NÚKIB

Průvodce požadavky bezpečnostní úrovně nízká

TLP:CLEAR

15. dubna 2026

Verze 1.0

Národní úřad
pro kybernetickou
a informační bezpečnost

Obsah

Seznam pojmů a zkratek

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 předchozí 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 Nízká

Pro lepší přehlednost a rychlou orientaci je v této kapitole uveden stručný výčet požadavků a úplné znění požadavků definovaných v příloze č. 1 vyhlášky pro bezpečnostní úroveň **nízká**.

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
Lokalita uložení a zpracování dat	1.2	1.2		
Přezkum zákonnosti a informování zákazníka při žádostech cizích orgánů o zpřístupnění dat zákazníka	2.1	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
Nástroje pro detekci a zmírnění DDoS útoků	4.3	4.3	4.5	4.5
Záznamy o přístupu k nezašifrovaným zákaznickým datům	5.1	5.1	5.1	5.1
Šifrování - v síti (mimo kontrolu poskytovatele) a v uložišti	5.2	5.2		

Soulad s ISMS dle ISO 27001 nebo režimem nižších povinností	6.1			
Nástroj pro sledování a vyhodnocování kybernetických událostí	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

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 Lokalita uložení a zpracování dat

Řádek 1.2	Poskytovatel uvádí informace o všech státech, na jejichž území jsou nebo mohou být uložena zákaznická data ve stavu neaktivních dat a specifické provozní údaje ve stavu neaktivních dat, a dále uvádí informace o všech státech mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, na jejichž území předpokládá zpracování zákaznických dat a specifických provozních údajů. Platí, že státy, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat nebo specifických provozních údajů, nejsou A) státy, z jejichž území se mohou nepravidelně vzdáleně připojovat pracovníci technické podpory poskytovatele cloud computingu za účelem technické podpory služby cloud computingu, která se v čase mění, a nemohou být specifikovány předem, nebo B) státy, z jejichž území poskytovatel může předávat zákaznická data nebo specifické provozní údaje za účelem poskytování volitelné doplňkové služby se zapojením třetích stran, která není sama o sobě cloud computingem, aktivované podle volby zákazníka, s tím, že poskytovatel jasně označí třetí stranu, jíž může předat zákaznická data nebo specifické provozní údaje, a je-li to možné, blíže specifikuje, jaká zákaznická data nebo jaké specifické provozní údaje zpravidla předává a na jakou předpokládanou dobu zákaznická data nebo specifické provozní údaje předává.

Do formuláře žádosti uveďte všechny státy, na jejichž území jsou ukládána zákaznická data ve stavu neaktivních dat a specifické provozní údaje ve stavu neaktivních dat.

Dále uveďte všechny státy, na jejichž území předpokládáte zpracování zákaznických dat a specifických provozních údajů – přitom vynechte členské státy Evropské unie (dále jen „EU“) a Evropského sdružení volného obchodu (dále jen „ESVO“).

Za lokality, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat a specifických provozních údajů, se nepovažují:

- státy, z jejichž území se mohou nepravidelně připojovat vaši pracovníci technické podpory, **nebo**
- státy, z jejichž území můžete předávat zákaznická data nebo specifické provozní údaje kvůli poskytování volitelné doplňkové služby, která sama o sobě není cloud computingem a je aktivována na základě volby zákazníka. V případě, že zákazníkovi plánujete nabízet a poskytovat tuto volitelnou doplňkovou službu, ve formuláři jasně označte třetí stranu, které mohou být předána zákaznická data nebo specifické provozní údaje. Pokud je to možné, uveďte, jaká zákaznická data nebo specifické provozní údaje zpravidla předáváte a rovněž na jakou předpokládanou dobu.

V případě, že vaše služba využívá jako podpůrný cloud computing skrze materiálního dodavatele službu, která ukládá či zpracovává zákaznická data a (nebo) specifické provozní údaje mimo území států EU a ESVO, je třeba toto při dokládání požadavku řádku 1.2 zohlednit. Bez ohledu na bezpečnostní úroveň, do které je služba podpůrného cloud computingu zapsána, bude mít

v katalogu ve formuláři označeno, že ukládá a (nebo) zpracovává informace orgánu veřejné správy mimo území EU a ESVO. Pokud je služba podpůrného cloud computingu, kterou vámi zapisovaná služba využívá, zařazena do bezpečnostní úrovně vysoká a nesplňuje požadavek na ukládání zákaznických dat a (nebo) specifických provozních údajů na území států EU a ESVO, najdete tento podpůrný cloud computing rovněž na úřední desce Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“ nebo také „NÚKIB“), kde je veden seznam služeb cloud computingu zapsaných v bezpečnostní úrovni vysoká na výjimku z uložení zákaznických dat a (nebo) specifických provozních údajů na území států EU a ESVO.

Jestliže vámi zapisovaná služba využívá podpůrný cloud computing, který ukládá a (nebo) zpracovává zákaznická data a (nebo) specifické provozní údaje mimo území EU a ESVO, s největší pravděpodobností se toto specifikum bude týkat i vámi zapisované služby a bude nutné v souladu s tím řádně vyplnit formulář žádosti a reflektovat tuto skutečnost při dokládání požadavku řádku 1.2. Při dokládání požadavku je možné explicitně odkázat na doklady, které materiální dodavatel předložil s jeho vlastní žádostí o zápis služeb do katalogu, a to buď v plném rozsahu, nebo s deklarací rozdílů v místech ukládání a (nebo) zpracování zákaznických dat a (nebo) specifických provozních údajů mezi poskytovatelem a jeho materiálním dodavatelem. Pokud se domníváte, že i přes využití takového podpůrného cloud computingu dokážete zajistit uložení a zpracování zákaznických dat a (nebo) specifických provozních údajů výhradně ve státech EU a ESVO, budete to muset v rámci dokládání jednoznačně prokázat.

Dokládá se:

- písemným popisem.

2.2 Žádosti o zpřístupnění a předání dat

2.2.1 Řádek 2.1 Žádosti o zpřístupnění dat zákazníka

Řádek 2.1	Poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat nebo specifických provozních údajů, nevyhoví této žádosti a odkáže tohoto žadatele na zákazníka nebo, v případě, že této žádosti vyhoví, o takové žádosti zákazníka bezodkladně informuje, pokud to právní řád, jemuž poskytovatel podléhá, poskytovateli nezakazuje. Poskytovatel dále po obdržení takové žádosti přezkoumá její zákonnost, zejména provede právní posouzení, ze kterého bude vyplývat, zda 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. 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.

Tento požadavek má za cíl poskytnout zákazníkovi služby jistotu, že jeho data nebudou zpřístupněna cizím státům bez zákonného důvodu. Zároveň má zajistit transparentnost a možnost zpětného doložení vašeho postupu.

Pokud obdržíte žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, máte primárně povinnost žádosti nevyhovět a tento orgán přesměrovat přímo na zákazníka, pokud vám v tom nebrání relevantní právní předpis. Cizozemským orgánem se rozumí státní orgán odlišný od státního orgánu České republiky.

Každou takovou žádost jste povinni posoudit všemi vhodnými způsoby. Žádaná data můžete předat pouze v případě, že z posouzení vyplyne, že žádost:

- má proveditelný, aplikovatelný a platný právní základ,
- je právně závazná
- a rozsah, v jakém je požadován přístup k datům zákazníka či jejich vydání, odpovídá účelu, za jakým byla žádost podána.

V případě, že žádost splňuje všechna vymezená kritéria a vyhovíte jí, bezodkladně o ní informujte zákazníka, pokud vám to právní řád nezakazuje. O provedeném posouzení a použitých podkladech vytvořte záznam, který uchováte alespoň po dobu pěti let, nebo jej prokazatelně předáte zákazníkovi.

Dokládá se:

- čestným prohlášením **nebo**
- částí smluvní dokumentace **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 údajů1), 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, Evropský hospodářský prostor nebo mimo státy, 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, 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.

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 Úřadem. 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.

[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

2.4.1 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:

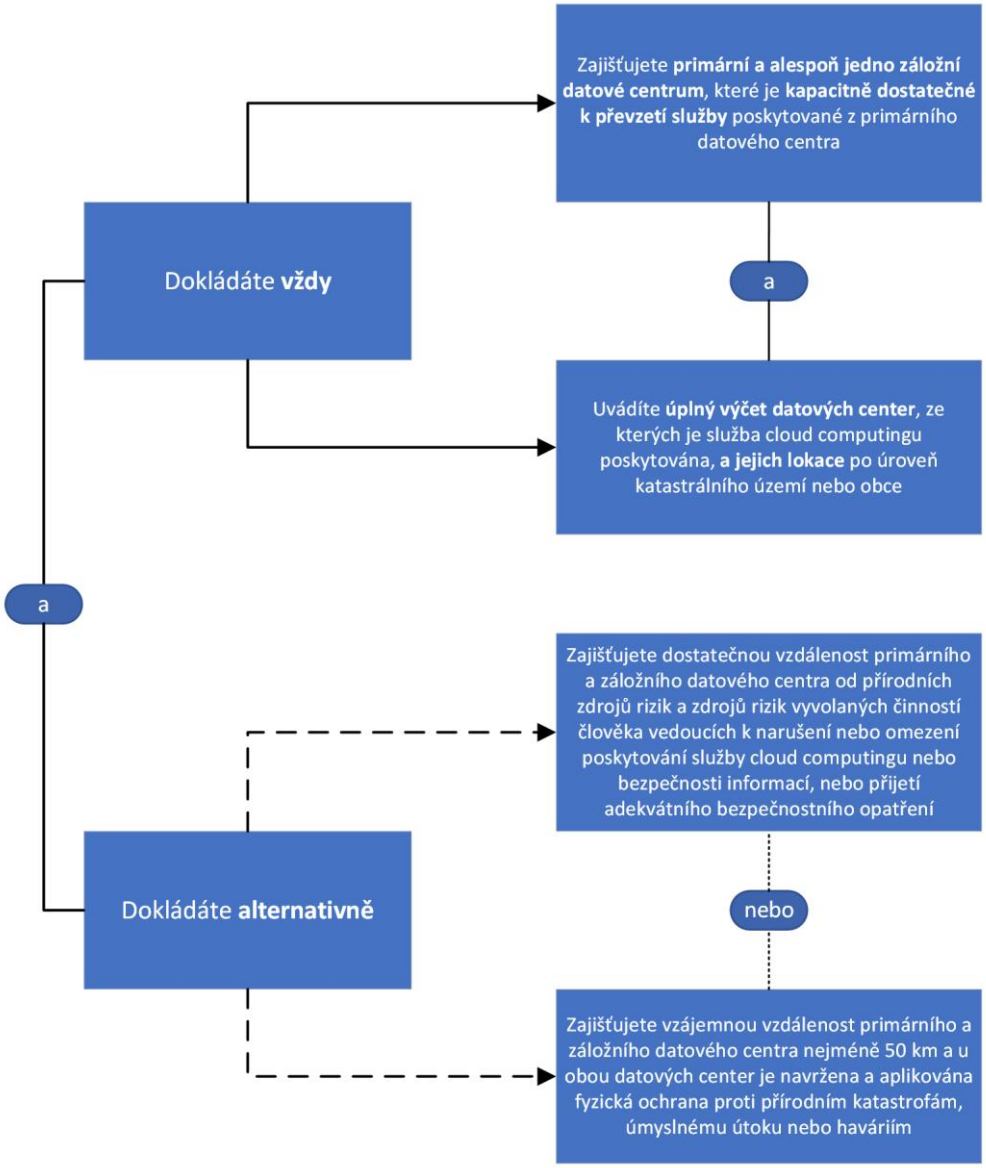
- **dostatečná vzdálenost od přírodních zdrojů rizik a rizik vyvolaných aktivitou člověka** vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací nebo
- **přijetí adekvátních bezpečnostních opatření,** kdy je třeba prokázat, že byť se datová centra nacházejí 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 doložení 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 Nástroje pro detekci a zmírnění DDoS útoků

Řádek 4.3	Poskytovatel je schopen poskytovat nástroj nebo službu pro detekci a zmírnění útoků typu odepření služby (DoS/DDoS) jak na síťové, tak aplikační úrovni.

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 vám 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.

2.5 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.

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 předchozího 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 Šifrování v síti mimo kontrolu poskytovatele a v úložišti

Řádek 5.2	Poskytovatel umožňuje ochranu zákaznického obsahu šifrováním při přenosu po sítích mimo kontrolu poskytovatele a v úložištích ve službě cloud computingu.

Doložte, že umožňujete šifrování zákaznického obsahu při přenosech po sítích mimo vaši kontrolu a v úložištích ve službě cloud computingu.

Za přenos po sítích mimo kontrolu poskytovatele se považuje veškerá komunikace, která probíhá mimo vámi spravované a kontrolované prostředí. Typicky jde o přenosy mezi uživateli a cloudovou službou nebo o jakoukoliv komunikaci přes veřejný internet. 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.

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.

2.6 Certifikace služby cloud computingu

2.6.1 Řádek 6.1. Soulad s ISMS dle ISO 27001 nebo režimem nižších povinností

Řádek 6.1	Poskytovatel provozuje službu cloud computingu v rozsahu systému řízení bezpečnosti informací, který je v souladu s požadavky vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností nebo s požadavky podle ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001.

Požadavkem tohoto řádku není to, aby zapisovaná služba byla certifikovaná, ale aby byla provozována v souladu s uvedenou certifikací, případně s vyhláškou č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

Společně s čestným prohlášením, že služba je provozovaná v souladu s danou certifikací nebo s vyhláškou č. 410/2025 Sb. doložte i prohlášení o aplikovatelnosti jednotlivých opatření.

Prohlášení o aplikovatelnosti (zkráceně SoA z anglického Statement of Applicability) je dokument systému řízení bezpečnosti informací, který slouží k transparentnímu vykazování plnění bezpečnostních požadavků. Obsahuje přehled relevantních bezpečnostních opatření (kontrol) vyplývajících z hodnocení rizik nebo platné legislativy a u každého z nich uvádí, zda je v organizaci implementováno. Součástí dokumentu je zdůvodnění pro zařazení či vyloučení jednotlivých opatření, které vychází z rozhodnutí o řešení identifikovaných rizik nebo z posouzení jejich aplikovatelnosti vzhledem k činnosti organizace a platným právním předpisům. Dokument dále uvádí aktuální stav implementace a odkazuje na interní politiky, procedury nebo důkazní materiály, které konkrétní způsob provedení a plnění požadavků prokazují.

Dokládá se:

- čestným prohlášením **a současně**
- prohlášením o aplikovatelnosti.

2.7 Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty

2.7.1 Řádek 7.1 Sledování a vyhodnocování kybernetických událostí

Řádek 7.1	Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí.

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.

Dokládá se:

- částí smluvní dokumentace **nebo**
- částí další dokumentace **nebo**
- částí 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 tohoto 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. Doložte, že máte zaveden proces odpovídající dikci vyhlášky.

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 provádění skenů zranitelností. 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 požadavek řádku 8.1 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.

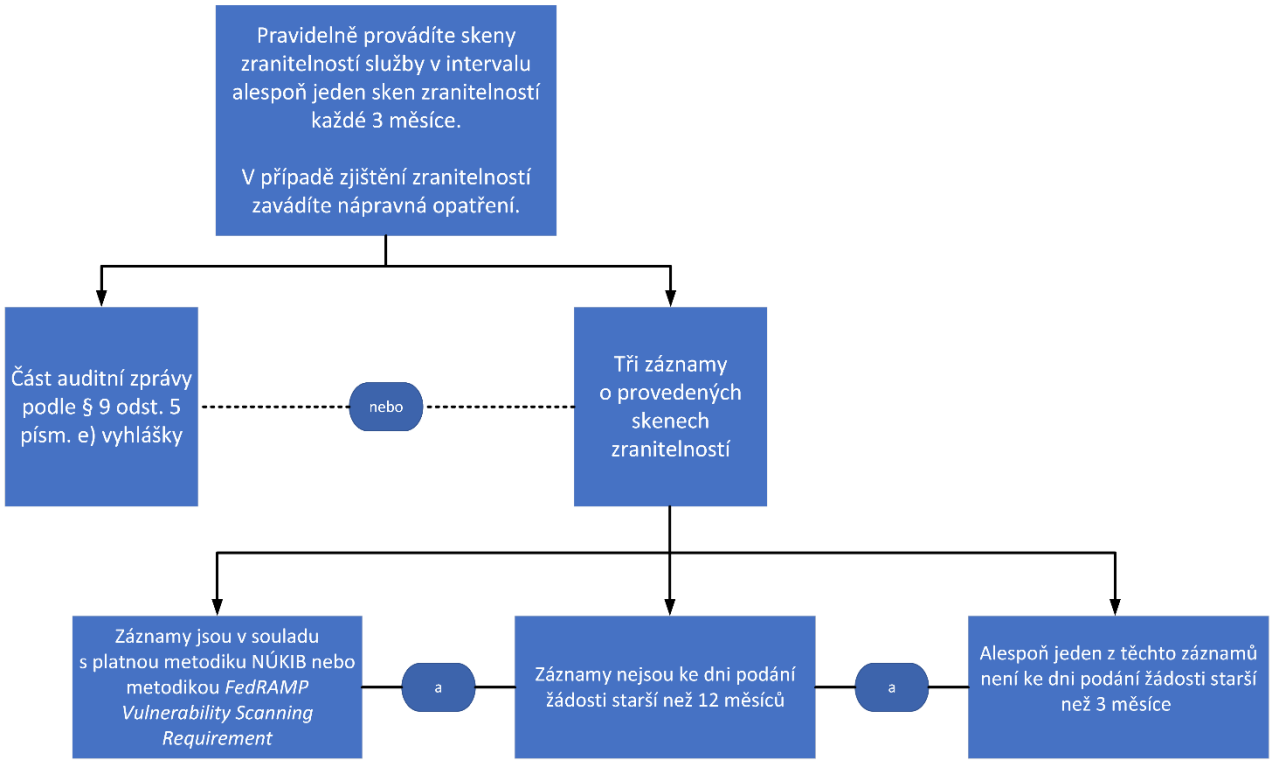
Dokládání požadavků na testování služby dle předchozí úpravy se věnuje Průvodce dokládání požadavků pro zápis služby cloud computingu podle přílohy č. 2 vyhlášky č. 316/2021 Sb.[2]

[2] Průvodce dokládání požadavků pro zápis služby cloud computingu podle přílohy č. 2 vyhlášky č. 316/2021 Sb. je 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[3] 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.

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.

[3] **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.

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