Informace k bezpečnostní dokumentaci podnikatele

Podle § 96 odst. 2 písm. b) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon“), je součástí žádosti podnikatele bezpečnostní dokumentace podnikatele.

Bezpečnostní dokumentací podnikatele (dále jen „bezpečnostní dokumentace“) se rozumí písemný dokument, ve kterém podnikatel na konkrétních podmínkách u podnikatele rozpracovává způsob ochrany utajovaných informací (dále jen „UI“) za užití jednotlivých druhů zajištění ochrany UI (§ 5 zákona) s ohledem na formu přístupu podnikatele k UI.

Užití jednotlivých druhů ochrany UI je odvislé od formy přístupu podnikatele k UI a dále od způsobu nakládání s UI v podmínkách podnikatele.

V praxi zákon rozlišuje dvě formy přístupu k UI:

1. § 20 odst. 1 písm. a) zákona (tzv. poskytování, kterým se rozumí seznamování se, poskytování, vznik a uchovávání UI); *„Podnikatel má přístup k UI, která u něho vzniká nebo je mu poskytnuta* (dále jen „poskytování a vznik UI“).

Tato forma přístupu k UI v sobě zahrnuje i formu přístupu podle § 20 odst. 1 písm. b) zákona, tzv. seznamování se s UI.

1. § 20 odst. 1 písm. b) zákona (tzv. seznamování se s UI); „*Podnikatel má přístup k UI, ke které mají přístup zaměstnanci podnikatele nebo osoby jednající jménem podnikatele nebo za podnikatele, a to v souvislosti s výkonem pracovní nebo jiné činnosti pro podnikatele na základě smlouvy, aniž by byla podnikateli poskytnuta nebo u něho vznikala“* (dále jen „seznamování se s UI“). Na základě této formy přístupu podnikatele k UI nemohou u podnikatele žádné UI vznikat a nemohou být u podnikatele žádné UI ukládány.

Obsah bezpečnostní dokumentace je stanoven v § 98 zákona.

***§ 98 zákona***

*Bezpečnostní dokumentace podnikatele stanoví systém ochrany utajovaných informací u podnikatele, musí být u podnikatele uložena, průběžně aktualizována a obsahuje*

*a) specifikaci utajovaných informací, k nimž má podnikatel přístup, včetně výčtu těchto utajovaných informací s uvedením jejich původce nebo poskytovatele, stupně utajení a specifikace zakázky, včetně utajovaných informací cizí moci, ke kterým má podnikatel přístup, popřípadě potvrzení podle § 97 písm. h) zákona,*

*b) analýzu možného ohrožení utajovaných informací, vhodná a účinná ochranná opatření ke snížení rizik,*

*c) způsoby realizace jednotlivých druhů zajištění ochrany utajovaných informací.*

**Ad a)** Toto ustanovení se vztahuje k charakteristice UI, původci a zakázce, na jejichž základě bude *(při podání žádosti)* nebo byla *(v rámci hlášení změn podle § 68 písm. d) zákona)* podnikateli UI poskytnuta, bez ohledu na způsob přístupu, tj. zda se jedná o fyzické poskytování UI za účelem uložení u podnikatele v jeho prostorách, vznik UI v prostorách podnikatele, ať již na základě smlouvy nebo z vlastní činnosti podnikatele, nebo o přístup ve formě seznamování se s UI v prostorách zadavatele, tj. bez faktické manipulace s UI v prostorách podnikatele.

Pokud při podání žádosti podnikatele nejsou známy všechny skutečnosti, vychází podnikatel při naplňování tohoto ustanovení z informací poskytnutých potencionálním zadavatelem a dále z nařízení vlády č. 440/2024 Sb., o katalogu oblastí utajovaných informací.

Uvedené ustanovení současně musí korespondovat se zdůvodněním žádosti podnikatele (§ 2 vyhlášky č. 384/2024 Sb., o průmyslové bezpečnosti).

**Ad b)** Analýza rizik je vlastním hodnocením podmínek u podnikatele ve vztahu k ochraně UI. V tomto bodě se podnikatel zaměřuje na zjištění faktických i potencionálních rizik jak v oblasti lidských zdrojů, tak i v oblasti technických prostředků užitých v podmínkách podnikatele.

Uvedené ustanovení velmi úzce souvisí s realizací jednotlivých druhů zajištění ochrany utajovaných informací, přičemž nejužší je souvislost s realizací opatření fyzické bezpečnosti a bezpečnosti informačních a komunikačních systému nebo kryptografické ochrany. V případě fyzické bezpečnosti zpracovává podnikatel „projekt fyzické bezpečnosti“ (§ 32 a násl. zákona), který je součástí bezpečnostní dokumentace podle § 98 písm. c) zákona.

Pro získání bližších informací k oblasti bezpečnosti informačních a komunikačních systémů a kryptografické bezpečnosti je nezbytné se obrátit na Národní úřad pro kybernetickou a informační bezpečnost (www.nukib.gov.cz) nebo navštívit jeho webové stránky.

**Ad c)** Způsoby realizace jednotlivých druhů zajištění ochrany UI jsou faktickým popisem realizace příslušných druhů zajištění ochrany UI v podmínkách podnikatele. Jak již bylo uvedeno shora, konkrétní druhy ochrany využívané podnikatelem souvisí jednak s formou přístupu podnikatele k UI a dále i se způsobem, jakým bude podnikatel s UI nakládat. V této části bezpečnostní dokumentace proto rozpracovává podmínky ochrany UI stanovené pro jednotlivé druhy zajištění ochrany UI zákonem a jeho prováděními předpisy

1. První formou přístupu je tzv. poskytování a vznik UI (*přístup podle § 20 odst. 1 písm. a) zákona*). V tomto případě podnikatel vždy realizuje nejméně opatření v oblasti personální, administrativní a fyzické bezpečnosti. Oblast fyzické bezpečnosti popisuje v projektu fyzické bezpečnosti (§ 32 a násl. zákona), jeho struktura je stanovena ve vyhlášce č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů. Pokud hodlá UI zpracovávat v informačním systému nebo s nimi nakládat v komunikačním systému, realizuje dále opatření v oblasti bezpečnosti informačních a komunikačních systémů.

Ve vztahu k bezpečnosti informačních a komunikačních systémů a kryptografické ochraně nepopisuje v bezpečnostní dokumentaci systém ochrany realizovaný v podmínkách podnikatele, ale pouze uvede, že bude daný druh zajištění ochrany UI realizovat, neboť oba uvedené druhy jsou předmětem samostatného řízení, které vede Národní úřad pro kybernetickou a informační bezpečnost. Bližší informace k oblasti bezpečnosti informačních a komunikačních systémů a kryptografické bezpečnosti naleznete na stránkách www.nukib.gov.cz.

Popis realizace jednotlivých druhů může podnikatel zapracovat přímo v bezpečnostní dokumentaci nebo ve formě příloh k bezpečnostní dokumentaci. V případě příloh k bezpečnostní dokumentaci uvede v textu dokumentu „Bezpečnostní dokumentace“ přehled realizovaných druhů ochrany UI ve svých podmínkách a odkaz na danou přílohu k bezpečnostní dokumentaci. Tyto přílohy jsou nedílnou součástí bezpečnostní dokumentace, a tudíž i nedílnou součástí žádosti podnikatele.

1. Druhou formou přístupu je tzv. seznamování se s UI (*přístup podle § 20 odst. 1 písm. b) zákona*). V tomto případě podnikatel realizuje pouze opatření v oblasti personální bezpečnosti. Pro vlastní zpracování platí postup popsaný v předchozím odstavci.

*Poznámka:*

*V bezpečnostní dokumentaci podnikatel nepopisuje realizaci průmyslové bezpečnosti, neboť průmyslovou bezpečností se rozumí systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k UI a k zajištění nakládání s UI u podnikatele v souladu se zákonem (srov. § 5 zákona).*

V bezpečnostní dokumentaci podnikatel **uvádí pouze ty druhy zajištění ochrany UI, které bude ve svých podmínkách realizovat**.

Rozsah bezpečnostní dokumentace není stanoven a je odvislý pouze od způsobu rozpracování a zapracování požadavků zákona a prováděcích právních předpisů konkrétních podmínek u podnikatele do uvedeného dokumentu.

Bezpečnostní dokumentace **musí odpovídat požadavkům zákona, prováděcích právních předpisů k zákonu a rovněž musí být v souladu s ostatními právními předpisy**.