NÚKIB

DOPORUČENÍ NÚKIB

k ustanovení § 10a zákona o kybernetické bezpečnosti a utajení informací podle zákona o ochraně utajovaných informací

Verze 1.2, platná ke dni 29. 1. 2019

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“), jejíž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti podle § 10a zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“) nebo jež byla utajena podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen „zákon o ochraně utajovaných informací“).

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

Tel.: +420 541 110 560

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.

1 Informace s hodnocením vysoké důvěrnosti

S účinností od 1. srpna 2017 bylo do zákona č. 181/2014 Sb., 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 nově umožňuje 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. Pro účely tohoto dokumentu není předmětnou druhá část tohoto ustanovení, tedy neposkytování informací z důvodu, že jsou vedeny v evidenci incidentů, neboť tuto evidenci vede pouze Národní úřad pro kybernetickou a informační bezpečnosti (dále jen „NÚKIB").

NÚKIB má za to, že pro posouzení a správné užití první části tohoto ustanovení (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 informace poskytnout či nikoliv, 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 také 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 NÚKIB vhodné uvažovat o použití § 10a zákona kybernetické bezpečnosti a takovou informaci neposkytnout. Tímto způsobem je vhodné ohodnotit například technickou či bezpečnostní dokumentaci.

Pokud informace není hodnocena z pohledu důvěrnosti na úroveň vysoká nebo kritická, nabízejí se dvě varianty. První je, že informace takového významu z pohledu zajišťování

kybernetické bezpečnosti nedosahuje, tedy není možné využít ustanovení § 10a zákona o kybernetické bezpečnosti a není možné ji z tohoto důvodu neposkytnout. Druhou je, že informace reálně může ohrozit zajišťování kybernetické bezpečnosti, ale není příslušně hodnocena a tedy lze 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 ve vztahu ke kybernetické bezpečnosti, lze jen stěží předpokládat, zda soudy zaujmou restriktivní výklad při využití § 10a zákona o kybernetické bezpečnosti nebo budou naopak akcentovat bezpečnostní aspekty chráněných bezpečnostních zájmů, a to nejen u hraničních případů.

2 Utajované informace

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 NÚKIB dohlíží i Národní bezpečnostní úřad.

S ochranou utajovaných informací souvisí i 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