NÚKIB

DOPORUČENÍ

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

Verze 2.1, platná ke dni 22.12.2022

Obsah

Úvod

Dokument obsahuje informace o možnostech neposkytnout informaci podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, (dále jen „zákon o svobodném přístupu k informacím“) v oblasti kybernetické bezpečnosti a bezpečnosti systémů nakládajících s utajovanými informacemi, za zákonem předpokládaných důvodů.

Některé informace v oblasti kybernetické bezpečnosti sice nemusí být utajeny podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen „zákon o ochraně utajovaných informací“), avšak stále mohou být vysoce citlivé a jejich zveřejnění může mít dalekosáhlé bezpečnostní dopady. Také z těchto důvodů počítá jak zákon č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“), tak sám zákon o svobodném přístupu k informacím s důvody a situacemi, za nichž nemá být daná informace veřejně poskytnuta. Tyto případy jsou popsány v první kapitole tohoto dokumentu. Vztah poskytování informací podle zákona o svobodném přístupu k informacím a utajování informací podle zákona o ochraně utajovaných informací je pak popsán v druhé kapitole tohoto dokumentu.

Národní úřad pro kybernetickou a informační bezpečnost vydává toto doporučení z důvodu, že je ústředním správním úřadem pro oblast kybernetické bezpečnosti a pro vybrané oblasti ochrany utajovaných informací podle zákona o ochraně utajovaných informací.

Tento dokument nemá a nemůže mít za cíl poskytnout závazný výklad zákona o svobodném přístupu k informacím.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

E-mail: regulace@nukib.cz

Upozornění:

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.

1 Poskytování informací v oblasti kybernetické bezpečnosti

Omezení poskytování informací lze v oblasti kybernetické bezpečnosti s určitým zjednodušením rozdělit na omezení pro informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti „obecně“ (upraveno v § 10a zákona o kybernetické bezpečnosti), na omezení pro informace, jejichž zpřístupnění by mohlo ohrozit účinnost opatření vydaného podle zákona o kybernetické bezpečnosti (upraveno také v § 10a zákona o kybernetické bezpečnosti), a dále omezení pro informace, jejíž poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření podle zákona o kybernetické bezpečnosti [§ 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím].

1.1 Ustanovení § 10a zákona o kybernetické bezpečnosti – informace, jejíž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti

S účinností od 1. srpna 2017 bylo do zákona o kybernetické bezpečnosti zákonem č. 205/2017 Sb., kterým se mění zákon o kybernetické bezpečnosti a související zákony, zavedeno nové ustanovení, a to § 10a, v rámci kterého se zavádí výjimka ze zákona o svobodném přístupu k informacím.

Ustanovení § 10a zákona o kybernetické bezpečnosti zní:

„Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle tohoto zákona, nebo informace, které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila, se podle předpisů upravujících svobodný přístup k informacím neposkytují.“

Jak z tohoto ustanovení plyne, zákon o kybernetické bezpečnosti nařizuje některé informace podle zákona o svobodném přístupu k informacím neposkytovat, avšak toto neplatí neomezeně; neposkytnutí informací musí být mimo jiné řádně a prokazatelně odůvodněno a vycházet ze zákonných důvodů. Jak samo ustanovení zmiňuje, jedná se v zásadě o tři různé druhy informací:

- Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti;
- Informace, jejichž zpřístupnění by mohlo ohrozit účinnost opatření vydaného podle zákona o kybernetické bezpečnosti;
- Informace, které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila.

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Úřad“) **má za to, že pro posouzení a správné užití prvních dvou důvodů** (tedy možné ohrožení zajišťování kybernetické bezpečnosti nebo možné ohrožení účinnosti opatření vydaného podle zákona

o kybernetické bezpečnosti) **je velmi vhodným institutem správně provedená vnitřní klasifikace informací v rámci hodnocení aktiv podle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat** (dále jen „vyhláška o kybernetické bezpečnosti“).

Při posuzování, zda by poskytnutí určité informace mohlo ohrozit zajišťování kybernetické bezpečnosti, je nezbytné zvážit, které informace jsou z hlediska zachování kybernetické bezpečnosti natolik důvěrné, že by jejich vyzrazením mohlo dojít k jejímu narušení. Taková informace by měla z pohledu důvěrnosti odpovídat úrovni „*vysoká*“ nebo „*kritická*“ podle přílohy č. 1 vyhlášky o kybernetické bezpečnosti. Pokud by zpřístupněním takové informace mohlo dojít k narušení kybernetické bezpečnosti, je podle názoru Úřadu nezbytné aplikovat § 10a zákona kybernetické bezpečnosti a takovou informaci neposkytnout. Tímto způsobem je vhodné ohodnotit například technickou či bezpečnostní dokumentaci (jejichž ochrana je akcentována i skutečností, že v komplexní podobě mohou být chráněny i podle zákona o ochraně utajovaných informací).

Stejně tak je potřeba postupovat v případě informace, jejíž zpřístupnění by mohlo ohrozit účinnost opatření vydaného podle zákona o kybernetické bezpečnosti. Jak z ustanovení samotného plyne, bude se v tomto případě jednat o informaci, jejíž zveřejnění by mohlo mít negativní dopad na opatření vydané podle zákona o kybernetické bezpečnosti. Opatřeními jsou podle § 11 odst. 2 písm. a) až c) zákona o kybernetické bezpečnosti:

- Varování;
- Reaktivní opatření;
- Ochranné opatření.

Na tomto místě je potřeba především uvést, že orgány a osoby spadající pod zákon o kybernetické bezpečnosti jsou povinny bez zbytečného odkladu oznámit Úřadu provedení reaktivního opatření a jeho výsledek. Obsah tohoto oznámení tak může být právě onou informací, jejíž zpřístupnění by mohlo ohrozit účinnost opatření vydaného podle zákona o kybernetické bezpečnosti. Nemusí se však jednat pouze o obsah oznámení, ale i o další informace související s reálným prováděním vydaného opatření ve strukturách orgánů a osob, kterým bylo uloženo provést opatření.

Pokud určitá informace není hodnocena z pohledu důvěrnosti úrovní „*vysoká*“ nebo „*kritická*“, lze k ní přistupovat dvěma způsoby. První je, že informace nedosahuje z pohledu zajišťování kybernetické bezpečnosti takového významu, aby byla zákonem o kybernetické bezpečnosti speciálně chráněna. Není tedy možné využít ustanovení § 10a zákona o kybernetické bezpečnosti a informaci neposkytnout (může být ovšem možné ji neposkytnout z některých

z dále uvedených důvodů – viz níže). Druhou variantou je, že informace reálně může ohrozit zajišťování kybernetické bezpečnosti, ale není příslušně hodnocena (lze tedy předpokládat, že byla nevhodně hodnocena důležitost aktiv, v důsledku čehož došlo k neplnění nebo nedostatečnému plnění povinností uložených § 4 odst. 2 zákona o kybernetické bezpečnosti).

Je potřeba upozornit, že při případném soudním řízení o oprávněnosti neposkytnutí informace podle § 10a zákona o kybernetické bezpečnosti jsou předmětem soudního přezkumu zejména důvody neposkytnutí informací, tedy také to, zda informace naplní definici tohoto ustanovení zákona. Argumentace prostřednictvím klasifikace informací při hodnocení aktiv se tak *prima vista* jeví jako nezbytná. Avšak vzhledem k tomu, že dosud neexistuje soudní praxe k uplatňování této výjimky z práva na informace, nelze předvídat, zda budou soudy aplikovat spíše restriktivní výklad a využití § 10a zákona o kybernetické bezpečnosti akceptují pouze ve skutečně závažných případech, nebo budou naopak upřednostňovat veřejný zájem na zajištění kybernetické bezpečnosti informací a aplikaci § 10a zákona o kybernetické bezpečnosti akceptují i v méně závažných, až hraničních případech.

Co se týče třetího důvodu pro neposkytnutí informací podle § 10a zákona o kybernetické bezpečnosti, evidenci kybernetických bezpečnostních incidentů, o níž uvedené ustanovení hovoří, vede Úřad. Výjimka pro informace z evidence incidentů se tedy uplatní ve vztahu k informacím poskytovaným Úřadem, příp. dalšími osobami, které informacemi o evidovaných incidentech disponují (zejm. pokud jim byly Úřadem poskytnuty v rámci spolupráce správních orgánů nebo v rámci poskytování součinnosti orgánům činným v trestním řízení).

1.2 Ustanovení § 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím – informace, jejíž poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření

S účinností od 24. dubna 2019 došlo ke změně zákona o svobodném přístupu k informacím zákonem č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

Touto změnou došlo k zavedení nového omezení práva na informace ve vztahu k povinnostem ze zákona o kybernetické bezpečnosti, a to v rámci § 11 odst. 1 písm. d), který zní:

„Povinný subjekt může omezit poskytnutí informace, pokud: (…) její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku“.

Odůvodnění k tomuto ustanovení[1] uvádí následující:

„V novém písmenu d) je zaveden pojem "bezpečnostní opatření". Jedná se o neurčitý právní termín, jehož obsah bude moci být flexibilně vykládán a definován a má zahrnovat veškerá opatření, jejichž účelem je zajišťování bezpečnosti, a to jak na straně státu, tak i soukromých subjektů – povinným subjektem je sice veřejná instituce, ale poskytnutím informace může být ohroženo i bezpečnostní opatření soukromé. V praxi se bude jednat o informace, které sice nejsou utajované, ale i přesto jsou citlivé povahy a není žádoucí, aby vešly v obecnou známost. Například půjde o detaily ostrahy objektů, strategické a taktické postupy bezpečnostních sborů, informace, jejichž zveřejnění by mohlo ohrozit kybernetickou bezpečnost atd. Aby toto ustanovení nemohlo být nadužíváno či zneužíváno, musí jít o opatření, které má svůj podklad v zákoně. Např. půjde o § 4 zákona č. 181/2014 Sb. o kybernetické bezpečnosti, ve znění pozdějších předpisů; § 5 zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, (…)*; čl. 32 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2016/679, § 30 odst. 2 či § 44 navrženého zákona o zpracování osobních údajů apod."*

Z důvodu pouze minimálních odlišností od finálního návrhu je také vhodné mít na paměti odůvodnění původního návrhu uvedeného ustanovení[2]:

„Další konkretizací navržené výjimky jsou parametry významného nebo přímého účinku posuzované informace. Významné ohrožení účinnosti by mělo být takové, které by samo o sobě vedlo k nemožnosti zajistit chráněný účel. Například při ostraze budov by znamenalo úplnou nejistotu o tom, zda se do budovy dostane či dostala neoprávněná osoba, tedy například výpadek části senzorů, monitoringu apod., způsobený tím, že by se útočník dozvěděl údaje, které to umožní. Přímé ohrožení účinnosti by mělo být takové, které k ohrožení účinnosti bezpečnostního opatření vede přímo, tzn. nevyžaduje řady dalších informací a zjištění, náročné analýzy, filtrace a separace údajů apod. Ochranu by měly získat jen ty informace, u kterých lze prokázat kombinaci uvedených rysů – poskytnutí by významně a přímo ohrozilo účinnost bezpečnostního opatření, například v případě kybernetické bezpečnosti kybernetickou bezpečnost a bezpečnost sítí a informačních systémů. Dalším vymezujícím parametrem je ***nezbytnost opatření****. Nebylo by totiž přiměřené, pokud by se umožnilo rozsáhlé a neobvyklé utajování informací jen proto, že si některý povinný subjekt vytvořil natolik mimořádné,*

[1] Návrh tohoto ustanovení a jeho odůvodnění nebyly součástí původního návrhu č. 139/0, vládního návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, ale až součástí druhého pozměňovacího návrhu č. 1075 poslance Ondřeje Profanta k tomuto vládnímu návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, s. 4-5.

[2] Jde o první návrh znění řešeného ustanovení, který byl i s odůvodněním představen v rámci prvního pozměňovacího návrhu č. 971 poslance Ondřeje Profanta k vládnímu návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. Tento první návrh byl předložen ve znění: *„Povinný subjekt může omezit poskytnutí informace, pokud: (…) d) její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu x pro účel nezbytné ochrany osob, majetku, jakož i veřejného pořádku nebo bezpečnosti České republiky*". Návrh č. 971, s. 6-7.

komplikované či sofistikované bezpečnostní opatření, které již není nezbytné, ale jehož funkce je na mimořádném rozsahu utajování závislá. Vždy totiž existuje určitá úměrnost mezi účinností bezpečnostního opatření a tím, do jaké míry jsou o něm dostupné informace – čím méně dostupných informací, tím vyšší účinnost. Tak lze teoreticky eskalovat potřebu utajování do nekonečna. Takové opatření nemůže požívat ústavní ochranu a nemůže být oprávněným důvodem pro rozsáhlé utajování a omezení přístupu k informacím. Chránit lze toliko ***nezbytná*** *opatření, což mj. plyne z ústavní kautely v čl. 17 odst. 4 Listiny, kde se přístup k informacím umožňuje omezit jen potud, pokud „jde o opatření v demokratické společnosti nezbytná“.“*

V souladu s těmito informacemi lze dovozovat, že omezení práva na informace uvedené v § 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím lze v zákonných mezích vztáhnout i na bezpečnostní opatření podle § 4 odst. 1 zákona o kybernetické bezpečnosti, resp. na takové informace o bezpečnostních opatřeních podle § 4 odst. 1 zákona o kybernetické bezpečnosti, jejichž poskytnutí by mohlo významně nebo přímo ohrozit účinnost bezpečnostního opatření.

Bezpečnostní opatření podle zákona o kybernetické bezpečnosti jsou tematicky uvedena v § 5 zákona o kybernetické bezpečnosti, přičemž jsou rozdělena na organizační a technická opatření. Takto stanovená bezpečnostní opatření jsou blíže specifikována v rámci § 3 až § 30 vyhlášky o kybernetické bezpečnosti (§ 3 až § 16 a § 30 organizační opatření, § 17 až § 29 technická opatření).

2 Poskytování informací v oblasti bezpečnosti systémů nakládajících s utajovanými informacemi

Další možností, jak lze citlivé nebo důležité informace subjektu chránit, je utajení informací podle zákona o ochraně utajovaných informací a nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací a dalších souvisejících předpisů.

Dle § 2 písm. a) zákona o ochraně utajovaných informací se utajovanou informací rozumí **informace** v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, **jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné**, a která je **uvedena v seznamu utajovaných informací**.

Újmou zájmu se rozumí poškození nebo ohrožení zájmu České republiky a tato se podle závažnosti poškození nebo ohrožení zájmu člení na mimořádně vážnou újmu (stupeň utajení „přísně tajné“), vážnou újmu (stupeň utajení „tajné“) a prostou újmu (stupeň utajení „důvěrné“). Jednotlivé kategorie této újmy jsou spolu s nevýhodností pro zájmy České republiky (stupeň utajení „vyhrazené“) blíže specifikovány v ustanovení § 3 zákona o ochraně utajovaných informací.

Seznamy utajovaných informací obsahují jednotlivé přílohy nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. Oblasti kybernetické bezpečnosti se věnuje příloha č. 19 tohoto nařízení a uvádí v této oblasti následující okruhy informací:

1. Informace o kritických zranitelnostech v zabezpečení informačních a komunikačních systémů regulovaných zákonem o kybernetické bezpečnosti.
2. Komplexní technická a bezpečnostní dokumentace a konfigurace informačních a komunikačních systémů regulovaných zákonem o kybernetické bezpečnosti v případě, že z nich lze získat informace o možných způsobech úspěšného narušení jejich bezpečnosti.
3. Dokumenty a informace vztahující se k technickým prostředkům k zajišťování kybernetické bezpečnosti.

Informace, která má být utajena podle zákona o ochraně utajovaných informací, musí vždy splňovat obě výše uvedená kritéria zároveň a není tedy možné například utajit informaci, která není uvedena v příloze nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. Stejně tak by neměla být utajena informace, která je sice typově uvedena v seznamu utajovaných informací, ale nesplňuje materiální stránku věci uvedenou v § 2 písm. a), resp. § 3 zákona o ochraně utajovaných informací.

Před zavedením systému ochrany utajovaných informací je potřeba zvážit a mít na paměti, že nakládání a ochrana utajovaných informací s sebou nese vysoké finanční, personální i technické nároky. Takové informace mohou být zpracovávány pouze informačními systémy certifikovanými na příslušný stupeň utajení a k informacím, které jsou klasifikovány určitým stupněm utajení, mohou přistupovat pouze osoby s bezpečnostní prověrkou minimálně stejného stupně, jako je stupeň utajení požadované informace. To platí jak pro přímé zaměstnance subjektu, tak pro případné externí dodavatele a všechny další dotčené osoby nebo subjekty.

Ochrana utajovaných informací se zajišťuje zavedením široké škály opatření v oblasti personální bezpečnosti, průmyslové bezpečnosti, administrativní bezpečnosti, fyzické bezpečnosti, bezpečnosti informačních nebo komunikačních systémů a kryptografické ochrany. Tato opatření jsou stanovena zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti a jeho prováděcími právními předpisy. Nad dodržováním těchto předpisů pak kromě Úřadu dohlíží i Národní bezpečnostní úřad.

S ochranou utajovaných informací souvisí ustanovení § 7 zákona o svobodném přístupu k informacím. Je-li požadovaná informace označena za utajovanou informaci podle zákona o ochraně utajovaných informací a žadatel k ní nemá oprávněný přístup, subjekt povinný poskytovat informace podle zákona o svobodném přístupu k informacím takovou informaci neposkytne.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
25. 7. 2018	1.0	Odb. RAP	Vytvoření dokumentu
12. 11. 2018	1.1	Odb. regulace	Grafická úprava dokumentu
28. 1. 2019	1.2	Odb. regulace	Změna kontaktních údajů
24. 8. 2020	2.0	Odb. regulace	Revize dokumentu
22. 12. 2022	2.1	Odb. regulace	Změna kontaktních údajů