PORTÁL NÚKIB

Často kladené otázky: Kybernetická bezpečnost obcí

TLP:CLEAR

15. ledna 2025

Verze 1.0

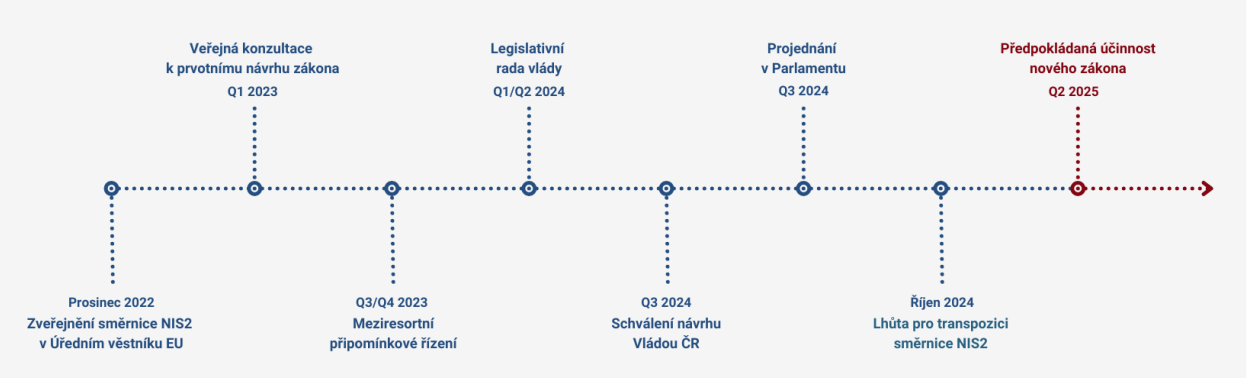
Národní úřad pro kybernetickou a informační bezpečnost

Co se dozvím v tomto dokumentu?

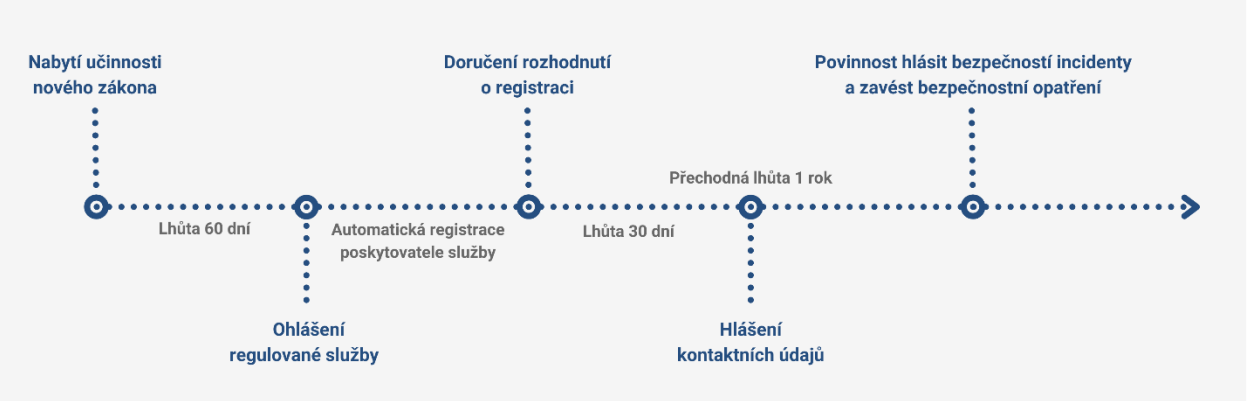
Tento dokument poskytuje stručné odpovědi na nejčastější otázky týkající se dopadů připravovaného návrhu nového zákona o kybernetické bezpečnosti na obce.

Pokud máte jakékoliv další otázky, podívejte se na www.portal.nukib.gov.cz nebo nám napište na regulace@nukib.gov.cz.

Harmonogram předpokládaného přijetí zákona



Harmonogram plnění jednotlivých povinností



Často kladené otázky

1 Obce s rozšířenou působností

1.1 Co budou muset plnit obce s rozšířenou působnosti?

Obec s rozšířenou působností je podle návrhu nového zákona o kybernetické bezpečnosti (dále jen „nový ZKB“) a vyhlášky o regulovaných službách **poskytovatelem regulované služby v režimu nižších povinností**. Budou se na ni vztahovat povinnosti z nového ZKB a vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále jen „vyhláška pro nižší režim“).

Hlavními povinnostmi jsou:

- ohlášení poskytování regulované služby,
- hlášení kontaktních údajů,
- hlášení incidentů s významným dopadem,
- zavádění bezpečnostních opatření dle vyhlášky pro nižší režim, a
- provedení protiopatření vydaných ze strany NÚKIB.

