úložištích se rozumí situace, kdy jsou data na discích šifrována. Nevyjadřuje to úroveň šifrování (úložištěm vs. operačním systémem vs. aplikací).

Dokládá se:

- částí smluvní dokumentace **nebo**
- částí další dokumentace **nebo**
- částí auditní zprávy.

[2] Například přenosy mezi servery nebo diskovými poli v rámci jednoho datacentra.
[3] Typicky jde o přenosy mezi uživateli a cloudovou službou nebo o jakoukoliv komunikaci přes veřejný internet.

2.5.3 Řádek 5.3 Šifrování dle doporučení NÚKIB při všech síťových přenosech a v úložišti

Řádek 5.3	Poskytovatel zákazníkovi umožňuje ochranu zákaznického obsahu šifrováním při všech síťových přenosech a v úložištích ve službě cloud computingu pomocí některého ze schválených algoritmů uvedených v aktuálně platném doporučení v oblasti kryptografických prostředků vydaném v souladu s nejlepší praxí Národním úřadem pro kybernetickou a informační bezpečnost, které je zveřejněno na jeho internetových stránkách, v rámci celé šifrovací sady. V případě, že poskytovatel nabízí šifrovací sady, které obsahují takové algoritmy, které nejsou schválené v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost, poskytovatel umožní zákazníkovi výběr těch šifrovacích sad, které aplikují algoritmy schválené v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost.

Tento požadavek má za cíl ověření kryptografického nastavení vaší služby a vztahuje se jak na data v úložištích cloudové služby, tak na šifrování při všech síťových přenosech. V těchto situacích je šifrování nezbytné k zajištění integrity, důvěrnosti a autenticity komunikace. Autenticita je přímo závislá na řádném procesu autentizace, kterým dochází k ověření identity komunikujících stran. Princip důvěrnosti a integrity platí i pro data uložená v úložištích — jejich šifrování chrání obsah i v případě fyzického odcizení nosičů nebo selhání jiných bezpečnostních opatření.

Aby bylo možné požadavek správně doložit, je nutné pracovat s následující terminologií:

- **šifrovací sada (Cipher Suite):** jde o ucelenou kombinaci kryptografických algoritmů, které společně zajišťují bezpečnost komunikace nebo uložení dat. Sada obvykle určuje algoritmus pro výměnu klíčů, autentizaci, vlastní šifrování a kontrolu integrity. Pro účely tohoto průvodce rozumíme šifrovací sadou i doplňující bezpečnostní parametry, které mají vliv na úroveň ochrany (např. délka klíče, mód šifrování).
- **kryptografický algoritmus:** jedná se o postup použitý k zajištění ochrany informací (např. AES, ChaCha20). Úřad ve svém doporučení neschvaluje celé protokoly (jako TLS nebo SSH), ale právě tyto konkrétní algoritmy v nich obsažené.

Tento požadavek vám ukládá povinnost nabízet schválené kryptografické algoritmy v rámci celého řetězce šifrovací sady. Samotná identifikace protokolu bez další specifikace neposkytuje dostatečnou informaci o skutečné úrovni zabezpečení. Protokoly představují pouze technický rámec, jehož výsledná odolnost je přímo závislá na konkrétních kryptografických algoritmech zvolených v rámci jeho vnitřního nastavení. Vaší povinností je proto uvést technické parametry zabezpečení, tedy nejen specifikovat použitý algoritmus, ale rovněž jeho parametry, jako jsou délky klíčů a konkrétní operační módy šifrování. V případě, že ze zápisu šifrovací sady nelze posoudit některý z parametrů (například autenticitu u nativních algoritmů TLS 1.3), uveďte tuto informaci zvlášť.

Příklady šifrovacích sad pro protokol TLS

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Příklady šifrovacích sad pro šifrování v úložištích

- AES-256-XTS
- AES-256-EME2
- Camellia-256-XTS

Pokud ve své službě podporujete více šifrovacích sad a některá z nich není schválená v doporučení NÚKIB[4] (např. z důvodu zpětné kompatibility), je nezbytné, abyste jasně označili ty sady, které splňují aktuální doporučení NÚKIB a abyste umožnili zákazníkovi jejich výběr. Zatímco konečná volba konfigurace je na zákazníkovi, vy odpovídáte za to, že bezpečné možnosti budou jasně identifikované a technicky dostupné. Pro úspěšné doložení splnění tohoto požadavku tedy jasně definujte alespoň jednu kompletní šifrovací sadu pro ukládání dat a jednu kompletní šifrovací sadu pro šifrování obsahu při přenosu, a to v souladu s doporučením NÚKIB a včetně uvedení technických parametrů použitého zabezpečení.

Dokládá se:

- částí smluvní dokumentace **nebo**
- částí další dokumentace **nebo**
- částí auditní zprávy.

[4] Minimální požadavky na kryptografické algoritmy – Doporučení v oblasti kryptografické bezpečnosti je dostupné zde: doporuceni-kryptograficka-bezpecnost-v4-1_uid_69a8216e3deb1.pdf

2.5.4 Řádek 5.4 Certifikované HSM moduly a správa klíčů

Řádek 5.4	Poskytovatel umožňuje uložení šifrovacích klíčů v certifikovaném hardware security modulu (HSM modulu) úrovně ochrany FIPS 140-2 level 2 a vyšší, FIPS 140-3 level 2 a vyšší nebo certifikaci podle Common Criteria Protection Profile (PP) EN 419 221-5 minimálně na EAL4 a vyšší, který je pod vzdálenou správou zákazníka nebo instalaci HSM modulu zákazníka do infrastruktury poskytovatele. Poskytovatel dále umožňuje bezpečnou likvidaci kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM modulu) řízenou zákazníkem a, v případě, že umožňuje uložení šifrovacích klíčů v certifikovaném HSM modulu, který je pod vzdálenou správou zákazníka, zajišťuje likvidaci vrchního přístupového klíče při ukončení služby cloud computingu, nebo, v případě, že umožňuje instalaci HSM modulu zákazníka do infrastruktury poskytovatele, umožňuje likvidaci vrchního přístupového klíče při ukončení služby cloud computingu.

Pro splnění tohoto požadavku doložte, že umožňujete zákazníkovi uložení šifrovacích klíčů do certifikovaného HSM modulu pod vzdálenou správou zákazníka nebo zákazníkovi umožňujete instalaci jeho vlastního HSM modulu do vaší infrastruktury.

Druhá část požadavku se váže k povinnosti umožnit bezpečnou likvidaci kryptografických klíčů uložených v HSM modulu řízenou zákazníkem. Postup se odvíjí od první části požadavku:

- u certifikovaného HSM modulu pod vzdálenou správou zákazníka – zajistěte likvidaci vrchního přístupového klíče při ukončení služby cloud computingu **nebo**
- u instalace vlastního HSM modulu zákazníka – umožněte likvidaci vrchního přístupového klíče při ukončení služby cloud computingu.

Dokládá se:

- částí smluvní dokumentace **nebo**
- částí další dokumentace.

2.6 Certifikace služby cloud computingu

2.6.1 Řádek 6.1 Certifikace ISO/IEC 27001 a ISO/IEC 27017 a 27018

Řádek 6.1	Poskytovatel je držitelem platné certifikace podle ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), do jejíhož rozsahu náleží posuzovaná služba cloud computingu provozovaná v souladu s postupy normy ČSN ISO/IEC 27017, ČSN EN ISO/IEC 27017 nebo ISO/IEC 27017 a v souladu s postupy normy ČSN ISO/IEC 27018, ČSN EN ISO/IEC 27018 nebo ISO/IEC 27018.

Pro splnění tohoto požadavku je třeba předložit, že jste držitelem daného platného certifikátu. Držitelem platné certifikace musíte být po celou dobu, kdy cloudovou službu zákazníkům nabízíte, a z tohoto důvodu je rovněž vaší povinností pravidelně dokládat, že certifikaci služby obnovujete.

Nejpozději dva měsíce po skončení platnosti certifikátu doložte DIA certifikát nový. Tato povinnost pravidelného dokládání je popsána v příloze č. 5 vyhlášky.

Společně s certifikátem doložte i k němu příslušné prohlášení o aplikovatelnosti.

Pokud certifikát jmenovitě neuvádí zapisovanou službu, je nutné tento nedostatek zhojit doložením čestného prohlášení, ve kterém potvrdíte, že daná služba náleží do rozsahu předloženého certifikátu.

