PORTÁL NÚKIB

Mapování bezpečnostních opatření dle prováděcího nařízení pro poskytovatele digitálních služeb a vyhlášky č. 409/2025 Sb.

TLP:CLEAR

24. února 2026

Verze 1.0

Národní úřad
pro kybernetickou
a informační bezpečnost

Obsah

1 Co se dozvím v tomto dokumentu?

Tento průvodní dokument obsahuje informace týkající se vzájemných provazeb bezpečnostních opatření dle prováděcího nařízení komise (EU) 2024/2690 (dále jen „prováděcí nařízení“) a bezpečnostních opatření dle vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „vyhláška“).

Pokud máte jakékoliv další otázky, podívejte se na www.portal.nukib.gov.cz nebo nám napište 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 Pro koho je dokument určen

Prováděcí nařízení je evropský předpis, který navazuje na směrnici NIS2 a stanovuje konkrétní pravidla pro zajištění kybernetické bezpečnosti u tzv. poskytovatelů digitálních služeb. Dle § 18 zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „zákon“) se prováděcím nařízením musí řídit poskytovatelé:

- služby **systému překladu doménových jmen**[1]**,**
- služby **správy a provozu registru domény nejvyšší úrovně,**
- služby **cloud computingu,**
- služby **datových center,**
- služby **sítě pro doručování obsahu,**
- **řízené služby,**
- **řízené bezpečnostní služby,**
- služby **on-line tržišť, internetových vyhledávačů a platforem sociálních sítí a,**
- služby **vytvářející důvěru.**

Podrobnější informace lze nalézt v podpůrném materiálu Definice regulovaných služeb v odvětví Digitální infrastruktura a služby.

Nařízení zejména určuje, jak mají poskytovatelé uvedených služeb řídit svá rizika, zavádět bezpečnostní opatření (výběr vhodných a přiměřených opatření se provede na základě výsledků hodnocení rizik) a za jakých okolností se kybernetický incident považuje za významný. Cílem prováděcího nařízení je sjednotit postupy v rámci Evropské unie a zvýšit odolnost digitální

[1] S výjimkou služby poskytované jako součást regulované služby podle bodu 16.1 dle vyhlášky č. 408/2025 Sb., o regulovaných službách.

infrastruktury proti kybernetickým hrozbám. Požadavky nařízení jsou v mnoha aspektech podobné s požadavky vyhlášky.

NÚKIB proto připravil tento dokument, který přibližuje provazby mezi prováděcím nařízením a vyhláškou. Dokument je užitečný především pro ty subjekty, u kterých dojde k souběhu poskytování jedné z výše uvedených digitálních služeb s poskytováním jiné regulované služby v režimu vyšších povinností.

3 K čemu dokument slouží

Tento dokument obsahuje přílohu s přehledem provazeb mezi prováděcím nařízením a vyhláškou a způsoby plnění bezpečnostních opatření. Cílem je usnadnit zavádění bezpečnostních opatření v organizacích, kde může dojít k překryvu bezpečnostních opatření podle prováděcího nařízení a vyhlášky.

3.1 Disclaimer a co naleznete v příloze

Pro vytvoření provazeb mezi nařízením a vyhláškou byl využitý výkladový materiál k prováděcímu nařízení ENISA – Technical Implementation Guidance, který naleznete níže v odkazech, dále bylo vycházeno z dosavadní praxe a odborných znalostí autorů tohoto dokumentu.

Je třeba upozornit, že při implementaci bezpečnostních opatření bude vždy záležet na kontextu konkrétního poskytovatele digitální služby, jeho bezpečnostních potřebách a provedeném hodnocení rizik.

V příloze tohoto dokumentu naleznete excelový soubor s tabulkami, na jehož jednotlivých listech se nachází rozepsaná bezpečností opatření z nařízení a vyhlášky. V těchto listech se lze orientovat dle sloupce „ID“, kde jsou jednotlivá čísla pro každé bezpečností opatření. Ve sloupci „ID bezpečnostního opatření“ lze nalézt možnou provazbu mezi nařízením a vyhláškou, případně naopak. Je nutné upozornit, že některé ID jsou provázány pouze s jedním bezpečnostním opatřením, zatímco jiné mohou mít vazeb více.

3.2 Legenda dokumentu

V případě, že bezpečností opatření mají vzájemnou provazbu, tedy bylo nalezeno možné propojení a podoba jednotlivých regulací, jsou zobrazeny jako zelené. V případech, kdy požadavky byly příliš odlišné nebo se v porovnávané regulaci vůbec nenacházejí, jsou zobrazeny jako červené, a tudíž není mezi prováděcím nařízením a vyhláškou u konkrétního bezpečnostního opatření žádné propojení. Šedá pole jsou vyznačena jako požadavek, který je příliš obecný, slouží spíše jako nadpis, a člení se až v následujících bezpečnostních opatřeních.

Zelená	**Shoda**, nalezena možná provazba. Bezpečnostní opatření je požadavkem nařízení i vyhlášky č. 409/2025 Sb.
Červená	**Shoda není**, nebyla nalezena žádná provazba
Šedá	**Nejedná se o konkretizovaný požadavek na aplikaci bezpečnostního opatření** (zpravidla se jedná o nadpis oddělující jednotlivé typy bezpečnostních opatření)

3.3 Užitečné odkazy

Regulace poskytovatelů digitálních služeb | Portál NÚKIB

https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/ces

NZKB 7. díl – Poskytovatelé digitálních služeb

4 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**
24. února 2026	1.0	OK	Vytvoření dokumentu