PORTÁL NÚKIB

Doporučení k (ne)poskytování informací v oblasti kybernetické bezpečnosti a bezpečnosti systémů nakládajících s utajovanými informacemi

TLP:CLEAR

16. dubna 2026

Verze 1.1

Národní úřad pro kybernetickou a informační bezpečnost

Obsah

1 Co se dozvím v tomto dokumentu?

Materiál se věnuje výjimkám z práva na informace v oblasti kybernetické bezpečnosti, které vycházejí z ustanovení § 36 zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jako **„zákon o kybernetické bezpečnosti“**), z ustanovení § 11 odst. 1 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím (dále jako **„zákon o svobodném přístupu k informacím“**), a také ze zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jako **„zákon o ochraně utajovaných informací“**).

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 Manažerské shrnutí dokumentu

Výjimky z práva na informace se v oblasti kybernetické bezpečnosti opírají o tři klíčové právní předpisy.

Za prvé, **§ 36 zákona o kybernetické bezpečnosti** stanovuje, že všechny informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, se neposkytují, a dále se neposkytují ty informace, které jsou v evidencích vedených Národním úřadem pro kybernetickou a informační bezpečnost (dále jako „Úřad“).

Za druhé, **§ 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím** umožňuje omezení poskytnutí informací, pokud by jejich zpřístupnění významně či přímo ohrozilo účinnost bezpečnostního opatření stanoveného podle zvláštního předpisu.

Za třetí, **zákon o ochraně utajovaných informací** poskytuje rámec pro identifikaci a zabezpečení informací, jejichž zveřejnění by mohlo způsobit újmu zájmům České republiky; tyto informace musí splňovat materiální i formální kritéria a být zpracovávány s přísnými technickými a personálními bezpečnostními opatřeními.

Společně tyto tři pilíře zajišťují, že povinné subjekty mohou chránit citlivé informace. Vždy je nutné **individualizované, přiměřené a přezkoumatelné odůvodnění** rozhodnutí o neposkytnutí informací a minimalizace zásahu do práva na informace prostřednictvím částečného zpřístupnění, anonymizace či zobecnění dat.

3 Výjimky z poskytování informací podle zákona o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti stanovuje, kdy povinné osoby podle zákona o svobodném přístupu k informacím nesmí určité informace poskytnout. Neposkytnutí informací musí být vždy řádně a prokazatelně odůvodněno a vycházet ze zákonných důvodů. Tato výjimka z práva na informace je obecně v souladu s čl. 17 odst. 4 Listiny základních práv a svobod, protože v určitých případech převáží ochrana kybernetické bezpečnosti, tedy bezpečnost státu a veřejnosti, nad právem na informace. Odmítnutí žádosti o informace musí vždy obsahovat přezkoumatelnou úvahu o nezbytnosti omezení.

Zákonné důvody pro odmítnutí žádosti o informace podle zákona o svobodném přístupu k informacím jsou uvedena přímo v § 36 zákona o kybernetické bezpečnosti:

> *„Informace, jejichž zpřístupnění by mohlo **ohrozit zajišťování kybernetické bezpečnosti**, nebo informace, které jsou **vedené v evidencích vedených Úřadem podle § 46**, se podle právních předpisů upravujících svobodný přístup k informacím a právo na informace o životním prostředí **neposkytují**.“*

Z ustanovení plyne, že se neposkytují dva typy informací:

1) Informace, jejichž zpřístupnění by mohlo **ohrozit zajišťování kybernetické bezpečnosti.**
2) Informace, které jsou vedené v **evidencích vedených Úřadem** podle § 46 zákona o kybernetické bezpečnosti.

Neposkytnutí informací z těchto důvodů musí být každopádně řádně odůvodněno (viz dále).

3.1 Ohrožení zajišťování kybernetické bezpečnosti

Podle prvního pravidla nesmí být informace zpřístupněna, pokud by její poskytnutí mohlo ohrozit zajišťování kybernetické bezpečnosti. Zhodnocení toho, zda zveřejnění určité informace představuje riziko, se odvíjí od její povahy a od toho, jaký může mít dopad na zajištění bezpečnosti daného subjektu.

Při hodnocení je vhodné zohlednit:

- **Obsah informace:** zejména detaily o bezpečnostních opatřeních, technická schémata a postupy, které by mohly být zneužity.
- **Souvislost s kybernetickou bezpečností:** informace musí být relevantní pro ochranu či fungování bezpečnostních opatření.
- **Pravděpodobnost ohrožení:** postačuje reálná možnost ohrožení, nikoliv jeho jistota.

Správně provedená **vnitřní klasifikace informací** poskytovatele regulované služby je doporučeným nástrojem pro aplikaci tohoto pravidla. Zákon nevymezuje konkrétní typy informací, ale jejich povahu, tedy potenciál ohrozit kybernetickou bezpečnost. Přesto lze vymezit oblasti, u kterých je nutné dbát zvýšené opatrnosti:

- **Informace o bezpečnostních opatřeních**: konkrétní podoba opatření, konfigurace technických a organizačních prvků.
- **Informace o zranitelnostech**: výsledky auditů, testování systémů.
- **Technické informace**: segmentace systémů, vazby, architektura, rozhraní.
- **Informace o řízení přístupů a oprávnění**: role, oprávnění, procesy schvalování.
- **Informace o kybernetických incidentech**: postupy detekce, monitoringu a řešení incidentů.
- **Informace o aktuálním stavu zabezpečení**: fáze implementace opatření, verze software.

Při soudním přezkumu odmítnutí žádosti o informace na základě tohoto pravidla je klíčové konkrétní odůvodnění, tedy které části informací mohou ohrozit kybernetickou bezpečnost a jaké konkrétní hrozby by jejich zveřejnění představovalo. Neposkytnutí nesmí být zobecněné na celý dokument bez dalšího, soudy v odůvodnění vyžadují rozlišení jednotlivých částí, například technických detailů a obecných závěrů. Je chybou, je-li test proporcionality proveden formálně, bez konkrétního posouzení jednotlivých informací a odůvodnění, proč veřejný zájem ustupuje.

Princip **minimalizace zásahu do práva na informace** znamená zkoumat možnosti:

- poskytnutí pouze části informace,
- anonymizaci či zobecnění dat,
- oddělení technických detailů od hodnotících závěrů.

Při uplatnění výjimky je nezbytné provést **test proporcionality**, který zahrnuje:

1. **Vhodnost:** skutečně by zveřejnění ohrozilo kybernetickou bezpečnost?
2. **Nezbytnost:** nelze použít mírnější opatření (např. částečné poskytnutí)?
3. **Přiměřenost:** nepřevažuje veřejný zájem nad ochranou bezpečnosti?

Odůvodnění uplatnění výjimky musí být konkrétní, individualizované a přezkoumatelné. Povinné subjekty musí jasně uvést, které části informací naplňují výjimku a jak by jejich zveřejnění ohrozilo kybernetickou bezpečnost. Neposkytnutí nelze odůvodnit pouze obecným vztahem k bezpečnosti, vždy je nutné posoudit povahu konkrétní informace.

Původní výjimka z práva na informace podle § 10a zákona č. 181/2014 Sb., o kybernetické bezpečnosti, stanovovala také, že se informace neposkytne, pokud by její zpřístupnění mohlo ohrozit účinnost protiopatření vydaného podle tohoto zákona. Tuto specifickou výjimku je nyní možné uplatnit v rámci obecné výjimky popsané v této kapitole. **Rozsah původní výjimky tedy nebyl zúžen**, pouze není nadále explicitně zmíněna specifická situace týkající se protiopatření.

3.1.1 Režim vyšších povinností

Podle vyhlášky č. 409/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, je poskytovatel povinen hodnotit aktiva z hlediska důvěrnosti, integrity a dostupnosti a zařazovat je do příslušných úrovní (viz příloha č. 1 této vyhlášky).