Dokládá se:

- platným certifikátem **a současně**
- prohlášením o aplikovatelnosti náležejícím k danému certifikátu **a současně**
- čestným prohlášením (pokud nejsou v rozsahu předkládaného certifikátu uvedeny jmenovitě všechny zapisované služby).

2.6.2 Řádek 6.2 Auditní zpráva SOC 2 Type 2 nebo C5 Type 2

Řádek 6.2	Poskytovatel je držitelem auditní zprávy SOC 2® Type 2 nebo auditní zprávy o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue (C5), a to ve formě Type 2, kdy tato auditní zpráva je vždy vydaná na poskytovateli nezávislým auditorem, není ke dni podání žádosti o zápis nabídky cloud computingu do katalogu cloud computingu starší než 24 měsíců a do jejíhož rozsahu jmenovitě náleží posuzovaná služba cloud computingu.

Cílem požadavku je ověřit, že jste držitelem

- auditní zprávy SOC 2® Type 2 v doménách bezpečnosti, dostupnosti, procesní integrity, důvěrnosti a soukromí **nebo**
- auditní zprávy o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue (C5), a to ve formě Type 2,

kdy tato auditní zpráva, nehledě na vaší volbě, není ke dni podání žádosti o zápis starší než 24 měsíců.

V souladu s povinností pravidelného dokládání (podle přílohy č. 5 vyhlášky) každých 24 měsíců evidence služby v katalogu předkládejte DIA auditní zprávu, která není ke dni podání starší než 24 měsíců.

Pokud auditní zpráva jmenovitě neuvádí zapisovanou službu, je namístě tento nedostatek zhojit doložením čestného prohlášení, ve kterém potvrdíte, že daná služba náleží do rozsahu předložené auditní zprávy.

Dokládá se:

- auditní zprávou **a současně**
- čestným prohlášením (pokud nejsou v rozsahu předkládané auditní zprávy uvedeny jmenovitě všechny zapisované služby).

2.7 Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty

2.7.1 Řádek 7.1 Sledování, vyhodnocování a zpřístupňování kybernetických událostí

Řádek 7.1	Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí. Poskytovatel umožňuje zákazníkovi vzdálený přístup k informacím o všech událostech týkajících se daného zákazníka. Nové události zpřístupní poskytovatel zákazníkovi bez zbytečného odkladu.

Sledování bezpečnostních událostí, jejich vyhodnocování a následné předávání informací o nich, je pro zákazníka nezbytné s ohledem na přijímání rozhodnutí o jeho datech vložených do cloudové služby. Zákazník si v případě zájmu s poskytovatelem dohodne, které monitorované informace jej zajímají a jakým způsobem si o nich přeje být informován.

Aby byl rozsah a význam tohoto požadavku jednoznačný, je nezbytné vycházet z následujících pojmů. Podle § 2 odst. 2 písm. e) zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „ZKB“), se kybernetickou bezpečnostní událostí rozumí taková událost, která může vyústit v kybernetický bezpečnostní incident. Podle § 2 odst. 2 písm. f) ZKB je kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v kybernetickém prostoru. Bezpečnost informací je podle § 2 odst. 2 písm. b) ZKB zajištění důvěrnosti, integrity a dostupnosti informací a dat.

Nástrojem pro sledování a vyhodnocování kybernetických bezpečnostních událostí se rozumí např. Security Information and Event Management (SIEM).

Doložte, že máte zavedený nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí. Rovněž doložte, že umožňujete zákazníkovi vzdálený přístup k informacím o všech událostech týkajících se daného zákazníka a že nové události zpřístupňujte zákazníkovi bez zbytečného odkladu.

Dokládá se:

- části smluvní dokumentace **nebo**
- části další dokumentace **nebo**
- části auditní zprávy.

2.7.2 Řádek 7.2 Notifikace o bezpečnostních incidentech a přijatých opatřeních

Řádek 7.2	Poskytovatel informuje zákazníka v případě narušení bezpečnosti informací zákaznických dat nebo specifických provozních údajů bez zbytečného odkladu, nejpozději však do 72 hodin od okamžiku, kdy se o narušení bezpečnosti zákaznických dat nebo specifických provozních údajů dozvěděl. Jakmile je řešení incidentu uzavřeno, informuje poskytovatel zákazníka o přijatých opatřeních.