1.2 Je třeba zabezpečovat úplně všechno?

Není povinné zabezpečovat úplně celou organizaci, resp. všechna její aktiva. Zabezpečuje se vždy minimálně v rozsahu daném regulovanou službou, pro kterou organizace spadá do působnosti nového ZKB. Stanovení rozsahu řízení kybernetické bezpečnosti je povinným krokem, od kterého se odvíjí rozsah veškerých dalších povinností, pokud by nebyl rozsah stanoven, zabezpečuje se celá organizace. Podrobný návod ke stanovení rozsahu regulované služby „Výkon svěřených pravomocí“ je obsažen v materiálu Kybernetická bezpečnost obcí.

1.3 Kdy je potřeba začít novou regulaci řešit?

Bude-li nový ZKB přijat v souladu s výše uvedeným harmonogramem a stane se účinným od 1. 7. 2025. Je třeba pamatovat na povinnost provedení **ohlášení poskytování regulované služby ideálně v měsíci následujícím po účinnosti zákona**.

Následně bude mít každá obec s rozšířenou působností roční přechodnou lhůtu na zavedení bezpečnostních opatření. Zejména v organizacích, které doteď kybernetickou bezpečnost vůbec neřešily, je vhodné začít tuto problematiku postupně řešit v následujících měsících způsobem popsaným v další otázce.

Již nyní je nezbytné počítat se zaváděním bezpečnostních opatření při plánování finančních a personálních kapacit, nebo bude-li obec s rozšířenou působností v dohledné době pořizovat nový hardware či software.

1.4 Jak začít se zaváděním kybernetické bezpečnosti?

Ideálním **prvním krokem** je zorientování se v organizaci, kdy je třeba si zodpovědět následující základní otázky:

- Jaké agendy a služby vykonávám? Co z toho je „výkonem svěřených pravomocí“?
- Co je potřeba k výkonu relevantních agend a služeb? Bez čeho se neobejdu?

Nový ZKB tento povinný krok označuje v § 12 jako „stanovení rozsahu řízení kybernetické bezpečnosti“.

Druhým krokem by mělo být **zjištění aktuálního stavu kybernetické bezpečnosti v organizaci**. Spousta organizací již má řadu bezpečnostních opatření zavedených, byť o tom nevede žádný záznam, případně o tom vůbec neví (zamčená serverovna, pravidelná změna hesla, zálohování, automatické aktualizace, nainstalování antivirového softwaru, rozlišování administrátorských a uživatelských účtů a související řízení přístupů atp.).

Smyslem těchto dvou kroků je mimo jiné to, aby si organizace určila rozsah, ve kterém bude následně zavádět bezpečnostní opatření a nezaváděla následně opatření zbytečná, neúčelná, nehodící se nebo již prováděná. Podrobný postup určení rozsahu regulované služby „Výkon svěřených pravomocí“ je popsán v materiálu Kybernetická bezpečnost obcí.

Stěžejním bezpečnostním opatřením s minimálními náklady a maximálním užitkem je **školení zaměstnanců**. NÚKIB poskytuje zdarma sadu kurzů na svém osvětovém portálu.

1.5 Vztahuje se regulace pouze na přenesenou působnost obce?

Regulovaná služba „Výkon svěřených pravomocí“ zahrnuje výkon **obou působností, tedy přenesené i samostatné**. Podrobný návod ke stanovení rozsahu regulované služby „Výkon svěřených pravomocí“ je obsažen v materiálu Kybernetická bezpečnost obcí.

1.6 Může být obec s rozšířenou působností poskytovatelem jiné regulované služby než „Výkon svěřených pravomocí“?

Nemůže. Podle § 7 písm. b) nového ZKB se za podnik nepovažují mj. územní samosprávné celky, kterými jsou právě i obce. Jednoduše řečeno – **obec není podnik.** Z toho vyplývá, že obec nemůže nikdy naplnit velikostní kritéria, tedy být například středním či velkým podnikem. Právě velikost podniku je přitom stěžejní podmínkou pro registraci regulované služby podle § 4 nového ZKB.

Příklad: *Obec má celkem 80 zaměstnanců, zároveň zajišťuje pro své občany i vodu a má příslušnou vodohospodářskou licenci vystavenou na své IČO. Obec však není podnik, nenaplní tak velikostní kritéria pro výkon této regulované služby.*

1.7 Musí mít obec s rozšířenou působností manažera kybernetické bezpečnosti?

Nemusí. Poskytovatel regulované služby v režimu nižších povinností však musí určit osobu, která odpovídá za řízení a rozvoj kybernetické bezpečnosti, dohled nad stavem kybernetické bezpečnosti a komunikaci v oblasti kybernetické bezpečnosti s vrcholným vedením. Tato osoba bude typicky zároveň **kontaktní osobou** komunikující s NÚKIB prostřednictvím Portálu NÚKIB, např. při hlášení incidentu, provedení požadovaného protiopatření atp.

1.8 Kdo je „vrcholným vedením" obce s rozšířenou působností?

Jedním z bezpečnostních opatření dle § 14 odst. 2 písm. b) nového ZKB jsou **„požadavky na vrcholné vedení"**. Toto bezpečnostní opatření je relevantní pro všechny poskytovatele regulované služby v režimu nižších povinností, tudíž i obce s rozšířenou působností.

Konkrétní povinnosti vrcholného vedení pak stanovuje § 5 vyhlášky pro nižší režim. Tatáž vyhláška definuje v § 2 písm. e) vrcholné vedení jako *„statutární orgán nebo jiná osoba nebo skupina osob v obdobném postavení"*.

Nový ZKB neobsahuje žádná speciální pravidla týkající se výkonu pravomocí a působnosti orgánů obce (zejm. zastupitelstva a rady). Rada obce má dle § 102 odst. 2 zákona o obcích mimo jiné:

- a) zabezpečovat hospodaření obce podle schváleného rozpočtu, provádět rozpočtová opatření v rozsahu stanoveném zastupitelstvem obce,
- f) stanovit rozdělení pravomocí v obecním úřadu, zřizovat a zrušovat odbory a oddělení obecního úřadu,
- i) kontrolovat plnění úkolů obecním úřadem a komisemi v oblasti samostatné působnosti obce,
- m) schvalovat organizační řád obecního úřadu.

Z praktických důvodů tedy považujeme za vhodný výklad, aby byla za vrcholné vedení považována rada obce. Není vyloučeno svěření určitých pravomocí např. obecnímu úřadu v souladu s § 102 odst. 3 zákona o obcích. Není-li v obci zvolena rada, postupuje se standardně podle § 99 odst. 2 zákona o obcích a její pravomoci vykonává starosta.

2 Podniky zřizované obcemi s rozšířenou působností

Obecně platí, že regulovaná služba „Výkon svěřených pravomocí" nezahrnuje činnost dalších samostatných organizací (podniků) zřizovaných či zakládaných obcemi. Organizace zřízená či založená obcí tedy nemusí plnit povinnosti vyplývající z nového ZKB, pouze z toho důvodu, že je zřizována, založena či vlastněna obcí.

Tyto závěry se obdobně uplatní také pro podniky zřizované či založené **dobrovolným svazkem obcí** (§ 49 a násl. zákona o obcích) či **společenstvím obcí** (§ 53a a násl. zákona o obcích).

Problematika kybernetické bezpečnosti **městských částí a obecní policie** je podrobně popsána v materiálu Kybernetická bezpečnost obcí.

V obecnosti lze říci, že to, co spadá pod IČO obce a vykonává nějakou svěřenou pravomoc, je součástí rozsahu služby Výkon svěřených pravomocí – například obecní policie, která je orgánem obce.

2.1 Vztahuje se regulace i na příspěvkové organizace zřizované obcemi?

Tyto organizace jsou samostatnými právnickými osobami s vlastním IČO. Je třeba samostatně posoudit, zda poskytují některou z regulovaných služeb a splňují další podmínky podle vyhlášky o regulovaných službách. Není přitom důležité, že je zřizovatelem obec. Nedochází ani ke sčítání velikostních kritérií, tedy počtu zaměstnanců a výše ročního obratu nebo bilanční sumy roční rozvahy (viz otázka 2.3). Orientačně je možné pro určení působnosti nového ZKB použít kalkulačku na Portálu NÚKIB.

Činnost např. školy, muzea či zdravotnického zařízení není součástí výkonu regulované služby „Výkon svěřených pravomocí" ze strany obce s rozšířenou působností.

Typickými příspěvkovými organizacemi zřizovanými obcemi jsou:

- **školy a školská zařízení** – nespadají do působnosti nového ZKB,
- **muzea** – nespadají do působnosti nového ZKB,
- **zdravotnická zařízení** (nemocnice) – může teoreticky spadat do působnosti nového ZKB jakožto poskytovatel regulované služby „Poskytování zdravotní péče" v odvětví Zdravotnictví.

2.2 Vztahuje se regulace na obchodní společnosti zakládané či vlastněné obcemi?

Tyto organizace jsou samostatnými právnickými osobami s vlastním IČO. Je třeba samostatně posoudit, zda poskytují některou z regulovaných služeb a splňují další podmínky podle vyhlášky o regulovaných službách. Obec může typicky zakládat a vlastnit či spoluvlastnit společnosti s ručením omezeným (s.r.o.) nebo případně akciové společnosti (a.s.).

Rozhodné bude, zda taková společnost poskytuje některou z regulovaných služeb a zároveň naplňuje kritéria velikosti. Není přitom důležité, že je zřizovatelem obec. **Nedochází ke sčítání velikostních kritérií**, tedy počtu zaměstnanců a výše ročního obratu nebo bilanční sumy roční rozvahy (viz otázka 2.3).

Orientačně je možné pro určení působnosti nového ZKB použít kalkulačku na Portálu NÚKIB.

2.3 Jak je to v s počítáním velikosti obecních podniků?

Obce s rozšířenou působností spadají do působnosti nového ZKB bez ohledu na počet zaměstnanců, roční obrat nebo bilanční sumu roční rozvahy. Podle § 7 písm. b) nového ZKB se za podnik nepovažují mj. územní samosprávné celky, kterými jsou právě i obce.

Podniky, které mohou obce zřizovat či zakládat, však ukazatele velikosti řešit musí, poskytují-li některou z regulovaných služeb. **Počet zaměstnanců, roční obrat nebo bilanční suma roční rozvahy samotné obce se však při počítání velikosti podniků zřizovaných či zakládaných obcí nezohledňují**.

Příklad:

Podnik zajišťující odpadové hospodářství pro jednu nebo více obcí bude svou velikost počítat bez ohledu na to, že je zřizován či vlastněn jednou nebo více obcemi či svazkem obcí. ***Nebude*** *tedy docházet ke sčítání počtu zaměstnanců či dalších finančních ukazatelů tohoto podniku a obce, která ho založila, resp. ho vlastní.*

Rozhodnými ukazateli velikosti podniku zajišťujícího odpadové hospodářství tak bude počet jeho zaměstnanců, roční obrat nebo bilanční suma roční rozvahy. Nedochází k žádnému sčítání těchto ukazatelů mezi daným podnikem a obcí, která je jeho (spolu)vlastníkem či zřizovatelem.

3 Obce prvního a druhého stupně

3.1 Vztáhne se nový ZKB na obce prvního a druhého stupně?

Nový ZKB se na obce prvního a druhého stupně nevztahuje. Poskytovateli regulovaných služeb podle návrhu zákona jsou pouze obce s rozšířenou působností.

Dochází pouze k menší novelizaci **zákona o informačních systémech veřejné správy**, který bude nově stanovovat, že **správci informačních systémů veřejné správy** (kterými mohou být i obce prvního a druhého stupně), jsou povinni na jimi spravované informační systémy veřejné správy **přiměřeně zavádět bezpečnostní opatření** pro poskytovatele regulované služby v režimu nižších povinností.

3.2 Co konkrétně musejí plnit obce prvního a druhého stupně?

Smyslem je, aby se všichni správci ISVS v maximální možné míře snažili spravovat a provozovat své ISVS bezpečným způsobem, a tam, **kde je to možné a vhodné**, zaváděli bezpečnostní opatření dle příslušné vyhlášky pro nižší režim.

Může jít o dílčí jednoduchá opatření typu: dodržování doporučené délky a složitosti hesel, pravidelné změny hesel, pravidelné aktualizace operačního systému a dalších využívaných programů, zálohování důležitých dat patřičným způsobem, řízení přístupů pro jednotlivé zaměstnance obecních úřadů. Podrobnosti jsou v návrhu vyhlášky pro nižší režim, jejíž původní návrh je dostupný na stránkách Poslanecké sněmovny jakožto Sněmovní tisk č. 759, nicméně finální verze ještě nebyla schválena.

Tato základní opatření jsou popsána v podpůrném materiálu Kybernetická bezpečnost obcí, případně lze vycházet také z podpůrného materiálu Minimální bezpečnostní standard.

3.3 Mohou být obce prvního a druhého stupně pokutovány za nepřijetí takových opatření?

Tyto obce nemůžou být pokutovány za neplnění výše popsané povinnosti. Z § 38 zákona o obcích však vyplývá povinnost péče řádného hospodáře, tzn. povinnost starat se o svůj majetek a chránit jej. Je potřeba vzít na vědomí, že případný kybernetický incident může obci způsobit významné škody a zásadně zkomplikovat její běžné fungování.

4 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 sdílená 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**
15. ledna 2025	1.0	OREG/OK	Vytvoření dokumentu