NÚKIB

Průvodce dokládání požadavků pro zápis služby cloud computingu

TLP:CLEAR

15. dubna 2026

Verze 1

Národní úřad
pro kybernetickou
a informační bezpečnost

Obsah

Seznam pojmů a zkratek ... 3
1 Co se dozvím v tomto dokumentu? ... 4
2 Právní rámec ... 5
3 Obecné požadavky a nedostatky při dokládání splnění požadavků ... 7
3.1 Požadavky na strukturu a náležitosti podkladů k ověření splnění požadavků ... 7
3.2 Základní pojmy ... 8
3.2.1 Obecné pojmy ... 8
3.2.2 Formy podkladů pro dokládání splnění jednotlivých požadavků ... 9
3.3 Typy požadavků ... 11
3.4 Časté obecné nedostatky při dokládání splnění požadavků ... 12
3.4.1 Nesprávné nebo zcela chybějící odkazování na dokládané dokumenty ... 12
3.4.2 Špatná forma či formát dokumentu ... 14
3.4.3 Nekonzistentnost v pojmenování služeb ... 14
3.4.4 Chybějící nebo nejasná vazba prokazovaných skutečností na zapisované služby ... 15
3.4.5 Nerespektování typu požadavku při dokládání ... 16
3.4.6 Chybějící odůvodnění při neuplatnění požadavku ... 16
3.4.7 Jiné pojmosloví ... 17
4 Stručný výčet požadavků ... 18
4.1 Místo zpracování a uložení dat ... 18
4.2 Žádosti o zpřístupnění a předání dat ... 19
4.3 Oprávnění k provedení kontroly ... 19
4.4 Zajištění poskytování služby ... 19
4.5 Nakládání s daty ... 20
4.6 Certifikace služby ... 21
4.7 Kybernetické bezpečnostní události a incidenty ... 21
4.8 Testování služby ... 21
4.9 Připojení do výměnného uzlu internetu ... 22
5 Podmínky využití informací ... 23

Seznam pojmů a zkratek

ČR	Česká republika
DIA	Digitální a informační agentura
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
ZoISVS	zákon č. 365/2000 Sb., o informačních systémech veřejné správy
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, právním rámcem a přibližuje obecné požadavky na dokládání splnění požadavků vyhlášky a časté nedostatky při dokládání. 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 o zápis nabídky cloud computingu do katalogu cloud computingu (dále jen „žádost“) a celkového procesu zápisu služeb cloud computingu do katalogu.

Podrobné vymezení požadavků pro jednotlivé bezpečnostní úrovně je obsahem samostatných dokumentů vytvořených pro každou bezpečnostní úroveň zvlášť.

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 Právní rámec

Právní rámec pro poskytování služeb cloud computingu orgánům veřejné správy tvoří kombinace zákonných povinností stanovených zákonem č. 365/2000 Sb., o informačních systémech veřejné správy (dále jen „ZoISVS“) a podrobných technických a bezpečnostních požadavků definovaných ve vyhlášce. Cílem této právní úpravy je zajistit, aby orgány veřejné správy využívaly prověřené služby cloud computingu, a tím se mitigovala rizika s cloudem spojená.

ZoISVS stanoví, že každý subjekt poskytující cloud computing pro zajištění provozu informačního systému veřejné správy nebo jeho části musí být předem zapsán do katalogu cloud computingu (dále jen „katalog“) vedeného Digitální a informační agenturou (dále jen „DIA“). Regulatorní rámec je obsažen v hlavě VI části první ZoISVS, přičemž stěžejní úpravu představuje zejména ustanovení § 6l a následující. Z této právní úpravy vyplývá, že orgán veřejné správy smí využívat pouze takové služby cloud computingu, které jsou – společně se svým poskytovatelem –zapsány v katalogu cloud computingu. Výjimku tvoří služby cloud computingu uvedené v § 6l odst. 4 ZoISVS, které regulaci nepodléhají (např. služba cloud computingu sloužící výlučně ke správě a řešení technických potíží nebo diagnostice programových anebo technických prostředků).

Proces zápisu probíhá formou správního řízení zahajovaného na žádost poskytovatele. Řízení je dvoufázové: nejprve je posuzována způsobilost a bezúhonnost poskytovatele, a teprve následně jsou posuzovány a zapisovány do katalogu jednotlivé cloudové služby, které poskytovatel hodlá nabízet. Zároveň je dle § 6n písm. e) a f) ZoISVS podmínkou, že pokud je poskytování zapisované služby cloud computingu závislé na využití jiné služby nebo služeb cloud computingu, je třeba, aby tento cloud computing a jeho poskytovatel byli rovněž v katalogu zapsáni.

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Úřad“ nebo také „NÚKIB“) do řízení o zápisu do katalogu vstupuje v několika specifických situacích:

- při zápisu poskytovatele cloud computingu, kdy si dle § 6r odst. 1 ZoISVS DIA od Úřadu vyžádá závazné stanovisko pro účely posouzení splnění požadavků dle § 6m odst. 1 písm. a) ZoISVS,
- při zápisu poskytovatele cloud computingu, kdy je dle § 6r odst. 5 ZoISVS DIA oprávněna vyžádat si od Úřadu informace pro účely posouzení splnění požadavků dle § 6m odst. 1 písm. c) ZoISVS a
- při zápisu služby cloud computingu do bezpečnostní úrovně střední, vysoká nebo kritická, kdy si dle § 6u odst. 1 ZoISVS DIA od Úřadu vyžádá závazné stanovisko pro účely posouzení splnění požadavků dle § 6n písm. b) a e) ZoISVS.

Konkrétní technické a bezpečnostní požadavky stanoví prováděcí vyhláška. Vyhláška se obsahově opírá o předchozí právní úpravu ve vyhlášce č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „vyhláška č. 316/2021 Sb.“).

Hlavní změny oproti vyhlášce č. 316/2021 Sb. zahrnují zejména:

- úpravy reflektující nový zákon č. 264/2025 Sb., o kybernetické bezpečnosti — zejména nové podmínky bezúhonnosti poskytovatele v návaznosti na aktualizovanou množinu přestupků a aktualizaci odkazů na prováděcí předpisy tak, aby nedocházelo k odkazům na derogované právní normy,
- zásadní zpřehlednění vyhlášky — zavedení jednotného pojmosloví forem podkladů dokládajících splnění požadavků, rozdělení původní přílohy č. 2 do čtyř samostatných příloh podle bezpečnostní úrovně cloudové služby a odstranění parametru třídy cloud computingu u jednotlivých požadavků,
- rozšíření množiny akceptovatelných auditních zpráv jako podkladů pro dokládání splnění požadavků, a to v reakci na praktické potřeby poskytovatelů,
- odstranění některých požadavků, které se ukázaly jako nadbytečné (např. části týkající se úrovně dostupnosti služby nebo požadavku na možnost importu/exportu dat ve vysokém objemu na šifrovaných fyzických nosičích) nebo
- upřesnění požadavků na skeny zranitelností a zprávy o penetračním testování, jejichž dosavadní obecnost vyvolávala nejistotu ohledně rozsahu a způsobu jejich dokládání.

3 Obecné požadavky a nedostatky při dokládání splnění požadavků

Obecným požadavkům a základním pojmům, které prostupují konkrétní požadavky v přílohách, se věnuje samotné paragrafové znění vyhlášky. Je nezbytné zohledňovat tyto požadavky při dokládání splnění jednotlivých požadavků dle příloh a nevnímat přílohy jako izolovanou část předpisu.

3.1 Požadavky na strukturu a náležitosti podkladů k ověření splnění požadavků

Podle § 9 odst. 1 vyhlášky je k ověření splnění požadavků podle § 4 potřeba doložit dva základní typy podkladů: **popis splnění požadavku v elektronickém formuláři (žádosti)**, který je dostupný na internetových stránkách DIA, a **další dokumenty**, tedy samostatné přílohy. Struktura všech těchto podkladů musí být dle § 9 odst. 3 vyhlášky přehledná a srozumitelná, čehož docílíte tím, že ve formuláři popíšete každou jednotlivou službu cloud computingu, kterou žádáte zapsat do katalogu, a pro každou z nich doložíte splnění požadavků podle § 4 vyhlášky.

V případě, že více zapisovaných služeb spadajících do totožné bezpečnostní úrovně a třídy splňuje požadavky podle § 4 shodně, můžete doložit splnění pro všechny služby dohromady pouze jednou, a následně jednoznačně uvést výčet všech služeb, na které se toto doložení vztahuje.

V případě, že žádáte zapsat nabídku cloud computingu, pro kterou je možné doložit splnění požadavků shodným podkladem, kterým jste již dříve prokázali splnění požadavků u své zapsané nabídky, můžete se na tento podklad odkázat. Je přitom nutné dodržet správný způsob odkazování na doložené podklady popsaný níže.

Podklady pro ověření splnění požadavků podle § 4 vyhlášky musí tedy obsahovat:

- **popis splnění požadavku** ve formulářové žádosti pro službu cloud computingu, kterou žádáte zapsat do katalogu, dokládající splnění požadavků v přílohách č. 1 až 4 vyhlášky, a
- **dokumenty**, kterými doložíte splnění požadavků podle příloh č. 1 až 4 vyhlášky.

V případě, že je pro doložení splnění požadavku podle § 4 nezbytné odkázat do jiného dokumentu, který je k formuláři připojen, musíte dodržet **správný způsob odkazování na doložené dokumenty**, který je popsán v § 9 odst. 4 vyhlášky. Učiníte tak ve formuláři žádosti uvedením **názvu připojeného dokumentu a kapitoly, strany, odstavce a případně konkrétní věty**, ze které splnění požadavku vyhlášky vyplývá. Je potřeba důsledně odkazovat na konkrétní části dokládaných dokumentů. Na všechny dokládané podklady se uplatní požadavek strojově čitelného formátu zaručující neměnnost obsahu jednotlivých dokumentů. Odkaz na webovou stránku není uznatelný, jelikož podoba webových stránek se mění v čase. Bližší informace jsou popsány níže v kapitole „Časté obecné nedostatky při dokládání splnění požadavků“.

Pro účely doložení splnění jednotlivých požadavků **akceptujeme podklady vyhotovené v anglickém jazyce**. Není tedy nezbytné překládat tyto podklady do jazyka českého.

3.2 Základní pojmy

Při přípravě podkladů je třeba věnovat mimořádnou pozornost terminologii, aby byl dodržen požadavek na přehlednost a srozumitelnost žádosti. Vyhláška v přílohách č. 1 až 4 pracuje se specifickými pojmy, které mají přesně vymezený význam. Tyto definice lze nalézt přímo v § 2 vyhlášky nebo v její důvodové zprávě.

3.2.1 Obecné pojmy

Zákaznická data jsou všechna data, která jsou uživatelem poskytnuta poskytovateli v průběhu užívání služby cloud computingu. Pokud jsou některá zákaznická data obsažena v provozních údajích, neztrácejí tím svou povahu a stále se jedná o zákaznická data.

Zákaznický obsah jsou textová, zvuková, audiovizuální, obrazová nebo jiná data (vlastní „soubory“ či „záznamy“), která byla uživatelem do služby vložena, a to bez jejich metadat a indexů k těmto datům.

Provozní údaje jsou data vygenerovaná nebo odvozená poskytovatelem v souvislosti s provozem a poskytováním služby cloud computingu.

Specifické provozní údaje jsou takové provozní údaje, které obsahují informace o identifikovaném nebo identifikovatelném uživateli. Jedná se o nejcitlivější provozní údaje, které jsou velice často osobními údaji, a také ty neosobní údaje, které jsou způsobilé identifikovat právnické osoby a další uživatele. Jednat se může například o provozní údaje s vysokou informační hodnotou (jaký uživatel, kdy a jak často přistupuje do informačních systémů/databází a do kterých). Na základě zavedení kategorie specifických provozních údajů vyhláška takovým údajům, které se svým významem blíží osobním údajům (a často jimi i jsou), poskytuje adekvátní ochranu a reflektuje tak požadavky vyplývající z práva na informační sebeurčení.

Zpracováním v širším smyslu se rozumí jakákoliv operace nebo soubor operací se zákaznickými daty a provozními údaji v elektronické podobě, prováděné pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, přenos či zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Bezpečnostní požadavky se liší podle toho, v jakém stavu se data zrovna nacházejí. Správné rozlišení těchto stavů je nezbytné pro určení, jaké konkrétní záruky musí poskytovatel pro danou bezpečnostní úroveň splnit.

- **Přenášená data (Data in Transit/In Motion)** jsou data pohybující se po komunikační síti (kabely, bezdrátové spoje) prostřednictvím fyzických přenosových médií.

- **Neaktivní data (Data at Rest)** jsou veškeré informace orgánu veřejné správy, které jsou trvale uloženy a skladovány v trvalém úložišti. Jedná se o stav, kdy data nejsou v daný okamžik předmětem aktivního výpočtu ani přenosu. Typicky jde o soubory na pevných discích, data v databázových tabulkách nebo zálohy na páskách.
- **Aktivní data (Data in Use)** jsou data, která jsou zpracovávána v daném okamžiku v operační paměti (RAM) nebo v procesoru (CPU). V tomto režimu jsou data pro software čitelná, aby s nimi mohl provádět operace (výpočty, vyhledávání, třídění).

Bezpečnostní úrovní nabízeného cloud computingu se rozumí taková bezpečnostní úroveň, do které nabízený cloud computing řadíte vy sami. Tato volba vyjadřuje, pro jak citlivé systémy veřejné správy je služba určena a jak přísná bezpečnostní kritéria jste schopni garantovat. Pokud si tedy zvolíte např. úroveň „vysoká“, je nutné splnit všechna kritéria v příloze č. 3 vyhlášky, která se na tuto úroveň vztahují. Bezpečnostní úroveň tedy definuje cílovou skupinu zákazníků z řad orgánů veřejné správy a rozsah povinností, které musí být splněny a dodržovány po celou dobu poskytování dané služby.

3.2.2 Formy podkladů pro dokládání splnění jednotlivých požadavků

Vyhláška nově v § 9 odst. 5 uvádí pět forem podkladů, jimiž je možné splnění požadavků doložit, a to včetně jejich definice. Podklady k doložení nejsou nadále popisovány u každého požadavku jednotlivě, ale přílohy ve sloupci „Podklad, kterým poskytovatel doloží splnění požadavku“ odkazují na předem vymezené definice.

Písemným popisem se rozumí text, který slouží k popisu skutečností, u kterých vyhláška nevyžaduje doložení žádnou z ostatních forem. Písemný popis může mít dvě podoby:

- **Samostatného dokumentu** (přílohy), na který odkážete ve formuláři.
- **Textu uvedeného přímo v příslušné kolonce** formulářové žádosti.

Čestné prohlášení je formálnější obdobou písemného popisu, kterým prokazujete splnění daného požadavku. Z dokumentu musí být jasně patrné:

- **kdo a kdy** prohlášení činí,
- **co** konkrétně jím dokládá, (včetně vazby na požadavek vyhlášky a rozsah služeb, které čestné prohlášení pokrývá),
- **podpis** osoby oprávněné jednat za poskytovatele.

V případě, že čestné prohlášení činí osoba odlišná od poskytovatele (např. externí zmocněnec nebo zaměstnanec, který není statutárním orgánem), musí být spolu s prohlášením doložen také **doklad o zmocnění** (plná moc či pověření), který tuto osobu k učinění prohlášení opravňuje.

