



Přehledně:

nový zákon o kybernetické bezpečnosti

Možná jste o něm ještě neslyšeli, ale už brzy se vás může týkat. Nový zákon **č. 264/2025 Sb., o kybernetické bezpečnosti**, přináší soukromým společnostem i úřadům od 1. listopadu 2025 nové povinnosti.

Tento materiál vám pomůže zjistit, zda spadáte do jeho působnosti a co je třeba udělat – **pomůže vám začít!**

Co je to zákon o kybernetické bezpečnosti?

Tento zákon připravil Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) na základě evropské směrnice NIS2. Cílem zákona je, aby vybrané organizace posílily svou odolnost proti kybernetickým hrozbám. Neplatí tedy pro každého občana, ale zaměřuje se především **na určité úřady a soukromé společnosti**.

Koho se zákon týká?

Zákon mluví o tzv. **poskytovatelích regulovaných služeb**.

Organizace se stává poskytovatelem regulované služby, pokud splní kritéria stanovená zejm. **vyhláškou č. 408/2025 Sb., o regulovaných službách**.

- Pokud vaše společnost nebo úřad poskytuje alespoň jednu z regulovaných služeb, zákon se vás týká.
- Pokud ne, mezi regulované poskytovatele nepatříte.

Co zákon požaduje?

Smyslem není nutit každou organizaci nakupovat drahé technologie nebo budovat velké bezpečnostní týmy.

Počítá se spíš s tím, že:

- se budete kybernetické bezpečnosti věnovat **systematicky**,
- zavedete **přiměřená bezpečnostní opatření**, která odpovídají vaší velikosti a činnosti,
- **zvýšíte svou odolnost** proti možným útokům.

Jak začít?

Zjistěte, jestli se vás zákon o kybernetické bezpečnosti týká:

- Projděte si **zákon a vyhlášku o regulovaných službách**.
- Pročtěte si Průvodce novým zákonem na Portálu NÚKIB ([Průvodce novým zákonem o kybernetické bezpečnosti | Portál NÚKIB](#))
- Použijte **online kalkulačku** na Portálu NÚKIB ([Kalkulačka | Portál NÚKIB](#)).
- Podívejte se i na další **podpůrné materiály a videa** dostupná na Portálu NÚKIB ([Podpůrné materiály | Portál NÚKIB](#)).

Pokud spadáte pod zákon:

- Do konce roku 2025 je potřeba se s regulovanými službami **ohlásit u NÚKIB prostřednictvím Portálu NÚKIB**. NÚKIB vás zaregistruje.
- Po registraci si stanovte tzv. **rozsah řízení kybernetické bezpečnosti**.
- Během následujícího roku začněte systematicky **zavádět přiměřená bezpečnostní opatření** a nastavte si proces **hlášení kybernetických bezpečnostních incidentů**.
- Kybernetické bezpečnosti se kontinuálně věnujte i v následujících letech.

Užitečné odkazy

- [Zákon č. 264/2025 Sb. o kybernetické bezpečnosti \(e-Sbírka\)](#)
- [Vyhláška č. 408/2025 Sb. o regulovaných službách \(e-Sbírka\)](#)
- [Vyhláška č. 409/2025 Sb. o bezpečnostních opatřeních pro vyšší režim \(e-Sbírka\)](#)
- [Vyhláška č. 410/2025 Sb. o bezpečnostních opatřeních pro nižší režim \(e-Sbírka\)](#)
- [Průvodce novým zákonem o kybernetické bezpečnosti | Portál NÚKIB](#)
- [Jak ohlásit regulovanou službu | Portál NÚKIB](#)
- [Hlášení údajů k regulovaným službám | Portál NÚKIB](#)
- [Kdo jsou zástupci organizace a jak se pověřují | Portál NÚKIB](#)

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou [Traffic Light Protocol](#). Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva**Podmínky použití****TLP: RED**

Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.

TLP: AMBER+STRICT

Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.

TLP: AMBER

Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.

TLP: GREEN

Informace může být sdílena v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.

TLP: CLEAR

Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	verze	změněno	popis změny
20. října 2025	1.0	OREG	Vytvoření dokumentu