Pro klasifikaci důvěrnosti informací a dat pro účely jejich sdílení lze využít mezinárodní standard Traffic Light Protocol (TLP). Při posuzování, které informace by mohly ohrozit zajišťování kybernetické bezpečnosti, je vhodné přihlížet k úrovni důvěrnosti dané informace. O neposkytnutí lze při zohlednění dalších výše zmíněných kritérií uvažovat u aktiv s úrovní „vysoká“ nebo „kritická“ (viz příloha č. 1, tabulka č. 1 vyhlášky).

3.1.2 Režim nižších povinností

V nižším režimu povinností vyhláška č. 410/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností nestanovuje povinnost klasifikovat informace dle důvěrnosti, jako je tomu v režimu vyšších povinností. To samozřejmě nevylučuje, že si poskytovatel zavede interní klasifikaci důvěrnosti informací dobrovolně.

Poskytovatel regulované služby v režimu nižších povinností může uvažovat o uplatnění výjimky z práva na informace v souvislosti s konkrétními povinnostmi a bezpečnostními opatřeními, které dle zákona a navazující vyhlášky plní a zavádí. Například:

- **Řízení přístupu**: informace se neposkytne, protože její znalost je určená jen konkrétní osobě a její znalost dalšími osobami by mohla ohrozit zajišťování kybernetické bezpečnosti.
- **Řešení kybernetických bezpečnostních incidentů**: zpřístupnění informace by zvýšilo pravděpodobnost incidentu tím, že odhalí slabá místa systému.
- **Pravidla pro technická aktiva / segmentace sítě**: poskytnutí informace určené pouze pro interní provozní účely a které by mohlo ohrozit zajišťování kybernetické bezpečnosti.

3.2 Informace vedené v evidencích Úřadu podle § 46

Druhé pravidlo pro uplatnění výjimky z práva na informace se vztahuje na informace, které jsou vedené v evidencích Úřadu podle § 46 zákona o kybernetické bezpečnosti. U těchto informací platí z jejich povahy, že by jejich zpřístupnění vždy mohlo ohrozit zajišťování kybernetické bezpečnosti. Pro účely zvýšení právní jistoty a předvídatelnosti je tato výjimka v § 36 zákona o kybernetické bezpečnosti explicitně uvedena, přestože by bylo možné ji dovozovat z prvního obecnějšího pravidla.

Zákon důsledně rozlišuje mezi pojmem evidence a pojmem seznam. Na seznamy se uvedená výjimka neuplatní (jedná se o veřejné informace). **Výčet evidencí je taxativní** a je uveden v samostatném ustanovení. Výjimka z práva na informace se tedy vztahuje na informace vedené v evidencích:

- regulovaných služeb včetně jejich poskytovatelů a jimi hlášených údajů,
- osob poskytujících služby registrace doménových jmen a jimi hlášených údajů,
- kybernetických bezpečnostních incidentů, událostí, hrozeb a zranitelností,

- dodavatelů bezpečnostně významných dodávek,
- koordinovaného zveřejňování zranitelností,
- penetračních testů a
- provedených kontrol a protokolů o kontrole.

4 Výjimka z poskytování informací podle zákona o svobodném přístupu k informacím

Zákon o svobodném přístupu k informacím podle § 11 odst. 1 písm. d) umožňuje povinnému subjektu omezit poskytnutí informace, pokud její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro ochranu bezpečnosti osob, majetku a veřejného pořádku.

Pojem bezpečnostní opatření zahrnuje všechna opatření zaměřená na zajištění bezpečnosti státu i soukromých subjektů. V praxi jde o citlivé informace, které nejsou utajované, ale jejich zveřejnění by bylo nežádoucí, např. detaily ostrahy objektů, strategické či taktické postupy bezpečnostních sborů nebo informace, jejichž zveřejnění by ohrozilo kybernetickou bezpečnost.

Ochranu získávají pouze informace, u nichž lze prokázat alespoň jeden z těchto rysů:

- **významné ohrožení účinnosti**: zveřejnění by samo o sobě znemožnilo dosažení chráněného účelu (např. ohrožení ostrahy budov),
- **přímé ohrožení účinnosti**: ohrožení nastává přímo, bez nutnosti řady dalších informací a zjištění, náročné analýzy, filtrace a separace údajů apod.

Dalším vymezujícím kritériem je **nezbytnost** opatření. Není přiměřené chránit informace jen proto, že subjekt zavedl mimořádně komplikované či sofistikované bezpečnostní opatření, pokud jeho rozsah není nezbytný. Existuje úměrnost mezi účinností opatření a dostupností informací, chránit lze pouze opatření nezbytná, což odpovídá ústavnímu principu proporcionality podle čl. 17 odst. 4 Listiny základních práv a svobod.

Informacemi o bezpečnostních opatřeních podle § 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím se nerozumí pouze informace o fyzických bezpečnostních opatřeních, ale i informace o ochraně IT infrastruktury a digitálních systémů. Informace technického charakteru (např. IP adresa serveru, na který jsou odesílána data z dopravního radaru), proto povinný subjekt nemusí poskytnout, pokud by jejich zveřejnění mohlo usnadnit narušení nebo obcházení systému. V případě dopravního radaru by poskytnutí IP adresy serveru mohlo umožnit kybernetický útok, který by znemožnil přenos záznamů o překročení rychlosti, a tím zásadně omezil nebo zcela ochromil jeho funkci (blíže viz rozsudek Nejvyššího správního soudu ze dne 26. března 2026, č. j. 1 As 208/2025 - 38)

Na základě těchto zásad lze omezit právo na informace i u bezpečnostních opatření podle § 14 zákona o kybernetické bezpečnosti, pokud jejich zpřístupnění může významně nebo přímo ohrozit účinnost bezpečnostních opatření a zároveň je nezbytné.

5 Poskytování informací v oblasti bezpečnosti systémů nakládajících s utajovanými informacemi

Pro úplnost je třeba zmínit, že další možností ochrany je utajení informací podle zákona o ochraně utajovaných informací a nařízení vlády č. 440/2024 Sb., o katalogu oblastí utajovaných informací, kterým se stanoví seznam utajovaných informací.

Podle § 2 písm. a) zákona o ochraně utajovaných informací se **utajovanou informací rozumí** *„informace v jakékoliv podobě a na jakémkoliv nosiči, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo být pro tento zájem nevýhodné, a kterou lze podřadit pod položku uvedenou v katalogu oblastí utajovaných informací.“*

Stupně utajení podle § 3 zákona o ochraně utajovaných informací jsou **přísně tajné, tajné, důvěrné a vyhrazené**, s ohledem na možnou újmu zájmu ČR či nevýhodnost pro zájmy ČR.

Katalog oblastí utajovaných informací v příloze nařízení vlády č. 440/2024 Sb. obsahuje mj. oblast **05. Kybernetická a informační bezpečnost**. Informace týkající se kybernetické bezpečnosti jsou však uvedeny také v dalších oblastech katalogu.

Pro utajení musí být splněna současně **materiální a formální kritéria** – informace musí být uvedena v katalogu utajovaných informací a zároveň musí splňovat materiální stránku podle § 2 a § 3 zákona o ochraně utajovaných informací.

Před zavedením ochrany utajovaných informací je třeba zohlednit finanční, personální i technické nároky. Informace mohou být zpracovávány pouze v certifikovaných informačních systémech a přístup k nim mají mít pouze osoby s bezpečnostní prověrkou odpovídající konkrétnímu stupni utajení. To platí pro interní zaměstnance i externí dodavatele či další dotčené subjekty.

Ochrana utajovaných informací zahrnuje opatření v oblasti:

- personální a průmyslové bezpečnosti,
- administrativní a fyzické bezpečnosti,
- bezpečnosti informačních a komunikačních systémů a
- kryptografické ochrany.

Tato opatření stanovuje zákon o ochraně utajovaných informací a jeho prováděcí předpisy. Na dodržování předpisů dohlíží Úřad a Národní bezpečnostní úřad.

Podle § 7 zákona o svobodném přístupu k informacím platí, že pokud je požadovaná informace označena jako utajovaná a žadatel k ní nemá oprávněný přístup, povinný subjekt informaci neposkytne.

6 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	OREG	Vytvoření dokumentu
16. dubna 2026	1.1	OREG	Doplnění kap. 4 (rozhodnutí NSS)