23. 10. 2025

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

Byznys a paragrafy, díl 20.: Nový zákon o kybernetické bezpečnosti

Vítáme vás u dalšího dílu naší série Byznys a paragrafy, kterou pro vás připravuje advokátní kancelář LAWYA. Od 1. listopadu tohoto roku nabývá účinnosti nový zákon č. 264/2025 Sb., o kybernetické bezpečnosti (dále jako „NzoKB“), který nahrazuje starý zákon o kybernetické bezpečnosti z roku 2014 (zákon č. 181/2014 Sb.). Hlavním důvodem pro přijetí nového zákona byla povinnost implementace směrnice NIS2 do českého právního řádu, která zavádí nové povinnosti pro povinné subjekty. Kdo je povinným subjektem? Jaké povinnosti má povinný subjekt? Na tyto otázky Vám přinášíme odpovědi v následujících řádcích.

Povinné subjekty

Původní právní úprava zařazuje povinné subjekty do osmi různých skupin.[1] Jednalo se o poskytovatele, správce nebo provozovatele základních a digitálních služeb, informačních a komunikačních systémů kritické infrastruktury anebo informačních a komunikačních systémů základních služeb. V tomto ohledu je systematika nového zákona jednodušší, jelikož mezi povinné subjekty řadí organizace, které působí v regulovaném odvětví, které poskytují regulovanou službu a které jsou dostatečně významné. Současně však nový zákon dopadne na větší množství organizací než doposud, jelikož se rozšiřuje okruh regulovaných odvětví.

Regulovaná odvětví budou[2] stanovena ve vyhlášce o regulovaných službách. Původní úprava regulovala především odvětví energetiky, dopravy, zdravotnictví, digitální infrastruktury či financí. Vyhláška o regulovaných službách bude nově mimo jiné regulovat i odvětví jako veřejná správa, potravinářský, chemický, obranný a vesmírný průmysl a digitální infrastruktura a věda, výzkum a vzdělání. Každé jednotlivé odvětví má ve vyhlášce o regulovaných službách i regulované služby v rámci těchto odvětví. Ty jsou uvedeny v příloze vyhlášky o regulovaných službách.

Poslední podmínkou je být dostatečně významnou organizací. Významnost je hodnocena především podle velikosti podniku.[3] S výjimkou odvětví digitálních infrastruktur a služeb, kde je organizace významná i pokud je mikropodnikem nebo podnikem malým, je organizace významná pouze pokud je považována za podnik střední nebo velký. Pokud organizace zaměstnává více než 250 zaměstnanců, její roční obrat přesahuje 50 milionů eur a/nebo bilanční suma roční rozvahy přesahuje 43 milionů eur,[4] je dostatečně významná.

Povinným subjektem jsou tedy organizace, které působí v regulovaném odvětví, v tomto odvětví poskytují regulovanou službu a jsou dostatečně významné. Je třeba podotknout, že posouzení naplnění kritérií musí každá organizace provést samostatně.

Povinnosti povinného subjektu

Povinné subjekty se nově musí samy ohlásit do 60 dní od naplnění kritérií povinného subjektu. Na základě toho Národní úřad pro kybernetickou a informační bezpečnost (dále jako „NÚKIB“) zahájí řízení z moci úřední a vydá rozhodnutí o registraci regulované služby. Po doručení tohoto rozhodnutí běží subjektu lhůty na splnění dalších povinností dle zákona. Pokud by subjekt s rozhodnutím nesouhlasil, může proti rozhodnutí podat rozklad. Ten však nemá odkladný účinek.

Další povinnosti jsou děleny podle toho, zda má subjekt určen režim vyšších či nižších povinností. Určení toho, která služba spadá pod který režim, je stanoveno v příloze vyhlášky o regulovaných službách, u každé jednotlivé regulované služby a každého jednotlivého regulovaného odvětví. Pokud je služba registrována jako služba dle § 5 NZoKB, například pokud může mít narušení této služby významný dopad na bezpečnost ČR, vnitřní pořádek nebo zdraví, je automaticky řazena do režimu vyšších povinností. Základním kritériem pro stanovení, zda subjekt spadá pod nižší či vyšší režim, je kromě jiných faktorů i velikost podniku.

Povinnosti subjektu v nižším režimu

Režim nižších povinností obsahuje opatření jako např. řešení kybernetických bezpečnostních incidentů, bezpečnost lidských zdrojů nebo systém zajišťování minimální kybernetické bezpečnosti.[5] Všechny tyto povinnosti platí také u režimu vyššího, je ve větším rozsahu a hloubce – hlavními rozdíly tedy jsou rozsah bezpečnostních opatření, pravidla pro hlášení incidentů i přísnost sankcí za nedodržení povinností. V nižším režimu je v případě bezpečnostního incidentu subjekt povinen incident nahlásit Národnímu CERT. Lhůta pro nahlášení je 72 hodin od zjištění a nejpozději do 30 dní od nahlášení musí být předložena závěrečná zpráva o incidentu.