V případě, že dojde k narušení bezpečnosti informací zákaznických dat nebo specifických provozních údajů, jste dle požadavku řádku povinni informovat zákazníka bez zbytečného odkladu, nejpozději do 72 hodin od okamžiku, kdy jste se o kybernetickém bezpečnostním incidentu dozvěděli.

Po uzavření řešení kybernetického bezpečnostního incidentu sdělte zákazníkovi, jaká nápravná opatření byla přijata. Tento postup zajišťuje transparentnost, rychlou reakci a minimalizaci dopadů na provoz zákazníka.

Aby byl rozsah a význam tohoto řádku jednoznačný, je nezbytné vycházet z následujících pojmů. Podle § 2 odst. 2 písm. f) ZKB je kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v kybernetickém prostoru. Podle § 2 odst. 2 písm. b) ZKB se bezpečností informací rozumí zajištění důvěrnosti, integrity a dostupnosti informací a dat.

Dokládá se:

- částí smluvní dokumentace **nebo**
- částí další dokumentace.

2.8 Testování služby cloud computingu

Vyhláška v tomto požadavku stanovuje povinnost provedení skenů zranitelností a penetračních testů, které mají ověřit zabezpečení služby. Cílem je zajistit, že nabízená služba je pravidelně prověřována a nemá nedostatky, které by znamenaly bezpečnostní riziko pro orgány veřejné správy. Za případné zjištěné zranitelnosti nehrozí žádný postih, citlivé informace v záznamu je rovněž možné začernit, pokud i tak zůstane patrné, že požadavek byl splněn.

Nová vyhláška zavedla 24měsíční přechodné období (od 1. 1. 2026 do 1. 1. 2028), které má nabídnout dostatečnou dobu pro přípravu a implementaci novelizovaných požadavků na testování zapisované služby. Dokládat požadavky řádků 8.1 a 8.2 vyhlášky jak při zápisu služby, tak i následně v rámci pravidelného dokládání během evidence služby v katalogu, můžete během přechodného období buď podle předchozí vyhlášky č. 316/2021 Sb. (účinné do 31. 12. 2025), nebo podle aktuální vyhlášky č. 505/2025 Sb. (účinné od 1. 1. 2026). Po skončení přechodného období, tedy po 1. 1. 2028, je již právní režim jednotný a je nutné dokládat splnění požadavku výhradně podle vyhlášky č. 505/2025 Sb.

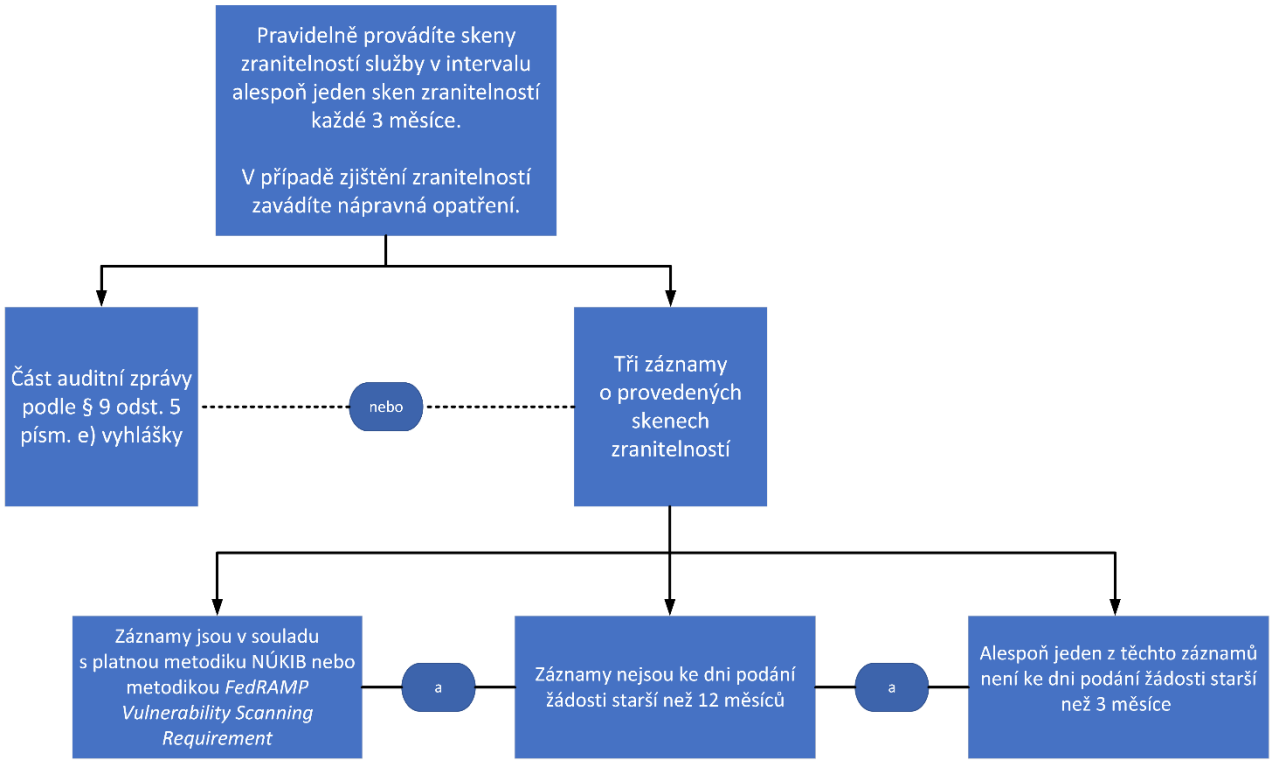
Dokládání požadavků na testování služby dle předchozí úpravy se věnuje Průvodce dokládání požadavků pro zápis služby cloud computingu podle přílohy č. 2 vyhlášky č. 316/2021 Sb.[5]

[5] Průvodce dokládání požadavků pro zápis služby cloud computingu podle přílohy č. 2 vyhlášky č. 316/2021 Sb. dostupný zde: Prvodce_dokldn_poadavk_pro_zpis_sluby_cloud_computingu-v.1.2.pdf

2.8.1 Řádek 8.1 Skenování zranitelností

Řádek 8.1	Poskytovatel pravidelně provádí skeny zranitelností služby cloud computingu v intervalu alespoň jeden sken zranitelností každé 3 měsíce a v případě zjištění zranitelností zavádí nápravná opatření.

Pro splnění požadavku je třeba alespoň jednou za tři měsíce provést sken zranitelností služby, a pokud jsou zjištěny zranitelnosti, přijmout odpovídající nápravná opatření k jejich odstranění.



Dokládá se:

- třemi záznamy o provedení skenů zranitelností**,**
  - které jsou v souladu s platnou metodiku NÚKIB[6] nebo metodikou *FedRAMP Vulnerability Scanning Requirements*,
  - které nejsou ke dni podání žádosti starší než 12 měsíců
  - a zároveň alespoň jeden z těchto záznamů není ke dni podání žádosti starší než 3 měsíce **nebo**
- částí auditní zprávy.

[6] **Metodika dokládání provádění skenů zranitelností a penetračního testování** pro zápis do katalogu cloud computingu je dostupná zde: Metodika_dokladani_pozadavku.pdf. Pokud NÚKIB vydá aktualizovanou metodiku, můžete začít předkládat doklady v souladu s novou metodikou až po 24 měsících od jejího zveřejnění.

Okamžikem zápisu služby do katalogu povinnosti poskytovatele nekončí. Vyhláška stanovuje systém pravidelné kontroly, který má zajistit, aby byla bezpečnost nabízené služby ověřována po celou dobu evidence v katalogu. Během přechodného období (tj. do 1. 1. 2028) můžete dokládat těmito způsoby:

- **podle vyhlášky č. 316/2021 Sb.:** V souladu s přílohou č. 4 pro řádek 10.1 vyhlášky č. 316/2021 Sb. předložte každých 24 měsíců evidence služby v katalogu čtyři záznamy o provedení skenů zranitelností dané služby provedených každých 6 měsíců evidence v katalogu, nebo auditní zprávu vydanou pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávy SOC 2® Type 2, s odkazem na tu část, ze které vyplývá splnění požadavku **nebo**
- **podle vyhlášky č. 505/2025 Sb.:** V souladu s přílohou č. 6 pro řádek 8.1 vyhlášky č. 505/2025 Sb. předložte každých 24 měsíců evidence služby v katalogu záznamy o provedení skenů zranitelností dané služby provedené alespoň jednou za každé 3 měsíce, nebo část auditní zprávy podle § 9 odst. 5 písm. e) vyhlášky, ze které vyplývá splnění požadavku.

2.8.2 Řádek 8.2 Penetrační testování

Řádek 8.2	Poskytovatel zajišťuje provádění penetračních testů podle aktuálně platného standardu NIST 800-115, metodiky OSSTMM nebo standardu OWASP ASVS Level 1 odpovídající charakteru zapisované služby cloud computingu a v souladu s aktuálně platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, nebo v souladu s metodikou FedRAMP. Dojde-li k aktualizaci metodiky Národního úřadu pro kybernetickou a informační bezpečnost, poskytovatel předkládá podklady ke splnění požadavku v souladu s aktualizovanou metodikou po 24 měsících od data zveřejnění aktualizované metodiky.

V závislosti na charakteru zapisované služby zajistěte provedení penetračního testu jedním z uvedených způsobů:

- podle aktuálně platného standardu NIST 800-115, metodiky OSSTMM nebo standardu OWASP ASVS Level 1, a to zároveň v souladu s aktuálně platnou metodikou NÚKIB **nebo**
- v souladu s metodikou *FedRAMP Penetration Test Guidance*.

Dokládá se:

- zprávou z provedení penetračního testu.

Okamžikem zápisu služby do katalogu povinnosti poskytovatele nekončí. Vyhláška stanovuje systém pravidelné kontroly, který má zajistit, aby byla bezpečnost nabízené služby ověřována po celou dobu evidence v katalogu. Během přechodného období (tj. do 1. 1. 2028) můžete dokládat dvěma způsoby:

- **podle vyhlášky č. 316/2021 Sb.:** V souladu s přílohou č. 4 pro řádky 10.2 a 10.3 vyhlášky č. 316/2021 Sb. předložte každých 24 měsíců evidence služby v katalogu specifikovanou zprávu z provedení penetračního testu. Zpráva nesmí být starší než 23 měsíců od data zápisu do katalogu nebo od dodání předchozí zprávy o provedení penetračního testu **nebo**
- **podle vyhlášky č. 505/2025 Sb.:**
  - V souladu s přílohou č. 6 pro řádek 8.2 vyhlášky č. 505/2025 Sb. předložte každých 24 měsíců evidence služby v katalogu zprávu z provedení penetračního testu dle uvedených metodik či standardů, která není starší než 24 měsíců od data vyhotovení předchozí předložené zprávy o provedení penetračního testu.
  - V rámci pravidelné kontroly je třeba prokázat, že na nálezy z předchozích penetračních testů vhodně reagujete. Doložte předložením zprávy o provedení penetračního testu, auditní zprávy dle § 9 odst. 5 písm. e) vyhlášky nebo prohlášení o aplikovatelnosti dle přílohy č. 5 vyhlášky, z nichž vyplývá realizace nápravných opatření vzhledem k nálezům předchozích penetračních testů.

2.9 Připojení do výměnného uzlu internetu (IXP) v ČR

2.9.1 Řádek 9.1 Připojení do výměnného uzlu internetu (IXP) v ČR

Řádek 9.1	Poskytovatel má zajištěno připojení do výměnného uzlu internetu (IXP) v České republice.

Vyhláška v tomto požadavku stanovuje povinnost připojení poskytovatele do výměnného uzlu internetu (IXP) v ČR. Jedná se o další z opatření pro zajištění vyšší dostupnosti služby cloud computingu. Připojení do výměnného uzlu internetu v ČR může mít pozitivní vliv i na důvěrnost informací v případě, že je do stejného výměnného uzlu internetu připojen i zákazník poskytovatele.

Dokládá se:

- výpisem z veřejně dostupné databáze subjektů připojených do výměnného uzlu internetu **nebo**
- platnou smlouvou s poskytovatelem služby výměnného uzlu internetu **nebo**
- čestným prohlášením.

3 Podmínky využití informací

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

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

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
15. dubna 2026	1.0	OREG	Vytvoření dokumentu