



Národní úřad
pro kybernetickou
a informační bezpečnost

Zavádění kybernetické bezpečnosti v prostředí obce

Časté otázky z praxe a odpovědi NÚKIB

Daniela Procházková



O čem to dnes bude?

- 01** Úvod k novému zákonu o kybernetické bezpečnosti
- 02** Základní povinnosti
- 03** Termíny a lhůty pro jejich plnění
- 04** Praktické otázky ORP a odpovědi



Zákon č. 264/2025 Sb., o kybernetické bezpečnosti

Účinnost od **1. listopadu 2025**

9 prováděcích právních předpisů
stovky jednání

3 roky, 8 měsíců a 9 dní
(od přípravy po účinnost)



Nejvýznamnější rozdíly v regulaci pro povinné osoby

Regulované systémy dle 181/2014 Sb.

Orientace na systém

Správce VIS/KII/PZS

Dopadová kritéria a povinné
systémy

Existence provozovatele systému

Jedna sada bezpečnostních
opatření pro všechny organizace

Poskytovatel regulované služby dle nZKB

Orientace na službu

Poskytovatel regulované služby

Primární kritérium velikosti
podniku

Významný dodavatel a MSP
MSSP

Dvě sady bezpečnostních
opatření pro různé organizace

Základní povinnosti dle nZKB



Ohlášení

Ohlášení regulované služby a nahlášení kontaktní osoby

Portál NÚKIB

Do 60 dní od naplnění podmínek pro registraci

Bezpečnostní opatření

Vyhláška o bezpečnostních opatřeních – nižší/vyšší režim

11/28 opatření nižší/vyšší režim

1 rok od doručení rozhodnutí o registraci

Hlášení incidentů

Vychází ze zákona a vyhlášky o bezpečnostních opatřeních

Významné incidenty – nižší a větší okruh vyšší

1 rok od doručení rozhodnutí o registraci

Provedení protiopatření

Vydá a doručí NÚKIB

Reaktivní protiopatření/varování

Lhůty dané protiopatřením

Základní povinnosti dle nZKB



Ohlášení

Ohlášení regulované služby a nahlášení kontaktní osoby

Portál NÚKIB

Do 60 dní od naplnění podmínek pro registraci

Bezpečnostní opatření

Vyhláška o bezpečnostních opatřeních – nižší/vyšší režim

11/28 opatření nižší/vyšší režim

1 rok od doručení rozhodnutí o registraci

Hlášení incidentů

Vychází ze zákona a vyhlášky o bezpečnostních opatřeních

Významné incidenty – nižší a větší okruh vyšší

1 rok od doručení rozhodnutí o registraci

Provedení protiopatření

Vydá a doručí NÚKIB

Reaktivní protiopatření/varování

Lhůty dané protiopatření

Základní povinnosti dle nZKB



Ohlášení

Ohlášení regulované služby a nahlášení kontaktní osoby

Portál NÚKIB

Do 60 dní od naplnění podmínek pro registraci

Bezpečnostní opatření

Vyhláška o bezpečnostních opatřeních – nižší/vyšší režim

11/28 opatření nižší/vyšší režim

1 rok od doručení rozhodnutí o registraci

Hlášení incidentů

Vychází ze zákona a vyhlášky o bezpečnostních opatřeních

Významné incidenty – nižší a větší okruh vyšší

1 rok od doručení rozhodnutí o registraci

Provedení protiopatření

Vydá a doručí NÚKIB

Reaktivní protiopatření/varování

Lhůty dané protiopatření



Bezpečnostní opatření – rozdíly vyšší a nižší režim

➤ Redukovaná bezpečnostní opatření pro nižší režim

organizační opatření – **vyšší** režim

1. systém řízení bezpečnosti informací,
2. povinnosti pro vrcholové vedení,
3. bezpečnostní role,
4. řízení bezpečnostní politiky a bezpečnostní dokumentace,
5. řízení aktiv,
6. řízení rizik,
7. řízení dodavatelů,
8. bezpečnost lidských zdrojů,
9. řízení změn,
10. akvizice, vývoj a údržba,
11. řízení přístupu,
12. zvládání kybernetických bezpečnostních událostí a incidentů,
13. řízení kontinuity činností a
14. audit kybernetické bezpečnosti

technická opatření – **vyšší** režim

1. fyzická bezpečnost,
2. bezpečnost komunikačních sítí,
3. správa a ověřování identit,
4. řízení přístupových oprávnění,
5. detekce kybernetických bezpečnostních událostí,
6. zaznamenávání událostí,
7. vyhodnocování kybernetických bezpečnostních událostí,
8. aplikační bezpečnost,
9. kryptografické algoritmy,
10. zajišťování dostupnosti regulované služby,
11. zabezpečení průmyslových, řídicích a obdobných specifických aktiv

bezpečnostní opatření – **nižší** režim

1. zajišťování kybernetické bezpečnosti,
2. povinnosti vrcholového vedení,
3. bezpečnost lidských zdrojů,
4. řízení kontinuity činností,
5. řízení přístupu,
6. řízení identit a jejich oprávnění,
7. detekce a zaznamenávání kybernetických bezpečnostních událostí,
8. řešení kybernetických bezpečnostních incidentů,
9. bezpečnost komunikačních sítí,
10. aplikační bezpečnost,
11. kryptografické algoritmy



Bezpečnostní opatření prakticky

Nižší režim:

- Nemusí dělat analýzu rizik
- Ve vyhlášce jsou stanovená nepominutelná opatření – ty musí zavést **vždy**
- U ostatních opatření vyhodnotí, zda je potřebuje a zda se vyplatí
- Pokud **ne**
 - dokumentovaný záznam se zdůvodněním, proč je nerelevantní
- Vede přehled bezpečnostních opatření – základní dokument, kde je uvedeno co je zavedeno a co ne a proč

Bezpečnostní opatření



Stanovení rozsahu řízení kybernetické bezpečnosti

Povinná základní bezpečnostní opatření

§ 3, § 4, § 5, § 6 a § 10 vyhlášky

- organizační a administrativní charakter
- východisko pro další opatření z vyhlášky

příklady opatření: dokumentace, lidské zdroje, odpovědná osoba a vrcholné vedení, smlouvy s dodavateli, kontinuita činností, incidenty



Přiměřeně zaváděná bezpečnostní opatření

§ 7, § 8, § 9, § 11, § 12 a § 13 vyhlášky

- převážně technický charakter
- přiměřenost, postupné zavádění
- kontinuální zlepšování

příklady opatření: vícefaktorová autentizace, přístupová práva, fyzická bezpečnost, aktualizace, skenování zranitelností, segmentace sítě, firewall, VPN, kryptografie



Základní povinnosti dle nZKB



Ohlášení

Ohlášení regulované služby a nahlášení kontaktní osoby

Portál NÚKIB

Do 60 dní od naplnění podmínek pro registraci

Bezpečnostní opatření

Vyhláška o bezpečnostních opatřeních – nižší/vyšší režim

11/28 opatření nižší/vyšší režim

1 rok od doručení rozhodnutí o registraci

Hlášení incidentů

Vychází ze zákona a vyhlášky o bezpečnostních opatřeních

Významné incidenty – nižší a větší okruh vyšší

1 rok od doručení rozhodnutí o registraci

Provedení protiopatření

Vydá a doručí NÚKIB

Reaktivní protiopatření/varování

Lhůty dané protiopatření



Hlášení kybernetických incidentů

CO SE HLÁSÍ?

Kybernetické bezpečnostní incidenty (ne události), které:

- mají **původ v kybernetickém prostoru**,
- mají **významný dopad** na poskytování regulované služby a
- u nichž do 24 hodin od jejich detekce **nelze vyloučit úmyslné zavinění**.

KOMU SE HLÁSÍ?

- Národnímu CERT – CSIRT.CZ – provozuje **CZ.NIC**
- Prostřednictvím **Portálu NÚKIB**

STANOVENÍ VÝZNAMNOSTI DOPADU KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU

§ 14

(1) Povinná osoba pro potřeby vyhodnocení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby stanoví

- a) únosnou míru újmy způsobené kybernetickým bezpečnostním incidentem, v jehož důsledku ještě není ohrožen život nebo zdraví osob nebo schopnost povinné osoby dostát svým závazkům,
- b) oblasti pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů zohledňující zejména
 1. provozní dopad kybernetického bezpečnostního incidentu na povinnou osobu a její schopnost poskytovat regulovanou službu,
 2. množství uživatelů regulované služby a jiných orgánů a osob zasazených kybernetickým bezpečnostním incidentem,
 3. časové, lidské a technické zdroje, které jsou potřebné k obnově poskytování zasazené regulované služby,
 4. typ a umístění aktiv dotčených kybernetickým bezpečnostním incidentem,
 5. citlivost informací a dat zasazených kybernetickým bezpečnostním incidentem a újmu, jakou může narušení bezpečnosti těchto informací a dat způsobit povinné osobě nebo jinému orgánu nebo osobě, a
 6. přímou příčinu kybernetického bezpečnostního incidentu, je-li povinné osobě známo, zda se jedná o lidskou chybu, technickou závadu nebo úmyslné jednání.

(2) Dopad kybernetického bezpečnostního incidentu na poskytování regulované služby je považován za významný, pokud

- a) přesáhne povinnou osobou stanovenou únosnou míru újmy způsobenou kybernetickým bezpečnostním incidentem podle odstavce 1 písm. a) a současně
- b) je oblast pro posouzení významnosti dopadu podle odstavce 1 písm. b) posouzena jako významná.



STANOVENÍ VÝZNAMNOSTI DOPADU KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU

§ 14

(1) Povinná osoba pro potřeby vyhodnocení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby stanoví

a) únosnou míru újmy způsobené kybernetickým bezpečnostním incidentem, v jehož důsledku ještě není ohrožen život nebo zdraví osob nebo schopnost povinné osoby dostát svým závazkům,

b) oblasti pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů zohledňující zejména

1. provozní dopad kybernetického bezpečnostního incidentu na povinnou osobu a její schopnost poskytovat regulovanou službu,

2. množství uživatelů regulované služby a jiných orgánů a osob zasažených kybernetickým bezpečnostním incidentem,

3. časové, lidské a technické zdroje, které jsou potřebné k obnově poskytování zasažené regulované služby,

4. typ a umístění aktiv dotčených kybernetickým bezpečnostním incidentem,

5. citlivost informací a dat zasažených kybernetickým bezpečnostním incidentem a újmu, jakou může narušení bezpečnosti těchto informací a dat způsobit povinné osobě nebo jinému orgánu nebo osobě, a

6. přímou příčinu kybernetického bezpečnostního incidentu, je-li povinné osobě známo, zda se jedná o lidskou chybu, technickou závadu nebo úmyslné jednání.

(2) Dopad kybernetického bezpečnostního incidentu na poskytování regulované služby je považován za významný, pokud

a) přesáhne povinnou osobou stanovenou únosnou míru újmy způsobenou kybernetickým bezpečnostním incidentem podle odstavce 1 písm. a) a současně

b) je oblast pro posouzení významnosti dopadu podle odstavce 1 písm. b) posouzena jako významná.

Základní povinnosti dle nZKB



Ohlášení

Ohlášení regulované služby a nahlášení kontaktní osoby

Portál NÚKIB

Do 60 dní od naplnění podmínek pro registraci

Bezpečnostní opatření

Vyhláška o bezpečnostních opatřeních – nižší/vyšší režim

11/28 opatření nižší/vyšší režim

1 rok od doručení rozhodnutí o registraci

Hlášení incidentů

Vychází ze zákona a vyhlášky o bezpečnostních opatřeních

Významné incidenty – nižší a větší okruh vyšší

1 rok od doručení rozhodnutí o registraci

Provedení protiopatření

Vydá a doručí NÚKIB

Reaktivní protiopatření/varování

Lhůty dané protiopatřením



Co ale dělat v praxi?

Přehled v organizaci

- Mé agendy/služby, co poskytují
- Co pro to potřebuji?
- Z toho vyplývá rozsah, ve kterém KB řeším.

Aktuální stav KB

- Mám již zavedena některá opatření?
- Zdokumentuji aktuální stav zavedených a nezavedených opatření.

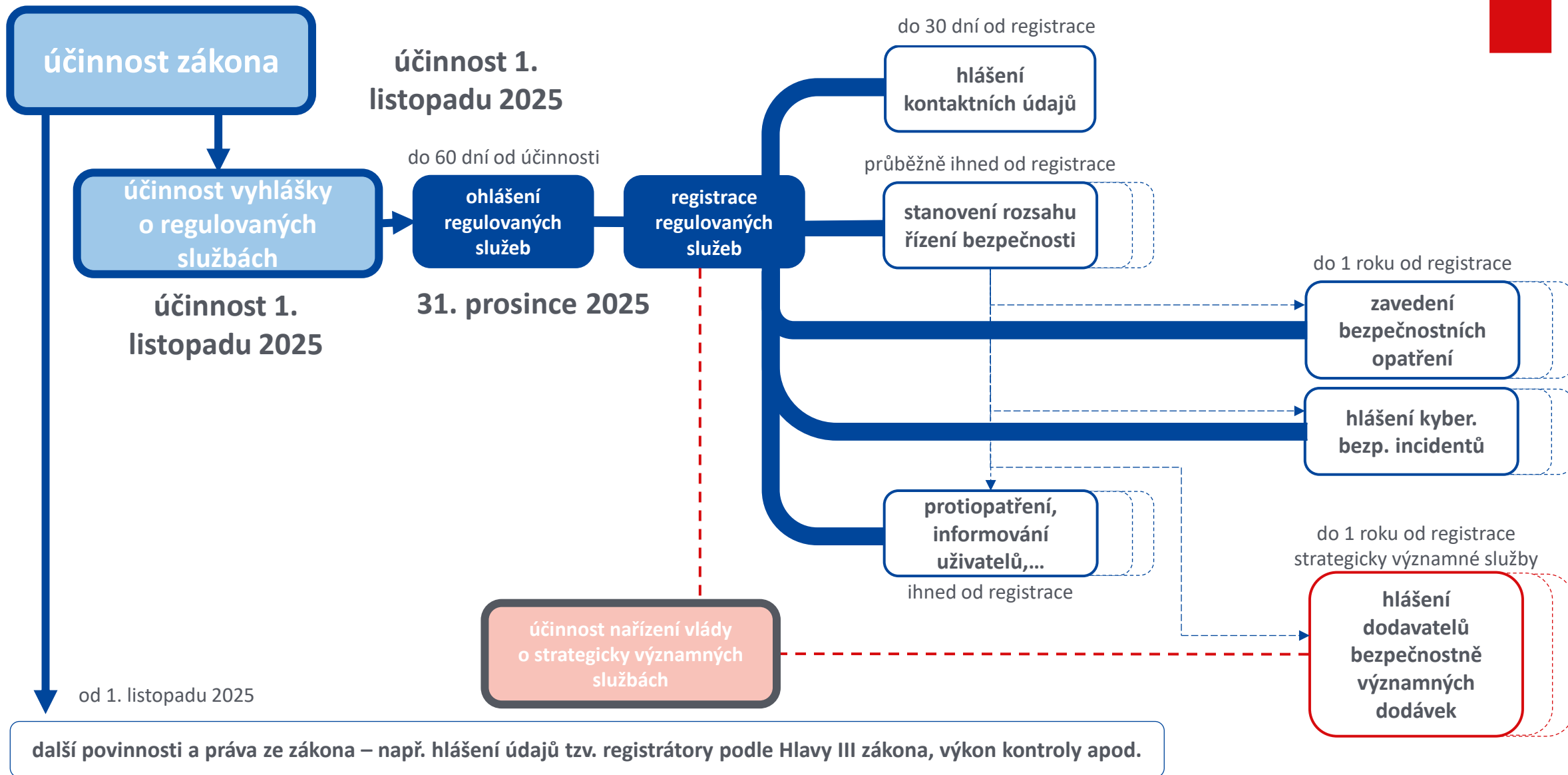
Určení priorit

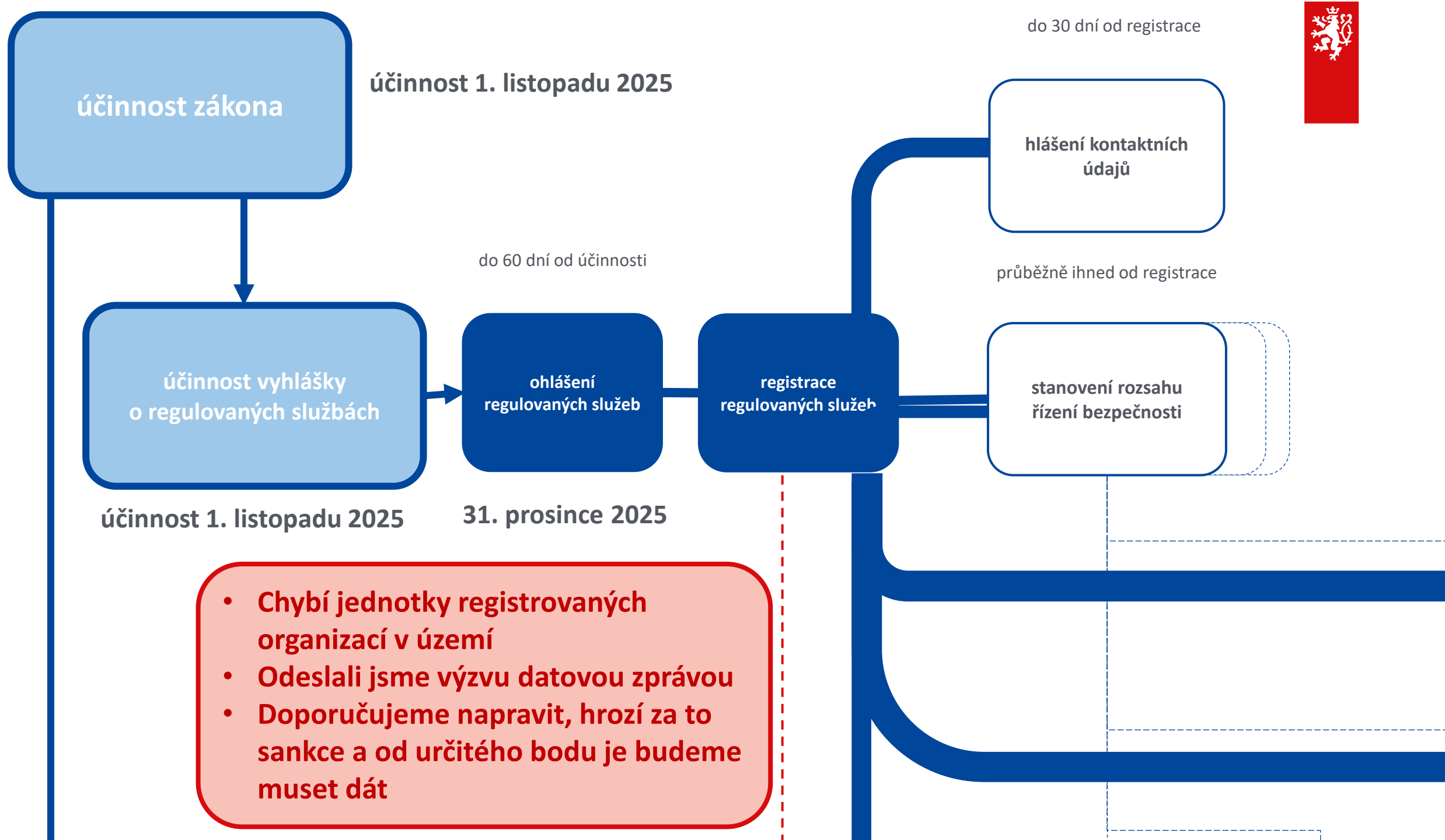
- Jaké mám kapacity?
- Co je má prioritní služba?
- Provedu analýzy, stanovím plán se zohledněním kapacit a priorit.

Zavádění opatření

- Určím odpovědné osoby.
- Priorita je vzdělávání zaměstnanců včetně vedení.
- Pokračuji dle plánu.

**A pokud si nejste jistí →
využijte podporu a informace
NÚKIB.**

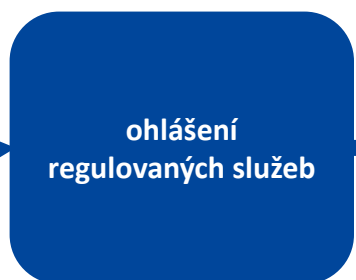




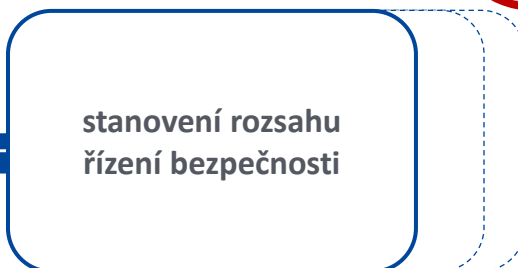


1. listopadu 2025

do 60 dní od účinnosti



31. prosince 2025

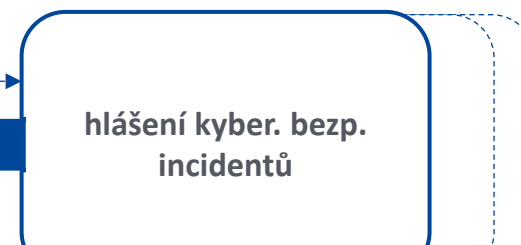
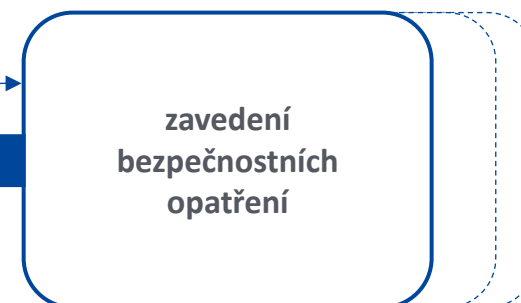


do 30 dní od registrace

průběžně ihned od registrace

- Místy chybí kontaktní údaje
- Pozor na rozdíl mezi zástupcem a kontaktní osobou
- Doporučujeme se snažit myslet na aktualizaci
- Změny jmen apod. čerpáme z registrů

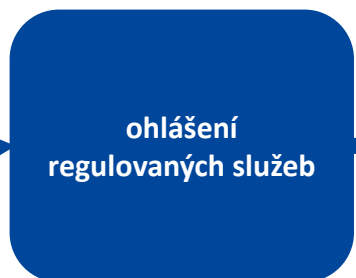
do 1 roku od registrace





1. listopadu 2025

do 60 dní od účinnosti



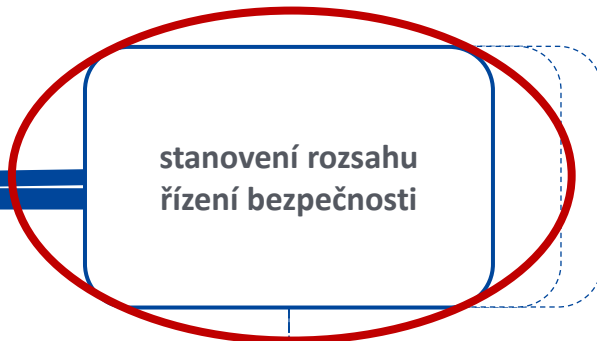
31. prosince 2025



do 30 dní od registrace

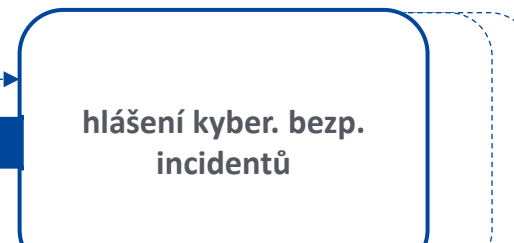
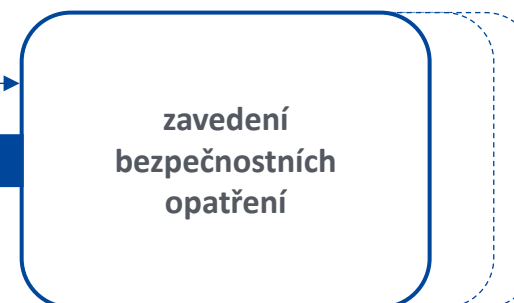


průběžně ihned od registrace



- Pokud a dokud není stanoven je rozsahem celá organizace
- Ze zkušenosti přenesená celá, u samostatné lze vyřazovat
- Udělat to prakticky a funkčně pro Vás – už jsme viděli, že je to možné

do 1 roku od registrace

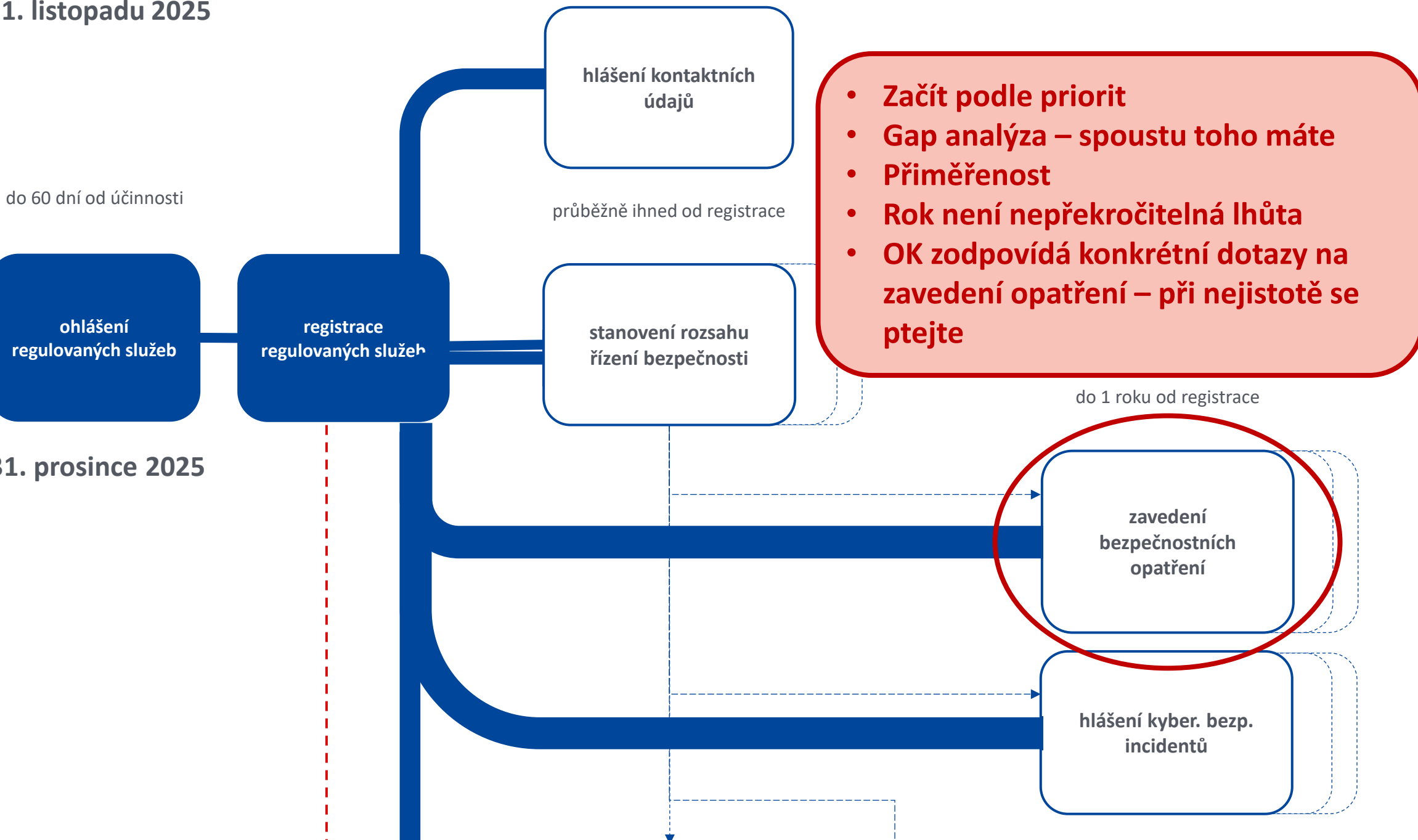




1. listopadu 2025

do 60 dní od účinnosti

1. prosince 2025





hlášení kontaktních
údajů

průběžně ihned od registrace

stanovení rozsahu
řízení bezpečnosti

do 1 roku od registrace

zavedení
bezpečnostních
opatření

hlášení kyber. bezp.
incidentů

protiopatření,
informování

do 1 roku od registrace strategicky
významné služby

- Ještě je hlásit nemusíte – rok na to získat tu schopnost
- Můžete dostat metodickou pomoc dle kapacit CERT (může být výhoda)
- Získat schopnost hlásit do 1 roku je nutné



01 Otázky z území a odpovědi NÚKIB



Jak celou kybernetickou bezpečnost uřídit?

Častá obava:

Máme jeden rok na zavedení všech těch opatření, ale teď nemáme nic z toho v rozpočtech a pak dostaneme akorát pokutu od NÚKIB, že jsme to neudělali. A navíc těch papírů...

Co na to NÚKIB:

1. Spoustu toho máte jen možná nevíte, že to je to ono. Legislativa má někdy jiný slovník než IT lidé.
2. Všechna **opatření nejsou striktně povinná** nebo povinná v plném rozsahu (platí pro vyšší i nižší režim).
 1. Princip **přiměřenosti**.
3. Rok není nepřekročitelná lhůta, po které by následovala okamžitě pokuta. Je důležité začít.
4. Některá opatření nepotřebují peníze v rozpočtu – vzdělávání apod.
5. Dokumentace by měla vznikat v **užitečném** rozsahu pro potřeby organizace.

Komplexní návod – režim nižších povinností – vzor přehledu BO



Vyhodnocení účinnosti zajišťování kybernetické bezpečnosti ke dni 31.3.2026						
Bezpečnostní opatření podle vyhlášky				Stav bezpečnostního opatření	Popis bezpečnostního opatření	
§	Název paragrafu	Úroveň členění		Text znění požadavku		
§ 3	Systém zajišťování minimální kybernetické bezpečnosti	1		Povinná osoba při zajišťování kybernetické bezpečnosti		
§ 3	Systém zajišťování minimální kybernetické bezpečnosti	1	a	zavede a provádí bezpečnostní opatření, která jsou přiměřená bezpečnostním potřebám, a	V procesu	Jsou zaváděna přiměřená bezpečnostní opatření dle potřeby organizace, fáze zavádění jednotlivých bezpečnostních opatření jsou popsány níže v tomto dokumentu.
§ 3	Systém zajišťování minimální kybernetické bezpečnosti	1	b	zavede a provádí alespoň bezpečnostní opatření podle odstavce 2 až 6, 8, 9 a 10	V procesu	Veškerá neopominutelná bezpečnostní opatření jsou přiměřeně zavedena nebo jsou v procesu zavádění. Aktuální stav bezpečnostních opatření je popsán níže v tomto dokumentu.

Prezentace byla naposledy uložena: Právě teď



Jak nastavit dokumentaci – návod nižší režim



Řízení bezpečnostní politiky a dokumentace

TLP:CLEAR

31. března 2026, verze 1.0

5 Obsah bezpečnostní dokumentace

5.1 Přehled bezpečnostních opatření

K čemu slouží:

Slouží jako přehled stavu zavedení všech bezpečnostních opatření uvedených ve vyhlášce č. 410/2025 Sb.

Co by měl pokrývat:

- Přehled všech bezpečnostních opatření, která byla zavedena, včetně popisu jejich zavedení.
- Přehled všech bezpečnostních opatření, která budou zavedena.
 - Termíny pro jejich zavedení.
 - Priority jejich zavedení.
 - Určení osoby odpovědné za jejich zavedení.
- Přehled všech bezpečnostních opatření, která nebyla zavedena, včetně odůvodnění jejich nezavedení.



eLearningy zdarma = jedno BO vyřešené



Kurz pro manažery kybernetické bezpečnosti 26



Kurz pro osoby pověřené kybernetickou bezpečností 26



Kurz pro vrcholné vedení
vyšší i nižší režim požadavků



Základy kybernetické bezpečnosti 26

Domluva pro hromadnou registraci:
osveta@nukib.gov.cz





Jak celou kybernetickou bezpečnost uřídit?

Častá otázka:

Zřizuju základní/střední školu, taky máme příspěvkovou organizaci, která zajišťuje pitnou vodu a obecní policii. Konzultovali jsme to a prý se to nějak ještě sčítá všechno, tak nevím. Co s tím?

Co na to NÚKIB:

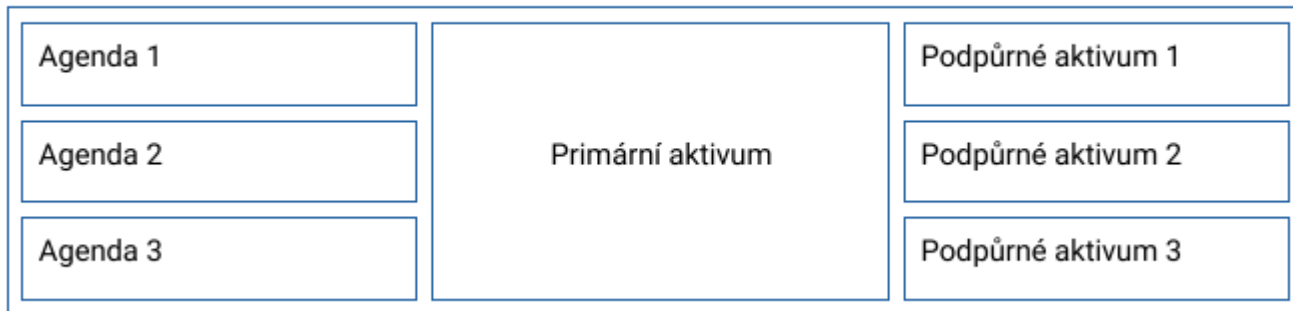
1. **Zřizované organizace** nespadají do regulace jen proto, že je zřizuje někdo regulovaný (ORP), **musí kritéria naplnit samy o sobě**.
 1. Školky, základní školy, obecní knihovny a další spíše nenaplní kritéria a ani se nenajdou v žádné službě.
 2. Vodárna už by se najít mohla – ale musí být alespoň střední podnik – její „IČO“ musí naplnit samo kritéria.
 3. Obecní policie je ze zákona jen odborem v rámci obce – ta je součástí obce a obec ji řešit musí.
2. Podniky se v rámci soukromého sektoru sčítají – ať už jde o partnerské nebo matku/dceru – u veřejného sektoru toto neplatí – **obec není podnik** = nemůže sám naplnit kritéria, která počítají s velikostí podniku ani se nepřipočítává k zřizovaným organizacím.



Co specifika obcí? Samostatná + přenesená působnost

Kybernetická bezpečnost obcí:

Obecný příklad:



Otázky ke kybernetické bezpečnosti obcí:

Podniky zřizované obcemi s rozšířenou působností

Vztahuje se regulace i na podniky zřízené obcí s rozšířenou působností?



Vztahuje se regulace i na příspěvkové organizace zřizované obcemi?





„Stošestkují“ mi věci, co nechci, co můžu dělat?

Příběh/otázka z praxe:

Na městský úřad přichází žádost podle zákona o svobodném přístupu k informacím. Žadatel chce IP adresy serveru, na který se odesílají snímky z rychloměru na silnici. Bezpečnostní a IT pracovníci informaci nechtějí poskytnout. Právní oddělení se obává, že není, jak tomu zabránit.

Řešení:

§ 36 zákona o kybernetické bezpečnosti nebo

= všechny informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, se neposkytují

§ 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím

= omezení poskytnutí informací, pokud by jejich zpřístupnění významně či přímo ohrozilo účinnost bezpečnostního opatření stanoveného podle **zvláštního předpisu**

Odůvodnění neposkytnutí

Test proporcionality:

Vhodnost:

Skutečně by zveřejnění ohrozilo kybernetickou bezpečnost?

Nezbytnost:

Nelze použít mírnější opatření (např. částečné poskytnutí)?

Přiměřenost:

Nepřevažuje veřejný zájem nad ochranou bezpečnosti?

Příklad:

Na městský úřad přichází žádost podle zákona o svobodném přístupu k informacím. Žadatel chce IP adresy serveru, na který se odesílají snímky z rychloměru na silnici.



SCAN ME



**Doporučení k (ne)poskytování informací
v oblasti kybernetické bezpečnosti
a bezpečnosti systémů nakládajících
s utajovanými informacemi**



V organizaci je obava, jestli to „neshodí“ soud.

- Rozsudek Nejvyššího správního soudu o aplikaci výjimky ze zákona o svobodném přístupu k informacím: 1 As 208/2025 – 38
 - Stěžovatel v řízení namítal i srovnání s veřejností IP adresy webu statutárního města.

Klíčový závěr:

- *[...] Míra hrozícího rizika pro řádné fungování rychloměru při poskytnutí požadované IP adresy není srovnatelná s běžnými riziky, která povinná osoba denně podstupuje proto, že jsou veřejné známé adresa jejího sídla nebo IP adresy jejích webových stránek. Naopak se Nejvyšší správní soud ztotožňuje s krajským soudem, že sdělení IP adresy prvního serveru, na který jsou přenášeny záznamy z měření rychlosti, by mohlo vést k přímému ohrožení účinnosti bezpečnostního opatření – rychloměru. **V případě omezení tohoto spojení (např. z důvodu DDoS útoku) by rychloměr přestal plnit svou funkci, jelikož by nemohl přenášet záznamy o překročení rychlosti a předávat je k dalšímu postupu.***



Soutěžení jde jen na cenu

Problém z praxe:

IT zaměstnanec nebo bezpečnostní pracovník chce soutěžit tak, aby nemusel na cenu, ale mohl si dodavatele vybrat i podle kvality nebo v souladu s varováním NÚKIB vůči některým technologiím. Právní tým je proti, je to riskantní – Shodí to ÚOHS.

Odpověď NÚKIB:

- I ÚOHS dlouhodobě umožňuje soutěžit jinak než na cenu – chápeme ale, že je to náročné.
- Existuje k tomu i rozhodovací praxe – tedy možné to je.

Metodika zadávání VZ v oblasti ICT a KB

Metodika by měla zadavatelům pomoci:

- převést analýzu rizik do konkrétních zadávacích podmínek
- promítnout varování a protiopatření NÚKIB do veřejných zakázek
- nastavit bezpečnostní požadavky přiměřeně a obhajitelně
- sladit požadavky kybernetické bezpečnosti se zásadami hospodářské soutěže
- pracovat s dodavatelským řetězcem





Koncepce stavebních úřadů nás posune do vyššího režimu

Otázka z praxe:

Od roku 2027 bude platit nová organizační struktura stavebního řízení. Vzniká Úřad rozvoje území a jeho územní pracoviště, od roku 2028 by měla fungovat územní pracoviště, pro která MMR vyjednává prostory a kooperaci s ORP. Přeřadí přítomností těchto pracovišť zařazených v režimu vyšších povinností ORP do režimu vyšších povinností?

Odpověď NÚKIB:

- Ne, pronájem prostor pro subjekt v režimu vyšších povinností nemění režim povinností pronajímatele prostor (ani pokud poskytuje internetové připojení).
- Ani zástupci MMR nepočítají s tím, že by se tak stalo.
- Jde o standardní pronájem prostor ze strany MMR.
- Naopak ORP si vyřadí jednu část své agendy z rozsahu řízení KB a bude tam plnit požadavky, na kterých se domluví s MMR.
- Bude promítnuto do FAQ pro obce na portálu.



Národní úřad
pro kybernetickou
a informační bezpečnost

**Děkuji
za pozornost**

Daniela Procházková
regulace@nukib.gov.cz