Smluvní dokumentace pokrývá pojmy návrhu smlouvy, smluvních podmínek, podmínek poskytování služby či jiných obdobných podkladů pro služby cloud computingu, které mají být do katalogu zapsány. Do této kategorie spadá veškerá dokumentace (budoucího) smluvního závazku, která bude upravovat dvoustranný právní vztah mezi vámi, jakožto poskytovatelem, a zákazníkem.

Je zásadní, aby dokumentace obsahovala jasný výčet služeb, ke kterým se vztahuje. Co se týče terminologie, tak zejména v těchto dokumentech je třeba zajistit, že jejich pojmosloví odpovídá pojmům užívaným ve vyhlášce. Je totiž typické, že smlouvy a smluvní podmínky nejsou připravovány pro účely žádosti o zápis služby do katalogu cloud computingu, a proto může být užití terminologie odlišné. V takových případech není potřeba přepisovat návrhy smluvní dokumentace tak, aby byla terminologicky v souladu s vyhláškou, postačí, pokud obsahově požadavky vyhlášky naplňuje. Zároveň připojíte písemný popis, kde bude vztah mezi terminologií návrhu smluvní dokumentace a vyhlášky objasněn.

Další dokumentace zahrnuje produktovou specifikaci, technickou dokumentaci nebo další jiný popis služby, který není smluvní dokumentací. Tento podklad slouží k doložení konkrétních technických vlastností služby nebo k popisu vnitřních postupů a procesů, se kterými je v rámci služby operováno. Zatímco smluvní dokumentace definuje budoucí právní závazek, tedy „co“ poskytovatel slibuje, další dokumentace prokazuje faktický technický stav a reálné fungování služby, tedy „jak“ jsou požadavky naplněny v praxi.

Auditní zprávou vydanou pro certifikaci/atestaci a částí platné certifikace se rozumí buď celá auditní zpráva, na jejímž základě byla poskytovateli daná certifikace či atestace udělena, nebo ta její část, ze které jednoznačně vyplývá splnění daného požadavku vyhlášky. Je přitom nezbytné striktně rozlišovat mezi certifikací, jakožto osvědčením o shodě, a auditní zprávou, jakožto podrobným materiálem. Pokud je u konkrétního požadavku v přílohách vyhlášky vyžadován podklad ve formě auditní zprávy, nepostačí doložení pouhé certifikace či atestace jako takové, jelikož samotný certifikát nemá ohledně detailního splnění specifického technického parametru potřebnou vypovídající hodnotu. Potvrzuje sice shodu se standardem jako celkem, ale neobsahuje konkrétní technický popis realizace opatření vyžadovaného vyhláškou. V takovém případě je třeba předložit buď celou auditní zprávu, nebo její relevantní část, která se přímo věnuje danému požadavku. V rámci vyplňování registračního formuláře je opět nezbytné dodržet správný způsob odkazování, tedy uvést nejen název dokumentu, ale i konkrétní kapitolu, stranu, odstavec, či dokonce konkrétní větu, která prokazuje naplnění požadavku vyhlášky.

Nová právní úprava významně rozšiřuje portfolio dokumentů, kterými lze konkrétní požadavky doložit. Pro účely zápisu služby cloud computingu se uznávají **následující auditní zprávy:**

- **auditní zpráva vydaná pro certifikaci 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),
- **auditní zprávy SOC 2® Type 2,**
- **auditní zpráva o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue (C5)**, a to ve formě **Type 2**, nebo
- **auditní zpráva o vyhodnocení shody s požadavky této vyhlášky.**

- Vyhláška tímto způsobem umožňuje doložit splnění požadavků prostřednictvím zprávy z nezávislého externího auditu, který byl proveden přímo pro vyhodnocení splnění požadavků této vyhlášky.

Aby byla auditní zpráva (bez ohledu na její typ) uznána, musí splňovat kritéria definovaná v § 9 odst. 6 vyhlášky:

- **Nezávislost:** Auditor musí být subjektem zcela nezávislým na poskytovateli. Nesmí jít o interní audit poskytovatele ani o audit provedený osobou, která je s poskytovatelem majetkově nebo personálně propojena.
- **Časová relevance:** Předkládaná auditní zpráva nesmí být ke dni podání žádosti o zápis **starší než 24 měsíců**. Toto opatření zajišťuje, že prokazovaná bezpečnostní opatření jsou aktuální a reflektují současný stav.
- **Vazba na zapisovanou službu:** Auditní zpráva musí jasně definovat svůj rozsah (scope). Pokud zpráva nebo certifikát neobsahuje jmenovitý výčet všech zapisovaných služeb (např. je vydána na celou divizi nebo společnost), lze tento nedostatek zhojit doložením **čestného prohlášení**. V něm musíte potvrdit, že infrastruktura a procesy popsané v auditu jsou identické s těmi, na kterých jsou provozovány konkrétní služby cloud computingu žádané k zápisu.

Splnění některých požadavků je třeba zároveň doložit i **prohlášením o aplikovatelnosti (SoA**). Jedná se o klíčový dokument, který jednoznačně definuje seznam konkrétních bezpečnostních opatření a kontrol, které jsou pro danou službu implementovány. Slouží jako nezbytný doplněk certifikace, protože prokazuje, že auditor prověřil právě ty oblasti, které vyhláška vyžaduje. Bez SoA nelze ověřit reálný věcný rozsah auditu ani to, zda se certifikát skutečně vztahuje na všechny relevantní požadavky.

Pokud je auditní zpráva vydána na odštěpný závod, divizi nebo jinou organizační složku, která nemá vlastní právní subjektivitu, může ji poskytovatel použít. Musí však doložit čestné prohlášení, že tato složka je jeho přímou součástí a že se závěry auditu plně vztahují na služby, které jako právnická osoba nabízí v katalogu.

V případě, že auditní zpráva obsahuje citlivé informace (např. konkrétní IP adresy, jména administrátorů nebo detailní topologii), vyhláška umožňuje tyto pasáže **neuvést nebo zakrýt (začernit)**. Nicméně i po takové úpravě musí zůstat dokument jako celek srozumitelný a musí z něj být jasně patrné, že daný požadavek vyhlášky byl auditorem ověřen jako splněný. Pokud by začernění znemožnilo věcné posouzení shody, bude podklad považován za nedostatečný.

3.3 Typy požadavků

Přílohy k vyhlášce stanovují dva základní typy požadavků. Pro správné doložení je nutné pochopit, zda vyhláška vyžaduje, aby služba něco dělala „sama od sebe“, nebo zda má pouze „nabízet možnost“ danou funkci využít.

- Požadavek na **zajištění:** Poskytovatel musí prokázat, že zapisovaná služba automaticky (by default) zákazníkovi zajišťuje danou funkcionalitu.
  - Příklad požadavkem řádku 4.2

    *„Poskytovatel **vždy zajišťuje** primární a alespoň jedno záložní datové centrum...“*
- Požadavek na **dostupnost**: Poskytovatel musí prokázat, že služba **obsahuje nástroje**, které zákazníkovi dovolují danou funkci využít. Tím se přenáší odpovědnost za aktivaci na zákazníka, který tak činí v rámci svých bezpečnostních opatření.
  - Příklad požadavkem řádku 5.2

    *„Poskytovatel **umožňuje** ochranu zákaznického obsahu šifrováním při přenosu a v úložištích...“*
  - Příklad požadavkem řádku 5.3

    *„Poskytovatel **umožňuje** ochranu... pomocí některého z algoritmů uvedených v doporučení [NÚKIB]...“*

3.4 Časté obecné nedostatky při dokládání splnění požadavků

Obecné nedostatky žádosti o zápis nabídky cloud computingu typicky vznikají nedodržením obecných požadavků vyhlášky, kterým se věnovaly předchozí podkapitoly. Tato podkapitola uvede obecné nedostatky, se kterými se při posuzování žádostí nejčastěji setkáváme. Je důležité věnovat problematice obecných nedostatků dostatečnou pozornost, jelikož jejich předcházením lze zásadně snížit časovou a administrativní náročnost celého procesu zápisu nabídky cloud computingu do katalogu.

3.4.1 Nesprávné nebo zcela chybějící odkazování na dokládané dokumenty

Zásadním a současně nejčastěji se vyskytujícím obecným nedostatkem žádostí je nesprávné, nedostatečné nebo zcela chybějící odkazování na dokládané dokumenty a jejich **konkrétní části**. Je důsledkem nedodržení obecného požadavku uvedeném v § 9 odst. 4 vyhlášky, který stanovuje, že v případě, že je pro doložení splnění jednotlivých požadavků nezbytné odkázat do jiného dokumentu, který je k formuláři žádosti připojen, provede se tak ve formuláři **uvedením kapitoly, strany, odstavce a případně i konkrétní věty**.

Při dokládání jednoho požadavku vícero dokumenty je nutné uvést ve formuláři všechny tyto dokumenty a důsledně u každého z nich konkretizovat jeho část, ze které splnění požadavku vyplývá (uvedením kapitoly, strany, odstavce a případně i konkrétní věty). V případě dokládání jednoho požadavku vícero dokumenty je rovněž vhodné ve formuláři ke každému odkazovanému dokumentu uvést, jaká část požadavku je daným dokumentem dokládána.

Kromě správného dokládání dokumentů a lepší specifikace jejich relevantních částí, ze kterých splnění příslušných požadavků vyplývá, je rovněž třeba na připojené dokumenty odkazovat pouze v případech, kdy je to nezbytné k doložení splnění požadavků. Poskytovatelé v řadě případů odkazují

na dokumenty, které nejsou pro doložení splnění požadavků relevantní. Tomuto je třeba se vyvarovat, neboť to způsobuje nepřehlednost žádosti a prodlužuje celé řízení.

Se způsobem odkazování na dokumenty se pojí také nutnost dodržet **jednotné pojmenování dokládaných dokumentů**, resp. ve formuláři uvádět skutečné názvy dokládaných dokumentů a tyto nijak neupravovat ani nezkracovat.

Pro názornost uvádíme příklady správného a špatného odkazování:

Příklad č.1

- **Jak je to správně:**

„Závazek ukládání zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu je obsažen ve smluvní dokumentaci – viz čl. 8. odst. 5 na str. 10 dokumentu ID1.2_02_Contractual Terms. Úplný výčet datových center a jejich lokace po úroveň katastrálního území nebo obce, ve kterých jsou zákaznická data uložena ve stavu neaktivních dat, je obsažen v auditní zprávě ISO 27001 – viz str. 3 dokumentu ID1.2_01_Auditni-zprava.“

- **Jak to vypadat nemá:**

„Splnění požadavku najdete v návrhu smlouvy a v dokumentu ID1.2-Auditni-zprava.“

Příklad č. 2

- **Jak je to správně:**

„Šifrování zákaznického obsahu při přenosu v souladu s doporučením NÚKIB vyplývá ze str. 3, kap. „xy“ dokumentu „technická_dokumentace“. Šifrování zákaznického obsahu v uložišti v souladu s doporučením NÚKIB vyplývá ze str. 5, kap. „yx“ dokumentu „technická_dokumentace“. Ze str. 8, kap. „yy“ dokumentu „technická_dokumentace“ vyplývá, že poskytovatel zákazníkovi umožňuje výběr těch šifrovacích sad, které aplikují algoritmy schválené v doporučení NÚKIB.“

- **Jak to vypadat nemá:**

„Splnění požadavku vyplývá z dokumentu „název_smluvní_dokumentace“.“

3.4.2 Špatná forma či formát dokumentu

Jedná se o nedostatek, kdy poskytovatel dokládá splnění určitého požadavku vyhlášky **formou dokumentu, který však vyhláška pro doložení daného požadavku nepřipouští**. Při zpracovávání žádosti je třeba důkladně číst jak samotný požadavek vyhlášky, tak i věnovat dostatečnou pozornost sloupci „Podklad, kterým poskytovatel doloží splnění požadavku“, ve kterém **vyhláška specifikuje, jaká forma podkladu je pro doložení daného požadavku vyžadována**. Pro úspěšné doložení splnění jednotlivých požadavků vyhlášky je nutné se tímto striktně řídit.

Typicky se setkáváme s tím, že poskytovatelé dokládají čestná prohlášení k požadavkům, u kterých však vyhláška tuto formu dokumentu pro doložení splnění daného požadavku nepřipouští. Příkladem lze uvést požadavek řádku 4.1 přílohy č. 3 vyhlášky. U tohoto požadavku ve sloupci „Podklad, kterým poskytovatel doloží splnění požadavku“ vyhláška stanovuje, že poskytovatel musí doložit plány zajištění kontinuity provozu a na obnovu po havárii, nebo auditní zprávu. Poskytovatel tedy nemůže tento požadavek doložit např. výše zmiňovaným čestným prohlášením, ve kterém deklaruje existenci požadovaných plánů, a nemůže jej doložit ani písemným popisem, smluvní dokumentací či další dokumentací. Tyto formy dokumentů pro doložení nebudou akceptovány, jelikož je třeba v souladu s vyhláškou doložit buď samotné plány nebo alternativně auditní zprávu, ze které vyplývá existence těchto plánů.

Obecným nedostatkem souvisejícím s formátem dokládaných dokumentů jakožto příloh k formulářové žádosti je nesplnění požadavku na jejich **strojovou čitelnost umožňující fulltextové vyhledávání**. **Akceptovány nejsou ani odkazy na webové stránky**, neboť tyto nezaručují neměnnost jejich obsahu v čase. Odkaz na webovou stránku lze nahradit doložením jejího snímku, který již požadavek na neměnnost obsahu v čase splňuje. V souladu se správním řádem rovněž **nejsou přijímány zaheslované dokumenty**. Zaheslované dokumenty nejsou vhodné ke zjištění stavu věci, protože do zaheslovaných souborů nemá Úřad (případně další orgány s need-to-know) bez dalšího přístup. Při dokládání požadavků vyhlášky je tedy nutné dokládat pouze nezaheslované soubory, aby bylo možné bez dalšího jasně posoudit splnění jednotlivých požadavků ze strany Úřadu.

3.4.3 Nekonzistentnost v pojmenování služeb

Tento nedostatek vzniká, pokud se poskytovatel v rámci žádosti **nedrží jednotného pojmenování služeb**, které žádá zapsat. Setkáváme se například s tím, že poskytovatel ve formuláři žádosti v záložkách „IaaS-PaaS“ a “SaaS a smíšené moduly“ uvádí jiné názvy služeb, než uvádí v záložkách „Podklady k ověření IaaS-PaaS“ a „Podklady k ověření SaaS“. Rovněž se tento nedostatek projevuje nesouladem mezi názvy služeb, které poskytovatel uvede ve formuláři žádosti, a jejich názvy, které jsou uvedeny v dokumentech, které poskytovatel připojuje k formuláři žádosti za účelem prokázání splnění jednotlivých požadavků vyhlášky (ve smluvních dokumentacích, certifikátech atp.). Taktéž platí, že názvy služeb by v rámci žádosti a v dokládaných dokumentech neměly být zkracovány, překládány do českého jazyka a neměly by obsahovat překlepy. V opačném případě mohou tyto nedostatky vyvolávat pochybnosti o určitosti vymezení zapisovaných služeb, komplikují vyhledávání a způsobují nepřehlednost žádosti. Poskytovatel může nesrovnalosti v pojmenování služeb zhojit

dokumentem, který účelově popíše označení, zkratky a cizojazyčná znění služeb, pokud tento dokument zajistí jednoznačnou identifikaci služby v souladu s formulářem DIA.

- **Pro názornost uvádíme příklad toho, jak to vypadat nemá:**

Označení služby ve formuláři žádosti v záložce "SaaS a smíšené moduly": „*Spisová služba Pro*"

Označení služby ve formuláři žádosti v záložce „Podklady k ověření SaaS": „*Spisová služba*"

Označení služby v doloženém dokumentu za účelem doložení splnění požadavku vyhlášky (např. certifikát, návrh smlouvy): „*Spisová služba Pro (SSP)*"

- Přestože se jedná o mírné odchylky v názvu a dá se předpokládat, že se jedná o tutéž službu, nelze takové doložení akceptovat a poskytovatel bude vyzván k objasnění. V rámci správního řízení není možné dovozovat, naopak musí být postaveno najisto, že dokládané skutečnosti se vztahují k zapisované službě.

Jestliže rozdělujete nabízené služby do balíčků služeb, musíte tyto **balíčky služeb jednoznačně definovat**. Někteří poskytovatelé dokládají dokumenty, které se vztahují k celému balíčku služeb, ale nejsou v nich jmenovány služby jednotlivě. V takovém případě je klíčové, aby byly v každém předloženém podkladu (nebo v přiloženém seznamu) všechny dotčené služby uvedeny jmenovitě. Pokud z dokumentace není jasné, na které konkrétní služby se vztahuje, nelze ji jako důkaz o splnění požadavku uznat. Tento nedostatek můžete napravit přiložením samostatného písemného popisu nebo čestného prohlášení, ve kterém jasně deklarujete seznam služeb, pro které daný podklad dokládáte. Zvláštní pozornost je třeba věnovat certifikátům (např. ISO) a auditním zprávám (např. SOC 2 Type 2), které často uvádějí jen obecný rozsah činností poskytovatele, ale nejmenují jednotlivé služby. Pokud tyto dokumenty neobsahují konkrétní názvy vašich služeb, je třeba k nim přiložit čestné prohlášení, ve kterém potvrdíte, že se daná certifikace nebo audit vztahuje i na tyto konkrétní služby. Cílem tohoto postupu je zajistit, aby v katalogu byla u každé služby jasně prokazatelná její bezpečnostní úroveň a způsob, jakým splňuje požadavky.

3.4.4 Chybějící nebo nejasná vazba prokazovaných skutečností na zapisované služby

Při dokládání splnění požadavků je klíčové, aby byla **vazba mezi předloženými dokumenty a konkrétními službami v nabídce zcela jednoznačná**. Dokumentace, kterou předkládáte za účelem prokázání splnění požadavků vyhlášky, musí vždy pokrývat celý rozsah zapisovaných služeb. Pokud se doložený podklad vztahuje pouze na část vaší nabídky, je z pohledu vyhlášky považován za neúplný. V praxi to znamená, že buď musí jeden dokument prokazatelně pokrývat všechny služby v žádosti nebo je třeba pro různé skupiny služeb doložit podklady samostatné. Pravidla dokládání požadavků vám sice umožňují využít jeden společný dokument pro více služeb najednou, ale i v tomto případě musíte v dokumentu jmenovitě uvést každou jednu službu, na kterou se toto doložení vztahuje. Jen tak lze zajistit, že u žádné služby v katalogu nezůstane pochybnost o tom, zda a jakým způsobem všechna bezpečnostní kritéria skutečně splňuje. Cílem této vazby je zajistit

přehlednost a srozumitelnost evidence, kterou vyhláška vyžaduje jako základní princip pro strukturu všech podkladů.

3.4.5 Nerespektování typu požadavku při dokládání

Tento nedostatek souvisí **s dvěma základními typy požadavků vyhlášky**. Jak je uvedeno v jedné z předchozích podkapitol, část požadavků vyhlášky vyžaduje po poskytovateli prokázat, že nějakou funkcionalitu v rámci zapisované služby **zajišťuje**, zatímco podstatou druhé skupiny požadavků je, že poskytovateli stačí doložit, že danou funkcionalitu **nabízí**. Častým nedostatkem souvisejícím s výše uvedeným je situace, kdy poskytovatel u požadavku na zajištění nějaké funkcionality dokládá, že tuto funkcionalitu zákazníkovi pouze nabízí a že bude aktivována až na základě zákazníkova požadavku. Takto doložený požadavek na zajištění nelze akceptovat. Při zpracovávání žádosti je tedy nezbytné pozorně číst jednotlivé požadavky a při dokládání požadavku vždy zohlednit, zda daný požadavek vyžaduje prokázat, že něco zajišťujete, nebo stačí doložit, že požadované jste schopni zákazníkovi nabídnout.

- **Pro názornost uvádíme příklad toho, jak to vypadat nemá:**

Požadavek řádku 7.1 přílohy č. 2 vyhlášky: *Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí.*

Poskytovatel dokládá smluvní dokumentaci a odkazuje na část, ve které je uvedeno: „*Na základě požadavku zákazníka poskytovatel ve službě cloud computingu implementuje nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí.*“

- Takto doložený požadavek řádku 7.1 přílohy č. 2 vyhlášky nebude akceptován, jelikož poskytovatel musí doložit, že nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí je v zapisované službě cloud computingu zaveden nezávisle na požadavku zákazníka.

