

ROWAN[®] LEGAL



Kybernetická bezpečnost

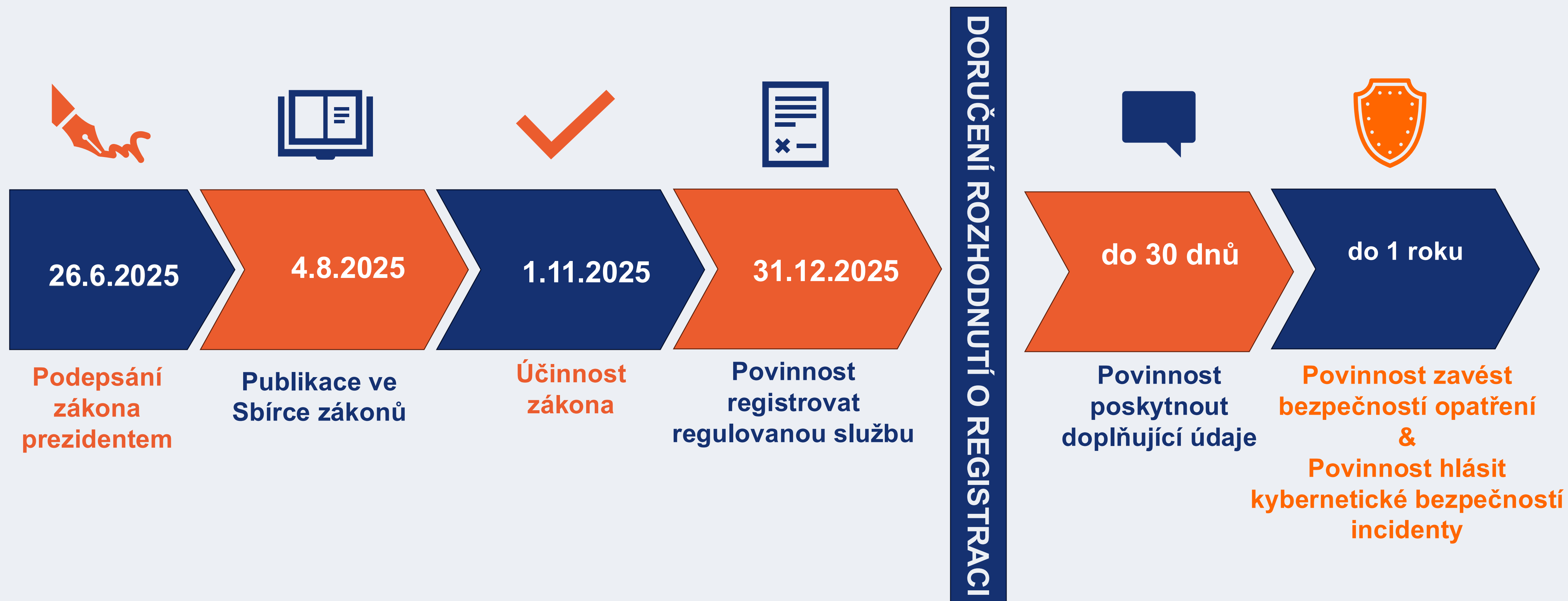
Klíčové kroky, které musíte zvládnout před účinností zákona

Mgr. et Mgr. Ing. Jan Tomíšek, Ph.D.
Mgr. Michaela Holíková

2. 9. 2025

rowan.legal

Harmonogram



Povinné osoby (veřejná správa, kritická infrastruktura)

Poskytuji regulovanou službu?

Regulované služby



Veřejná správa



Energetika
Elektřina



Energetika
Ropa



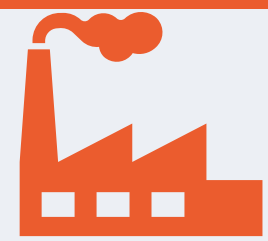
Energetika
Zemní plyn



Energetika
Teplárenství



Energetika
Vodík



Výrobní
průmysl



Potravinářský
průmysl



Chemický
průmysl



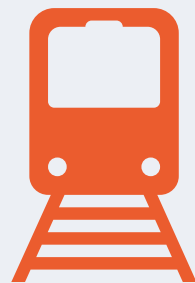
Vodní
hospodářství



Odpadové
hospodářství



Letecká
doprava



Drážní doprava



Námořní vodní
doprava



Silniční doprava



Digitální
infrastruktura a
služby



Finanční trh



Zdravotnictví



Vědy, výzkum a
vzdělávání



Poštovní a
kurýrní služby



Obranný
průmysl



Vesmírný

Kritická infrastruktura

§ 5

Podmínky pro registraci regulované služby jsou dále splněny v případě, že

...

d) jde o službu, jejíž poskytovatel je subjektem kritické infrastruktury podle právního předpisu upravujícího krizové řízení a kritickou infrastrukturu; v takovém případě je regulovanou službou služba odpovídající prvku kritické infrastruktury určenému u tohoto subjektu.

Zákon č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře)

ROWAN[®] LEGAL



Dodavatelé

Poskytuji regulovanou službu?

**Jsem významný dodavatel pro své
zákazníky?**

Regulované služby



Veřejná správa



Energetika
Elektřina



Energetika
Ropa



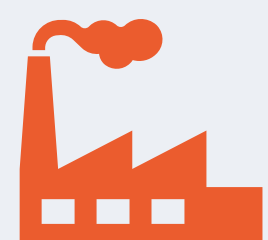
Energetika
Zemní plyn



Energetika
Teplárenství



Energetika
Vodík



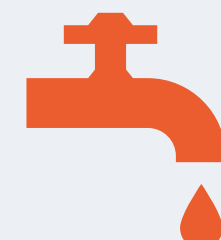
Výrobní
průmysl



Potravinářský
průmysl



Chemický
průmysl



Vodní
hospodářství



Odpadové
hospodářství



Letecká
doprava



Drážní doprava



Námořní vodní
doprava



Silniční doprava



Digitální
infrastruktura a
služby



Finanční trh



Zdravotnictví



Vědy, výzkum a
vzdělávání



Poštovní a
kurýrní služby



Obranný
průmysl



Vesmírný

Regulované služby – odvětví Digitální infrastruktura a služby

16.8 Poskytování služby cloud computingu

16.9 Poskytování služby datového centra

16.12 Poskytování služby vytvářející důvěru podle přímo použitelného předpisu Evropské unie

16.13 Poskytování řízené služby

16.14 Poskytování řízené bezpečnostní služby

One-stop-shop?

Ne tak úplně...

Významný dodavatel

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

§ 2 písm. i) významným dodavatelem se rozumí „ten, kdo povinné osobě poskytuje plnění, které je významné z hlediska zajištění kybernetické bezpečnosti regulované služby“

Povinnosti zákazníků I

(1) Povinná osoba při řízení dodavatelů

- a) stanoví pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací,
- b) prokazatelně seznamuje své dodavatele s pravidly podle písmene a) a vyžaduje plnění těchto pravidel,
- c) řídí rizika spojená s dodavateli,
- d) identifikuje a eviduje své významné dodavatele ve smyslu § 2 písm. i),
- e) prokazatelně písemně informuje své významné dodavatele o jejich evidenci podle písmene d),
- f) zajistí v souvislosti s řízením rizik spojených s významnými dodavateli, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní ustanovení uvedená v příloze č. 6 k této vyhlášce a**
- g) pravidelně přezkoumává plnění smluv s významnými dodavateli z hlediska systému řízení bezpečnosti informací.

Povinnosti zákazníků II

(2) Povinná osoba u významných dodavatelů dále:

- a) provádí **v rámci výběrového řízení a před uzavřením smlouvy, s výjimkou smluv uzavíraných podle zákona o zadávání veřejných zakázek, hodnocení rizik** souvisejících s plněním podle přílohy č. 5 k této vyhlášce,
- b) stanoví **v rámci uzavíraných smluvních vztahů způsoby a úrovně realizace bezpečnostních opatření** a určí obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření,
- c) provádí **pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření** u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany a
- d) zajistí v reakci na rizika a zjištěné nedostatky jejich řešení, která budou přijata bez zbytečného odkladu.

Proaktivně nebo reaktivně?



Společné kroky

První kroky

- **Určení rolí a odpovědností**
- **Stanovení rozsahu**
- **Akční plán implementace bezpečnostních opatření**



Určení rolí a odpovědností

- Cílem je zajistit, aby každý věděl, co má dělat, kdo rozhoduje a kdo nese odpovědnost – a aby to bylo doložitelné a funkční v každodenní praxi.
- Výbor pro řízení kybernetické bezpečnosti
 - Alternativně v začátcích může být např. pracovní skupina
- Manažer kybernetické bezpečnosti
- Architekt kybernetické bezpečnosti
- Auditor kybernetické bezpečnosti
- Garant aktiva
- Nižší režim: pověřená osoba pro kybernetickou bezpečnost



Stanovení rozsahu

- Cílem je určení tzv. **stanoveného rozsahu**, v rámci kterého povinná osoba **zavádí bezpečnostní opatření**.
- Předepsaný postup:
 - a) Identifikace **všech primárních aktiv** organizace
 - b) Určení primárních aktiv, která **souvisí s poskytováním regulované služby**
 - c) Přiřazení **souvisejících podpůrných aktiv** k aktivům určeným podle písmene b)
- **POZOR:** Dokud nejsou určena primární aktiva a přiřazena související podpůrná aktiva, jsou **veškerá aktiva součástí stanoveného rozsahu**.

Akční plán implementace bezpečnostních opatření

- **Analýza stavu** plnění bezpečnostních opatření
- **Prioritizace** nápravných opatření a dalších kroků
- **Časový harmonogram** – roční lhůta
- Integrace do **rozpočtu** a projektového řízení
- Řízení **dodavatelů** – kontrola SLA, smluvní úpravy, sdílená odpovědnost
- **Školení** a komunikace
- **Měření a pravidelný reporting**
- Kontinuální zlepšování



Děkujeme za Vaši pozornost

Mgr. et Mgr. Ing. Jan Tomíšek, Ph.D.

Mgr. Michaela Holíková