Deloitte.

Kybernetická bezpečnost
Zákon o kybernetické bezpečnosti

V oblasti regulace kybernetické bezpečnosti v České republice nastal důležitý legislativní vývoj. Transpozicí **směrnice NIS2** byl vyhlášen nový zákon č. 264/2025 Sb., o kybernetické bezpečnosti. Ten **od 1. listopadu 2025** kromě dalšího významně rozšiřuje svoji působnost na mnohé sektory, jako je například automobilový průmysl (výroba), výroba zdravotnických pomůcek, výroba farmaceutických produktů a přípravků, zpracování a distribuce potravin, odpadové hospodářství a další.

Zákon zavádí **dva režimy povinností**, které umožňují přizpůsobit rozsah regulačních nároků podle velikosti a strategické důležitosti organizace.

Nižší režim	platí pro subjekty, které sice patří mezi regulované subjekty, ale dopad jejich případného výpadku je **nižší**.
Vyšší režim	platí pro subjekty, jejichž činnost je považována za **kritickou**, například z pohledu služeb veřejnosti nebo závislosti dalších organizací.

Oba režimy stanoví povinnost zavést **bezpečnostní opatření**, hlásit **kybernetické incidenty** a dodržovat **základní pravidla** kybernetické bezpečnosti, přičemž se liší rozsahem povinností a hloubkou implementace.

NA KOHO ZÁKON DOPADÁ?

Deloitte.

V souladu se směrnicí NIS2 český zákon o kybernetické bezpečnosti definuje regulované služby, včetně následujících:

- **VEŘEJNÁ SPRÁVA**
- **ENERGETIKA**
- **VÝROBNÍ PRŮMYSL**
- **POTRAVINÁŘSTVÍ**
- **CHEMICKÝ PRŮMYSL**
- **VODNÍ HOSPODÁŘSTVÍ**
- **NAKLÁDÁNÍ S ODPADY**
- **DOPRAVA**
- **DIGITÁLNÍ SLUŽBY**
- **FINANČNÍ TRH**
- **ZDRAVOTNICTVÍ**
- **VÝZKUM**
- **POŠTOVNÍ SLUŽBY**
- **VESMÍR**
- **OBRANA**

Mnozí poskytovatelé regulované služby musí **sami posoudit**, zda patří do působnosti zákona na základě kritérií jako sektor podnikání a další:

Strategická důležitost

› Strategicky významnou službou je regulovaná služba, jejíž narušení by mohlo mít **závažný dopad na bezpečnost České republiky** nebo vnitřní pořádek.

Velikost podniku & obrat

› Zákon se týká společností, které mají minimálně **50 zaměstnanců** a obrat ve výši než **10 mil. EUR**. Kritérium velikosti se nevztahuje na poskytovatele **důvěryhodné služby**, poskytovatele **služby DNS** ani na **správce TLD**.

Odpovědný regulátor: Odpovědným regulátorem je **NÚKIB**.

VYBRANÉ POVINNOSTI

Dotčené subjekty jsou povinny:

› **Ohlásit se NÚKIB** nejpozději do **60 dní** ode dne splnění kritérií pro registraci.
› Zavést **bezpečnostní opatření** do 1 roku ode dne doručení rozhodnutí o registraci.
› Provést audit nebo **sebehodnocení** a určit manažera kybernetické bezpečnost.
› Uzavřít smlouvy s třetí osobou (dodavatelem) reflektující požadavky zákona.

JAK MŮŽEME POMOCI?

Deloitte.

Prostřednictvím spolupráce mezi jednotlivými týmy Deloitte vám poskytneme služby, které zabezpečí komplexní soulad se zákonem o kybernetické bezpečnosti a související regulací jako například GDPR, AI Act, a to po právní i technické stránce.

Poskytujeme následující služby:

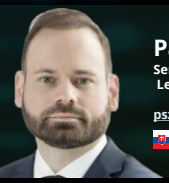
- **Posouzení aplikace zákona na společnost**
- **Právní poradenství u souvisejících regulacích**
- **Analýza nedostatků (GAP analýza)**
- **Analýza rizik a vyhodnocení existujících procesů**
- **Identifikace nápravných opatření**
- **Podpora při implementaci požadavků**
- **Odborná příprava a vzdělávání**
- **Revize a aktualizace vnitřních předpisů**
- **Posouzení a revize dodavatelských řetězců**

Prvním krokem k souladu je **důkladná analýza**, která ukáže oblasti pro zlepšení. K takovým analýzám používáme **naše ověřené nástroje**. Začněte sebehodnocením vyspělosti pomocí našeho **NIS2 Maturity Self-Assessment Tool**.

KONTAKTUJTE NÁS

Jakub Höll
Director, Consulting
CZ & SK Cyber Lead
jholl@deloittece.com

Jaroslava Kračúnová
Director, Legal
jkracunova@deloittece.com



Pavol Szabó
Senior Managing Associate, Legal
pszabo@deloittece.com