3.4.6 Chybějící odůvodnění při neuplatnění požadavku

Jestliže se určitý požadavek vyhlášky na některou ze zapisovaných služeb neuplatní, není dostačující do formuláře žádosti pouze uvést „*tento požadavek se neuplatní*“ nebo „*požadavek není pro danou službu relevantní*“. V takové situace je nutné dodržet následující postup. V první řadě je nutné v příslušné kolonce elektronického formuláře, případně v samostatném dokumentu, uvést informaci, že se daný požadavek neuplatní. Z této informace musí být vždy patrné, **ke které konkrétní službě** uvedené celým názvem se toto prohlášení vztahuje. Dále **je nutné důkladně zdůvodnit, proč tomu tak je**, tedy nestačí pouze uvést, že je požadavek irelevantní. Argumentace poskytovatele by měla vycházet z technické dokumentace nebo principu fungování služby. V ideálním případě by mělo dané tvrzení být rovnou podloženo přiloženým dokumentem (např. technickou specifikací).

3.4.7 Jiné pojmosloví

Jedná se o nedostatek projevující se tím, že poskytovatel ve formuláři žádosti a v dokumentech, které k žádosti připojuje za účelem prokázání splnění požadavků vyhlášky, používá **jiné pojmosloví, než se kterým pracuje vyhláška** (pojmosloví se věnuje jedna z předchozích podkapitol). V důsledku toho vzniká nejistota ohledně toho, zda poskytovatel dokládá úplné splnění jednotlivých požadavků. Velmi často se setkáváme s tím, že poskytovatel dokládá dokument obsahující pojem osobní údaj, ačkoliv požadavek požaduje doložení splnění pro zákaznická data či specifické provozní údaje, což nejsou obsahově nutně překrývající se pojmy. Je ideální, pokud vaše dokumentace využívá stejnou terminologii jako vyhláška. Pokud ve své interní dokumentaci využíváte jiné pojmosloví, **je nutné v žádosti výslovně objasnit, že se vámi používané pojmy obsahově shodují s těmi ve vyhlášce**.

4 Stručný výčet požadavků

Pro lepší přehlednost je v této kapitole uveden stručný výčet požadavků definovaných v jednotlivých přílohách vyhlášky v rámci jednotlivých bezpečnostních úrovní. Cílem této části je poskytnout rychlou orientaci a umožnit snadnou komparaci požadavků napříč bezpečnostními úrovněmi.

Následující tabulky jsou koncipovány jako přehledová matice, která obsahuje:

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

4.1 Místo zpracování a uložení dat

Lokalita správy a dohledu	1.1	1.1	1.1	1.1
Lokalita uložení a zpracování dat	1.2	1.2		
Uložení zákaznických dat na území EU/ESVO (výjimka možná) a výčet datových center			1.2	
Uložení specifických provozních údajů na území EU/ESVO (výjimka možná) a výčet datových center			1.3	
Zpracování zákaznických dat na území EU/ESVO (výjimka možná)			1.4	
Zpracování specifických provozních údajů na území EU/ESVO (výjimka možná)			1.5	
Režim zpracování dat mimo EU/ESVO a správa souhlasů zákazníků			1.6	
Zpracování zákaznických dat a specifických provozních údajů na území ČR (výjimka možná)				1.2

4.2 Žádosti o zpřístupnění a předání dat

Přezkum zákonnosti a informování zákazníka při žádostech cizích orgánů o zpřístupnění dat zákazníka	2.1	2.1		
Přezkum zákonnosti, informování zákazníka a aktivní právní odpor při žádostech cizích orgánů o zpřístupnění dat zákazníka			2.1	
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

4.3 Oprávnění k provedení kontroly

Přezkum zákonnosti a informování zákazníka při žádostech cizích orgánů o zpřístupnění dat zákazníka	3.1	3.1	3.1	3.1

4.4 Zajištění poskytování služby

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 v ČR nebo alespoň dvou státech EU/ESVO			4.4	
Umístění datacenter v ČR				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

4.5 Nakládání s daty

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		
Šifrování - při všech síťových přenosech a v uložišti			5.2	
Automatické (by default) šifrování - při všech síťových přenosech a v uložišti				5.2
Šifrování dle doporučení NÚKIB - v síti (mimo kontrolu poskytovatele) a v uložišti		5.3		
Šifrování dle doporučení NÚKIB - při všech síťových přenosech a v uložišti			5.3	5.3
Podpora vlastních šifrovacích klíčů a správa v HSM modulu			5.4	
Bezpečná likvidace šifrovacích klíčů			5.5	
Certifikované HSM moduly a správa klíčů				5.4

4.6 Certifikace služby

Soulad s ISMS dle ISO 27001 nebo režimem nižších povinností	6.1			
Certifikace ISO/IEC 27001 a ISO/IEC 27017		6.1		
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

4.7 Kybernetické bezpečnostní události a incidenty

Nástroj pro sledování a vyhodnocování kybernetických událostí	7.1			
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

4.8 Testování služby

Skenování zranitelností	8.1	8.1	8.1	8.1
Penetrační testování			8.2	
Penetrační testování				8.2

4.9 Připojení do výměnného uzlu internetu

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

5 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