Povinnosti subjektu ve vyšším režimu

Režim vyšších povinností obsahuje opatření, která jsou obdobná jako ta upravená v minulé právní úpravě. Jsou dělena na organizační a technická opatření a mezi ty základní patří například stanovení bezpečnostních rolí, správa a ověřování identit, fyzická bezpečnost či zvládání kybernetických bezpečnostních událostí a incidentů.[6] V případně bezpečnostního incidentu je subjekt ve vyšším režimu povinen jej nahlásit přímo NÚKIBu. Oproti nižšímu režimu je subjekt ve vyšším režimu povinen při bezpečnostním incidentu předložit prvotní hlášení do 24 hodin od zjištění incidentu.

Specifika pro odvětví digitálních infrastruktur a služeb

Jak již bylo výše zmíněno, významnou službou je v odvětví digitální infrastruktury a služeb i mikropodnik nebo malý podnik. Do tohoto odvětví spadá například[7] služba datového centra, služba cloud computingu, služba registrace doménových jmen.[8] Pokud by subjekt byl povinnou osobou s tím, že poskytuje službu datového centra, jeho konkrétní povinnosti jsou stanoveny v § 18 odst. 1 NzoKB.[9] Jde o minimální výběr povinností z vyššího režimu a musí být naplňovány v míře a způsobem podle prováděcího předpisu Evropské komise k směrnici NIS 2.

Tento subjekt musí tedy minimálně identifikovat, hodnotit a snižovat rizika. Dále musí zpracovat a udržovat bezpečnostní politiku a dokumentaci. Je povinen připravit postupy, jak reagovat na kybernetický bezpečnostní incident a pro tyto případy provádět cvičení. Subjekt musí svá data zálohovat a testovat jejich obnovu. Musí dále řídit dodavatele, tedy mít připraven risk managment. Subjekt by měl řídit i své lidské zdroje, tedy provádět pravidelná školení, bezpečnostní prověrky či řízení přístupů. Subjekt je povinen nahlašovat všechny kybernetické bezpečnostní incidenty s významným dopadem na poskytování dané regulované služby.

Závěr pro běžného podnikatele

Závěrem lze dodat, že nový zákon o kybernetické bezpečnosti se standardně nevztáhne na fyzické osoby, malé podniky a organizace, které neposkytují regulované služby nebo nepůsobí v regulovaných odvětvích. Pro „běžné“ podnikatele či živnostníky tedy nová právní úprava nemá dopad.

Nejste si jisti, zda nový zákon dopadne i na Vaši organizaci? Chcete se ujistit, jaké povinnosti Vám

mohou z nového zákona vyplývat? Neváhejte nás kontaktovat, rádi Vám dopad nového zákona právě na Vaši organizaci objasníme.

Sledujte další díly seriálu Byznys a paragrafy, a pokud chcete mít přehled o aktuálních právních změnách a praktických doporučeních, přihlaste se k odběru našeho měsíčního newsletteru, který vám přináší nejnovější právní novinky a užitečné tipy.

Přihlásit se k odběru newsletteru můžete >>> zde.

Děkujeme, že jste s námi, a těšíme se na pokračování společné cesty světem práva a podnikání!

Mgr. Ivana Šilhánková,
advokátka

Barbora Spáčilová,
právní praktikanta

LAWYA

LAWYA, advokátní kancelář s.r.o.

Sídlo:
Tučapy 240
683 01, Tučapy

Kontaktní adresa:
Králova 298/4
616 00, Brno

tel.: +420 543 216 310
e-mail: info@lawya.cz

---

[1] § 3 zákona o kybernetické bezpečnosti z roku 2014

[2] V době uzávěrky článku není návrh vyhlášky schválen vládou a v systému VeKLEP není ani uveden termín konání schůze vlády, kdy by měl být návrh schvalován. Autorky vychází

z předloženého návrhu vyhlášky dostupného >>> zde.

[3] Ve smyslu Sdělení Ministerstva průmyslu a obchodu č. 7/2023 o vyhlášení českého znění doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.

[4] Přepočet eur na koruny je vždy podle aktuálního vyhlášeného kurzu České Národní banky.

[5] Více viz § 14 odst. 2 NZoKB.

[6] Více viz § 14 odst. 1 NZoKB.

[7] Více viz bod 16 přílohy k návrhu vyhlášky o regulovaných službách.

[8] S přístupem do Centrálního registru doménových jmen pro více než 100 000 doménových jmen druhého řádu v doméně .cz.

[9] „(…) alespoň řízení rizik, řízení bezpečnostní politiky a bezpečnostní dokumentace, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, řízení dodavatelů, bezpečnou akvizici, vývoj a údržbu, aplikační bezpečnost, bezpečnost lidských zdrojů, kryptografické algoritmy, řízení přístupu a správu a ověřování identit (…)“

Další články:

- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí
- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše
- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- Právní povaha sítě elektronických komunikací – režim náhrady škody
- Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory