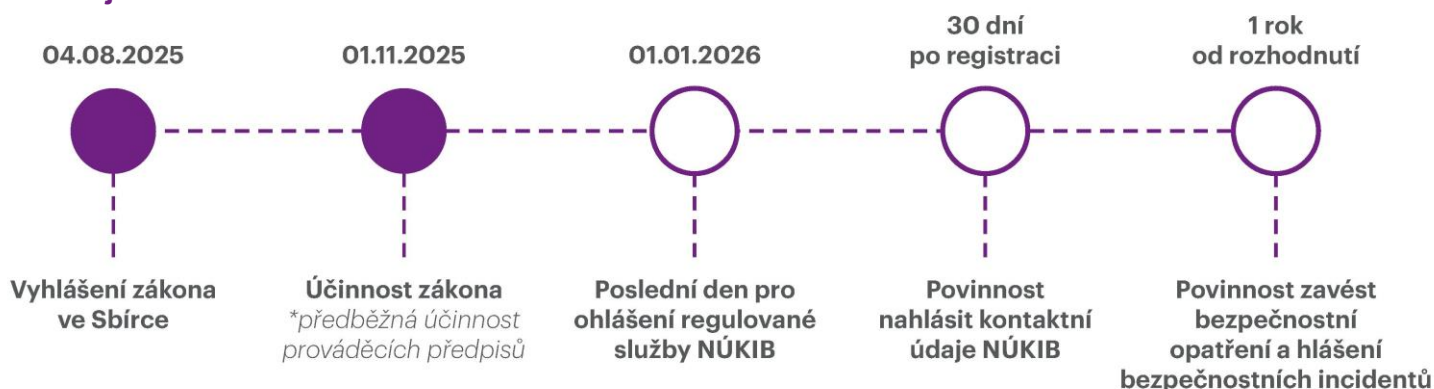


# Nový zákon o kybernetické bezpečnosti: Účinnost nZKB a nové podpůrné materiály

Listopad 2025

Přinášíme vám aktualizované vydání newsletteru, ve kterém Vás budeme informovat o aktualitách, které souvisejí s přípravou na registraci u NÚKIB a implementací NIS2 – a to až do okamžiku konečného termínu pro registraci. V tomto vydání Vám představíme nové podpůrné materiály čerstvě zveřejněné NÚKIB.



## Nový zákon o kybernetické bezpečnosti a většina prováděcích předpisů nabyla účinnosti 1. listopadu

Od tohoto data běží všem subjektům poskytujícím regulované služby lhůta 60 dnů pro ohlášení služeb NÚKIB prostřednictvím [Portálu NÚKIB](#). Určení rozsahu regulovaných služeb je klíčové. Před jejich ohlášením je vhodné provést důslednou analýzu fakticky poskytovaných služeb, tedy ne pouze s ohledem na zápisy ve veřejných rejstřících. K určení rozsahu lze využít [kalkulačku](#) na stránkách NÚKIB.

V případě neohlášení některé ze služeb v této lhůtě čelí subjekty sankcím až 250 milionů Kč nebo až do výše 2 % čistého celosvětového ročního obrátu. Ohlášení širšího rozsahu naopak znamená zvýšené náklady na implementaci potřebných bezpečnostních opatření a související administrativy.

## NÚKIB zveřejnil klíčové podpůrné materiály, které usnadní plnění povinností dle nové regulace

V souvislosti s účinností nového zákona o kybernetické bezpečnosti, zveřejnil Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) 21. října 2025 nové podpůrné materiály. Tyto materiály obsahují praktické návody a přehledné informace, které pomohou při ohlášení regulované služby a plnění povinností, které z nové regulace vyplývají.

### Přehled podpůrných materiálů NÚKIB

| Materiály                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#"><u>Materiál k počítání velikosti podniku</u></a>                         | Vysvětluje, jak postupovat při určování velikostní kategorie subjektu podle nového zákona, přičemž vychází z doporučení Evropské komise 2003/361/ES o definici mikropodniků a malých a středních podniků. Velikost podniku se určuje na základě počtu zaměstnanců, ročního obrátu a bilanční sumy roční rozvahy. Materiál podrobně vysvětluje majetkovou provázanost, na základě, které se mohou společnosti považovat za propojené a jejichž velikost se sčítá. Podobně vysvětluje také provázanost personální. Zdůrazňuje, že zákon zavádí několik výjimek z obecných pravidel. Tak například osoby se zcela oddělenými technickými aktivy se nepovažují za partnerské či propojené podniky. Tato výjimka se typicky může uplatnit při investování do start-upů, kde nedochází k provázání informačních systémů nebo sdílení hardwaru napříč holdingem.                                  |
| <a href="#"><u>Materiál k hlášení kybernetických bezpečnostních incidentů</u></a>    | Ozřejmuje, co je incidentem a událostí, kdo má povinnost incidenty hlásit, jaký je postup a jaké sankce hrozí za opožděné nebo neprovedené ohlášení. Incidenty musí být hlášeny prostřednictvím Portálu NÚKIB (případně e-mailem či datovou schránkou) bez zbytečného odkladu, nejpozději do 24 hodin. Proces zahrnuje prvotní hlášení, následné oznámení do 72 hodin, průběžné zprávy na výzvu a závěrečnou zprávu do 30 dnů. Speciální pravidla se vztahují na vybrané digitální služby dle nařízení Komise (EU) 2024/2690. Samotný vznik incidentu není přestupkem, přestupkem je jeho neohlášení ve stanovené lhůtě.                                                                                                                                                                                                                                                                   |
| <a href="#"><u>Materiál ke stanovení rozsahu řízení kybernetické bezpečnosti</u></a> | Osvětluje klíčové pojmy, zejména rozlišení primárních aktiv (poskytované služby a informace) a podpůrných aktiv (technická, personální a organizační zajištění). Rozsah řízení musí zahrnovat všechna aktiva související s poskytováním regulované služby a tvoří základ pro další povinnosti, jako je zavádění bezpečnostních opatření či hlášení incidentů. Stanovení rozsahu probíhá ve třech krocích – určení primárních aktiv, jejich posouzení z hlediska poskytování regulované služby a určení souvisejících podpůrných aktiv. Rozsah musí být řádně zdokumentován a pravidelně aktualizován. Do doby jeho stanovení platí výchozí rozsah všech aktiv poskytovatele. Nově nabytá nebo změněná aktiva jsou automaticky součástí rozsahu, dokud nedojde k jejich řádnému posouzení a potenciálnímu vyjmutí.                                                                          |
| <a href="#"><u>Materiál k informační povinnosti podle § 19 zákona</u></a>            | Popisuje povinnosti poskytovatele regulované služby vůči uživatelům jeho služby podle § 19 ZKB. Poskytovatel oznámí bez zbytečného odkladu uživatelům kybernetický bezpečnostní incident s významným dopadem, pokud to považuje za vhodné z důvodu zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv. Posouzení, zda je vhodné informovat o incidentu s významným dopadem, vždy závisí na konkrétní situaci, okolnostech a uvážení poskytovatele regulované služby. Zákon nestanovuje přesná kritéria, kdy oznámení je či není vhodné. NÚKIB však může ve správním řízení rozhodnout, že poskytovateli uloží povinnost informovat uživatele o incidentu nebo naopak uloží zákaz informovat, přičemž v rozhodnutí vždy stanoví rozsah informační povinnosti nebo zákazu a při rozhodování zvažuje bezpečnostní otázky, nikoliv obchodní zájmy poskytovatelů. |

## Návody

### Návod k ohlášení regulované služby

Ohlášení regulované služby je první povinností podle § 6, kterou musí organizace splnit do 60 dnů prostřednictvím formuláře na Portálu NÚKIB dostupného od 1. listopadu 2025. Ohlášení provádí statutární orgán nebo pověřený zástupce po přihlášení přes Identitu občana, přičemž formulář vyžaduje určení velikosti podniku a výběr poskytovaných regulovaných služeb s automatickým určením režimu povinností. Po odeslání ohlášení obdrží organizace do datové schránky rozhodnutí o registraci, od jehož doručení začínají běžet lhůty k dalším povinnostem.

### Návod k pověření zástupců organizací

Zástupci organizace jsou fyzické osoby pověřené statutárním orgánem k provádění úkonů podle zákona o kybernetické bezpečnosti. Pokud má organizace českého statutára a pověřuje osobu s českým dokladem, používá se formulář přes Portál NÚKIB s automatickým zpracováním po přihlášení přes Identitu občana, zatímco v případě cizího statutára nebo pověřování cizince se používá formulář přes datovou schránku.

### Návod k hlášení údajů k regulovaným službám

Hlášení kontaktních a doplňujících údajů podle § 11 musí poskytovatel provést do 30 dnů od doručení rozhodnutí o registraci. Formulář vyplňuje statutární orgán nebo pověřený zástupce po přihlášení přes Identitu občana, přičemž je třeba zadat kontaktní osoby a k jednotlivým regulovaným službám přiřadit tyto osoby a doplnit rozsahy veřejných IP adres a používaných doménových jmen. Údaje lze nahlásit rovnou při ohlášení regulované služby.

## Schémata

### Schéma pro samoidentifikaci v odvětví Výzkum a vývoj

Znázorňuje proces samoidentifikace pro regulovanou službu 19.1. Výzkum a vývoj dle nového zákona o kybernetické bezpečnosti. Některé výzkumné organizace mohou spadat i do režimu vyšších povinností, a to za situace, kdy v posledních 5 letech vykonávaly tzv. citlivou výzkumnou činnost (aplikovaný výzkum vojenského materiálu pro budoucí využití pro vojenské účely) nebo aplikovaný výzkum v oblasti pokročilých polovodičů, umělé inteligence, kvantové technologie nebo biotechnologie.

## Další chystané materiály NÚKIB

Zmíněné dokumenty však zdaleka nevyčerpávají seznam materiálů, které mohou povinné subjekty od NÚKIB očekávat. Lze tedy předpokládat také další, jako jsou:

- |                                                                 |                                                 |
|-----------------------------------------------------------------|-------------------------------------------------|
| i. materiál ke stanovení rozsahu ISMS,                          | v. souběh povinností dle prováděcího nařízení   |
| ii. výklad definic v odvětví digitální infrastruktury a služeb, | a národní úpravy,                               |
| iii. výklad přiměřenosti při zavádění bezpečnostních opatření,  | vi. materiál ohledně řízení dodavatelů,         |
| iv. srovnání stávající vyhlášky č. 82/2018 Sb.,                 | vii. propojení zákona o kritické infrastruktuře |
| s režimem vyšších a nižších povinností,                         | a kybernetické bezpečnosti                      |

V případě jakýchkoliv dotazů se neváhejte obrátit na náš pražský TMT tým. Rádi zodpovíme Vaše dotazy a poskytneme Vám potřebnou podporu.

## Klíčové kontakty



**Zdeněk Kučera**

Partner, Praha

D +420 236 082 283

[Email](#)



**Jiří Kvaček**

Seniorní advokát, Praha

D +420 236 082 228

[Email](#)



**Jiří Švejda**

Seniorní advokát, Praha

D +420 236 082 263

[Email](#)

## ABOUT DENTONS

Redefining possibilities. Together, everywhere. For more information visit [dentons.com](https://www.dentons.com)