8. 8. 2025

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Režimy povinností dle nového zákona o kybernetické bezpečnosti

Nový zákon o kybernetické bezpečnosti (dále jen „NZKB“),[1] který transponuje požadavky směrnice Evropského parlamentu a Rady (EU) 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (dále jen „NIS2“), nově definuje dvě kategorie povinných osob podřízených NZKB, a to zejména podle povahy jejich činnosti či oblasti, ve které působí, a rozlišuje dva základní režimy povinností. V tomto článku se zaměříme na základní přehled těchto režimů a rozdílů mezi nimi.

Dle čl. 15 recitálu směrnice NIS2 mají být subjekty zařazeny do dvou kategorií, a to jako základní subjekty (essential entity s vyšší mírou povinností) a důležité subjekty (important entity s nižší mírou povinností) s přihlédnutím k míře kritické důležitosti, pokud jde o odvětví nebo druh služby, kterou poskytují, a také k jejich velikosti. Český zákonodárce toto rozdělení do NZKB promítnul formou stanovení dvou režimů poskytovatelů regulovaných služeb, a to režimu nižších a vyšších povinností. Na poskytovatele v režimu vyšších povinností jsou, jak již název kategorie napovídá, kladeny vyšší požadavky než na poskytovatele v režimu nižších povinností.[2]

Dle § 8 odst. 1 NZKB je v režimu vyšších povinností poskytovatel regulované služby, který z důvodu své velikosti, počtu uživatelů, geografického rozšíření služby, dopadu na fungování odvětví nebo jiného poskytovatele regulované služby nebo rizikovosti provozu je značně ekonomicky, společensky nebo bezpečnostně významný pro Českou republiku. V režimu nižších povinností je pak poskytovatel regulované služby podřízený NZKB, který není v režimu vyšších povinností. Podmínky rozdělení poskytovatelů regulovaných služeb stanoví vyhláška o regulovaných službách, a to konkrétně její příloha č. 1, ve které je vždy u příslušné regulované služby uvedeno, jaký režim povinností se na konkrétního poskytovatele vztahuje. Např. v případě regulované služby „výkon svěřených pravomocí“ v rámci odvětví „veřejná správa“ je poskytovatelem v režimu vyšších povinností ústřední orgán státní správy, kraj či hlavní město Praha, zatímco poskytovatelem v režimu nižších povinností je obec s rozšířenou působností (tzv. trojková obec), městská část hlavního města Prahy či vysoká škola.[3] Dle důvodové zprávy jsou obce s rozšířenou působností mezi poskytovatele regulované služby zařazeny zejména proto, že jsou jim v přenesené působnosti svěřeny pravomoci, jejichž neplnění by mělo významný dopad na obyvatelstvo. Obce I. či II. stupně (tzv. základní či dvojkové obce) do uvedeného výčtu v rámci regulované služby „výkon svěřených pravomocí“ spadat (dle aktuálního znění návrhu vyhlášky) nebudou. Jako další příklad lze uvést regulovanou službu „poskytování veřejně dostupné služby elektronických komunikací podle zákona o elektronických komunikacích“, v rámci které bude poskytovatelem v režimu vyšších povinností osoba poskytující veřejně dostupnou službu elektronických komunikací podle zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů, pokud je velkým či středním podnikem (případně pokud poskytuje služby skrze určitý počet aktivních SIM karet nebo aktivních pevných internetových přípojek), zatímco v režimu nižších povinností bude tato osoba, pokud je malým nebo mikropodnikem. S ohledem na definici § 2 odst. 3 písm. a) zákona o elektronických komunikacích[4] se nabízí otázka, zda případně nebude poskytovatelem regulované služby v režimu nižších povinností také podnikatel (např. provozovatel kavárny, sportoviště apod.), který pro své návštěvníky poskytuje přístup k internetu (wifi připojení). Pokud jde o podnikatele, který pro své návštěvníky zajišťuje bezplatné wifi připojení a toto není jeho hlavní činností, nebude považován za poskytovatele služby

elektronických komunikací a potažmo poskytovatele regulovaných služeb. Pro úvodní posouzení pro účely samoidentifikace a zjištění pravděpodobného režimu povinností je možné využít tzv. kalkulačky dostupné na portálu Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „***NÚKIB***“).[5]

Dále je potřeba dodat, že v souladu s § 8 odst. 1 NZKB je jeden poskytovatel regulovaných služeb vždy pouze v jednom režimu bez ohledu na to, zda má např. několik služeb spadajících do režimu nižších povinností a jednu spadající do režimu vyšších povinností; spadá-li byť jediná služba do režimu vyšších povinností, uplatní se pro danou osobu tento režim. Shodně také z informací prezentovaných na webu NÚKIB vyplývá, že jedna osoba (jedno IČO) má za každých okolností vždy jen jeden režim poskytovatele regulované služby.[6] Specifické postavení pak mají poskytovatelé služeb ve smyslu § 5 NZKB, kteří jsou vždy v režimu vyšších povinností (srov. § 8 odst. 3 NZKB).

Odlišnosti jednotlivých režimů spočívají zejm. v rozsahu přijímaných bezpečnostních opatření ve smyslu § 14 NZKB, který v odst. 1 stanoví širší rozsah povinností pro poskytovatele regulovaných služeb v režimu vyšších povinností. Dle důvodové zprávy k citovanému ustanovení NZKB reflektují požadavky na poskytovatele v režimu vyšších povinností požadavky mezinárodních norem a standardů a nejlepší praxe na plný a účinný systém řízení bezpečnosti informací. Pro poskytovatele regulované služby v režimu nižších povinností je pak stanovena užší množina povinností, představující základní bezpečnostní opatření (organizačního a technického typu), která by měla být v dnešní době základem běžného provozu ICT. Poskytovatel v režimu nižších povinností má pochopitelně možnost (dobrovolně) přijmout opatření určená pro vyšší režim. NZKB dále počítá s tím, že podrobnosti budou stanoveny v prováděcím předpisu, a to v samostatné vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností a vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, které v zásadě provádějí (specifikují) jednotlivá organizační a technická opatření, jejichž výčet je v § 14 NZKB. Kupříkladu v režimu vyšších povinností má poskytovatel regulované služby povinnost stanovení bezpečnostních rolí v rámci organizačních opatření, což v praxi např. znamená povinnost ustanovit manažera či architekta kybernetické bezpečnosti, zatímco v režimu nižších povinností taková povinnost stanovena není; platí však obecná povinnost určit osobu odpovědnou za kybernetickou bezpečnost.[7] Obecně však platí, že právní úprava v oblasti kybernetické bezpečnosti je postavena na tzv. performativních pravidlech a konkrétní organizační a technické postupy ponechává na samotných poskytovatelích, resp. dle důvodové zprávy k NZKB jsou legislativou požadavky zpřesňovány pouze tam, kde je to s přihlédnutím k praktickým zkušenostem a poznatkům z praxe NÚKIB nezbytné.

S ohledem na výše uvedené lze shrnout, že NZKB v souladu se směrnicí NIS2 zavádí diferencované nastavení povinností podle významu a dopadu činností jednotlivých poskytovatelů regulovaných služeb, a to prostřednictvím režimů vyšších a nižších povinností. Jejich hlavní rozdíl spočívá v rozsahu povinně přijímaných bezpečnostních opatření dle § 14 NZKB, přičemž konkrétní požadavky upravují prováděcí předpisy (vyhlášky). Nová právní úprava je převážně založena na tzv. performativních pravidlech a dává subjektům poměrně výraznou míru flexibility neboli nepochybně neexistuje „jedna správná“ cesta, jak dosáhnout souladu s pravidly NZKB a NIS2. U poskytovatelů v režimu nižších povinností přitom představují požadovaná opatření minimální standard, který by měl být samozřejmou součástí provozu každého ICT prostředí. Nastavení režimu povinností má za cíl nalézt rovnováhu mezi potřebou chránit (nejen) digitální infrastrukturu a požadavkem na přiměřenost regulatorního/administrativního zatížení zejména u menších nebo nově regulovaných subjektů.

Mgr. Milan Šebesta, LL.M. et LL.M.

Partner

Mgr. Milan Friedrich, LL.M.
Advokát

MT Legal s.r.o., advokátní kancelář

Praha | Brno | Ostrava

Tel.: +420 222 866 555
Fax: +420 222 866 546
e-mail: info@mt-legal.com

---

[1] V době přípravy tohoto článku byl návrh nového zákona o kybernetické bezpečnosti podepsán prezidentem republiky a dne 8. 7. 2025 odeslán k publikaci >>> zde.

[2] Kdispozici >>> zde.

[3] Výčet poskytovatelů v režimu vyšších či nižší povinností uvedený v tomto článku není úplný a jedná se pouze o vybrané příklady z přílohy č. 1 vyhlášky o regulovaných službách.

[4] Ustanovení § 2 odst. 3 písm. a) zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů: Pro účely tohoto zákona se dále rozumí

1. službou elektronických komunikací služba obvykle poskytovaná za úplatu prostřednictvím sítí elektronických komunikací, která s výjimkou služeb poskytujících obsah přenášený prostřednictvím sítí a služeb elektronických komunikací nebo vykonávajících redakční dohled nad tímto obsahem zahrnuje tyto druhy služeb:

1. službu přístupu k internetu,

2. interpersonální komunikační službu,

3. služby spočívající zcela nebo převážně v přenosu signálů, například přenosové služby používané pro poskytování služby komunikace mezi stroji a pro rozhlasové a televizní vysílání.

[5] K dispozici >>> zde.

[6] K dispozici >>> zde.

[7] Ustanovení § 4 odst. 3 návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností: „Povinná osoba určí osobu odpovědnou za kybernetickou bezpečnost, která v oblasti kybernetické bezpečnosti odpovídá za řízení a rozvoj kybernetické bezpečnosti, dohled nad stavem kybernetické bezpečnosti a komunikaci s vrcholným vedením, přičemž pověřena může být osoba, která pro tuto činnost

a) bez zbytečného odkladu absolvuje odborné školení podle § 6 písm. g) nebo

b) prokáže odbornou způsobilost v oblasti kybernetické bezpečnosti.“

Další články:

- AML - od zákona č. 253/2008 Sb. k AMLR: co konkrétně musí česká povinná osoba změnit do roku 2027
- Podmíněné propuštění ve světle zásady ústnosti a přímosti
- Byznys a paragrafy, díl 37.: Povinná forma jednání ve smlouvách
- Poučení z krizového vývoje v kauze bitcoiny
- EUDAMED: Jednotná databáze mění pravidla hry na trhu zdravotnických prostředků
- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy