PORTÁL NÚKIB

Často kladené otázky: Výkon svěřených pravomocí

TLP:CLEAR

9. února 2026

Verze 1.0

Národní úřad pro kybernetickou a informační bezpečnost

Obsah

1 Co se dozvím v tomto dokumentu?

Tento dokument obsahuje odpovědi na často kladené otázky související s regulovanou službou Výkon svěřených pravomocí. Tato regulovaná služba je specifická způsobem svého vymezení, jelikož zahrnuje širokou škálu veřejných institucí vykonávajících různorodé agendy.

S ohledem na tato specifika a časté dotazy ze strany veřejné správy považujeme za nezbytné zodpovědět nejasnosti související s ohlášením regulované služby, následným hlášením údajů i stanovením rozsahu řízení kybernetické bezpečnosti.

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

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

2 Ohlášení regulované služby

2.1 Co přesně se má ohlásit? Je třeba hlásit původní významné informační systémy či prvky kritické informační infrastruktury?

Poskytovatel regulované služby Výkon svěřených pravomocí hlásí tuto službu vždy pouze jednou. Ohlášení služby se neprovádí opakovaně pro každou jednotlivou agendu vedenou v Registru práv a povinností, případně pro každý z informačních systémů sloužících k výkonu těchto agend.

Vzhledem k přechodu z konceptu regulovaných informačních systémů na regulované služby se u ohlášení regulované služby neprojeví kontinuita mezi původním zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a novým zákonem č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „nový ZKB“). Původně regulované systémy (ať už významné informační systémy nebo prvky kritické informační infrastruktury) spadají všechny dohromady pod jednu regulovanou službu Výkon svěřených pravomocí.

Výše popsaný způsob ohlášení nebrání tomu, aby poskytovatel regulované služby interně evidoval jednotlivé informační systémy a k nim přiřazená primární aktiva v rámci řízení KB v organizaci.

2.2 Nejsme si jisti, kam přesně v rámci v odvětví Veřejná správa spadáme. Jde někde zjistit více informací?

Podrobnější výklad k jednotlivým kategoriím poskytovatelů regulované služby Výkon svěřených pravomocí v příloze č. 1 vyhlášky č. 408/2025 Sb., o regulovaných službách (dále jen „vyhláška o regulovaných službách“), je dostupný v Důvodové zprávě k vyhlášce o regulovaných službách (str. 4 a následující).

Pokud nenaleznete odpověď ani v důvodové zprávě, napište dotaz na regulace@nukib.gov.cz.

2.3 Je třeba počítat velikost podniku?

Pro regulovanou službu Výkon svěřených pravomocí není třeba řešit velikost podniku.

Podle § 7 nového ZKB platí, že se **organizační složky státu, územní samosprávné celky** (obce a kraje) **a Česká národní banka** (dále jen "ČNB") **nepovažují za podnik,** tudíž se u nich velikost podniku neřeší.

Na profesní komory či vysoké školy se výjimka dle § 7 nového ZKB neuplatní, a tyto organizace tedy jsou podnikem. V rámci odvětví veřejné správy však není velikost podniku podmínkou pro registraci regulované služby Výkon svěřených pravomocí. Pokud tedy není profesní komora či vysoká škola poskytovatelem jakékoliv další regulované služby, není třeba u nich velikost podniku počítat.

2.4 Mohou být organizační složky státu, územní samosprávné celky nebo ČNB poskytovateli jiných regulovaných služeb?

Organizační složky státu, územní samosprávné celky a ČNB teoreticky **mohou být poskytovateli dalších regulovaných služeb** (nad rámec služby Výkon svěřených pravomocí). Tato možnost připadá v úvahu pouze u regulovaných služeb, kde velikost podniku není jednou z podmínek pro registraci. Ověření lze provést prostřednictvím Kalkulačky na Portálu NÚKIB, kde jsou tyto varianty zohledněny.

Teoreticky tak může být organizační složka státu nebo územní samosprávný celek například kvalifikovaným poskytovatelem služby vytvářející důvěru, případně kvalifikovaným správcem systému elektronické identifikace v rámci odvětví Digitální infrastruktura a služby.

Obec či kraj však **nemohou být** poskytovateli regulované služby např. Provozování kanalizace pro veřejnou potřebu či Provozování vodovodu pro veřejnou potřebu, protože u obou těchto regulovaných služeb je velikost podniku podmínkou pro registraci regulované služby.

2.5 Je třeba zvlášť ohlašovat organizace zřizované či vlastněné obcí či krajem?

Obchodní korporace či příspěvkové organizace zřizované či vlastněné krajem či obcí mají vlastní IČO, a posuzují se tudíž samostatně. Taková organizace si musí samostatně vyhodnotit, zda je poskytovatelem regulované služby např. prostřednictvím Kalkulačky na Portálu NÚKIB. Pokud splní podmínky registrace, pak samostatně provede ohlášení regulované služby.

Typickým příkladem mohou být společnosti zřízené obcí či krajem vykonávající službu Provozování kanalizace pro veřejnou potřebu, Provozování vodovodu pro veřejnou potřebu, Poskytování zdravotní péče, případně regulované služby z odvětví Digitální infrastruktura a služby.

Vzhledem k tomu, že se obce a kraje nepovažují za podnik, nedochází při počítání velikosti podniku ke sčítání ukazatelů mezi obcí či krajem a zřizovanou či vlastněnou organizací.

Specifické postavení městské policie či městských částí (které nejsou specificky zmíněny v rámci služby Výkon svěřených pravomocí) je blíže popsáno v podpůrném materiálu Kybernetická bezpečnost obcí.

2.6 Je třeba zvlášť ohlašovat organizace zřizované organizační složkou státu, resp. podřízené organizace?

Postavení takových podřízených či zřízených organizací bohužel není nijak jednotně upraveno a řídí se většinou specifickým zákonem. Pokud taková organizace naplní podmínku významnosti poskytovatele regulované služby pro službu Výkon svěřených pravomocí v příloze č. 1 vyhlášky o regulovaných službách, pak by měla provést samostatné ohlášení regulované služby.

Pro příspěvkové organizace zřízené organizačními složkami státu platí obdobně odpověď uvedená výše u předchozí otázky. **Takové organizace si musí samostatně vyhodnotit, zda jsou s ohledem na svou činnost a velikost poskytovateli regulované služby**. Každopádně neplatí, že by příspěvková organizace automaticky spadala do působnosti nového ZKB pouze z toho důvodu, že je zřízena organizační složkou státu, a to bez ohledu na to, zda tato organizační složka státu je či není poskytovatelem regulované služby.

2.7 Jak je možné zjistit, kdo je v základních registrech veden jako statutární orgán organizace, který může provést ohlášení regulované služby?

Informace o statutárních orgánech konkrétní organizace je možné získat pomocí služby Veřejný výpis údajů osoby evidované v registru osob.

Další podrobnosti k procesu ohlášení regulované služby či pověřování zástupců organizace jsou uvedeny v materiálech Jak ohlásit regulovanou službu a Kdo jsou zástupci organizace a jak se pověřují.

2.8 Pokud organizace nenaplňuje kritéria dle vyhlášky o regulovaných službách, může se stát, že bude stejně zařazena do regulace?

Pokud Vaše organizace:

- aktuálně nespadá do žádné z kategorií uvedených u regulované služby Výkon svěřených pravomocí ve vyhlášce o regulovaných službách (nesplňujete tzv. podmínky významnosti poskytovatele regulované služby), a zároveň
- jste dříve byli správcem významného informačního systémů nebo prvku kritické informační infrastruktury podle původního zákona o kybernetické bezpečnosti,

pak je možné, že Vás Národní úřad pro kybernetickou a informační bezpečnost (**NÚKIB) určí jako poskytovatele regulované služby podle § 5 nového ZKB**. Toto ustanovení obsahuje kritéria, na základě kterých může k určení ze strany NÚKIB dojít.

Určení podle § 5 nového ZKB probíhá v rámci správního řízení, které **vede NÚKIB z moci úřední**. Není tedy potřeba podávat jakoukoliv žádost o určení. **Toto určování bude probíhat především v průběhu**

roku 2026. Teoreticky je možné podat podnět k zahájení určovacího řízení, pokud by organizace na své určení spěchala. Na určení podle § 5 nového ZKB však neexistuje právní nárok.

Předběžné konzultace k určování je možné provést prostřednictvím e-mailu regulace@nukib.gov.cz.

3 Stanovení rozsahu řízení kybernetické bezpečnosti (KB)

3.1 Co vše zahrnuje regulovaná služba Výkon svěřených pravomocí?

Každý z orgánů vyjmenovaných v rámci služby Výkon svěřených pravomocí byl zřízen za účelem výkonu zákonem specifikovaných agend, čemuž odpovídají zákonem svěřené pravomoci.

Zjednodušeně řečeno má poskytovatel regulované služby Výkon svěřených pravomocí do svého stanoveného rozsahu řízení KB zahrnout veškerá aktiva, která potřebuje k tomu, aby byl schopen řádně vykonávat veškeré svěřené pravomoci (svou agendu).

Toto vymezení vyplývá z povahy veřejné správy, kde jednotlivé organizace existují za jasně vymezeným účelem. Obchodní společnosti oproti tomu často vykonávají mnoho různých činností, z nichž některé mohou být regulovanými službami dle nového ZKB a jiné nemusí. Z tohoto důvodu může u soukromé společnosti teoreticky spadat do stanoveného rozsahu řízení KB pouze úzce vymezená množina aktiv. U veřejné správy tato situace spíš nastávat nebude. To však neznamená, že by v rámci veřejné správy bylo potřeba zabezpečovat vždy veškerá aktiva dané organizace a už vůbec to neznamená, že se veškerá aktiva musí zabezpečovat na stejné úrovni.

Vzhledem k odlišnostem jednotlivých organizací nelze paušálně vyjmenovat konkrétní aktiva, která budou typicky spadat do stanoveného rozsahu řízení KB. Do tohoto rozsahu mohou spadat aktiva související mimo jiné s:

- fungováním agendových informačních systémů[1],
- fungováním elektronické pošty organizace,
- výkonem spisové služby,
- vedením úřední desky nebo
- zajišťováním kontrolní či inspekční činnosti.

Nejde o kompletní seznam, ale pouze u výčet příkladů. Řada organizací bude disponovat dalšími specifickými aktivy souvisejícími s Výkonem svěřených pravomocí.

[1] Viz § 2 písm. f) zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

3.2 Která aktiva mohou spadat mimo stanovený rozsah řízení KB při poskytování služby Výkon svěřených pravomocí?

Aktiva **nesouvisející** s poskytováním regulované služby Výkon svěřených pravomocí **nemusejí spadat do stanoveného rozsahu řízení KB**. K zavádění a provádění bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů či provádění reaktivních protiopatření přitom dochází pouze v rámci stanoveného rozsahu.

S ohledem na různé kontexty regulovaných organizací **není možné vyjmenovat typová aktiva, která půjde vždy vyjmout ze stanoveného rozsahu**. Vždy bude záležet na konkrétním kontextu organizace a vzájemných vazbách primárních a podpůrných aktiv.

3.3 Co je třeba zvážit při vyjmutí určitého aktiva ze stanoveného rozsahu řízení KB?

Při úvahách o vyjmutí určitého aktiva ze stanoveného rozsahu řízení KB je třeba zvážit mimo jiné následující otázky.

1) **Může mít aktivum byť jen nepřímý vliv na řádné poskytování regulované služby?**

> Aktiva k zajištění fyzické bezpečnosti (turnikety na čipové karty a související software) na první pohled přímo nesouvisí s poskytováním služby Výkon svěřených pravomocí. Pokud by narušení důvěrnosti, integrity či dostupnosti těchto aktiv mohlo způsobit, že se např. zaměstnanci nedostanou do svých kanceláří, nebo se do prostor úřadu mohou neoprávněně dostat cizí osoby, může dojít k **narušení řádného poskytování služby Výkon svěřených pravomocí**.
>
> Tato aktiva by tedy měla být součástí stanoveného rozsahu řízení KB (jde navíc o bezpečnostní opatření podle § 17 vyhlášky č. 409/2025 Sb.).

2) **Jsou dostatečně zohledněny možné dopady narušení integrity či důvěrnosti (nejen dostupnosti)?**

> Poskytovatel regulované služby Výkon svěřených pravomocí se může domnívat, že je schopen řádně poskytovat službu i v případě **nedostupnosti** určitého aktiva. To samo o sobě nestačí k vyjmutí tohoto aktiva ze stanoveného rozsahu řízení KB. Je třeba brát v potaz také možné dopady narušení **důvěrnosti či integrity**.
>
> Dostupnost určitých údajů v papírové podobě neznamená, že je nemusím zabezpečovat v jejich elektronické formě. Nedostupnost údajů v elektronické formě by sice neměla dopad na dostupnost služby, nicméně stále hrozí narušení integrity či důvěrnosti.

3) **Je podpůrné aktivum propojeno s dalšími aktivy, z nichž některá spadají do stanoveného rozsahu řízení KB?**

Praktickým příkladem je koncová stanice (počítač), která běžně není používána k Výkonu svěřených pravomocí, ale lze se skrze ni dostat i k dalším aktivům, která už s Výkonem svěřených pravomocí souvisí. Pokud by z takové stanice šlo přistupovat např. k informacím, které jsou primárním aktivem ve stanoveném rozsahu, pak by samotná stanice nemohla spadat mimo stanovený rozsah.

Při stanovování rozsahu řízení KB je třeba vzít v úvahu vzájemné propojení aktiv (reálný stav v organizaci).

3.4 Odkud čerpat informace o tom, co spadá mezi svěřené pravomoci?

Poskytovatelé regulované služby Výkon svěřených pravomocí vychází z předpisů, které určují jejich pravomoci (např. NÚKIB ze zákona o kybernetické bezpečnosti a částečně ze zákona o utajovaných informacích).

Přehled o vykonávaných agendách lze získat také z Registru práv a povinností, který obsahuje informace o tom, jaké agendy konkrétní orgán veřejné moci vykonává. Doporučujeme ověřit, zda se na výkonu agendy poskytovatel regulované služby skutečně podílí, tedy zda údaje v RPP odpovídají realitě.

Podpůrně lze vycházet z organizační struktury poskytovatele regulované služby, která je typicky rozčleněna podle vykonávaných agend (byť není vyloučeno, že více organizačních celků pracuje na stejné agendě, případně jeden celek vykonává více dílčích agend).

3.5 Spadají do stanoveného rozsahu řízení KB také centrálně spravované systémy, které používáme pouze jako uživatelé?

Poskytovatelé regulované služby Výkon svěřených pravomocí standardně pracují s informačními systémy, které jsou spravovány a provozovány např. ústředními orgány státní správy. Typicky základní registry, z nichž řada orgánů či úřadů využívá údaje, ale nespravují tyto systémy. Obdobně používají všechny „úřady" k výkonu své působnosti Informační systém datových schránek, který však spravuje Ministerstvo vnitra, resp. provozuje Česká pošta.

Využívání těchto systémů vyplývá přímo ze zákona a poskytovatel služby Výkon svěřených pravomocí nemá možnost tyto systémy nepoužívat. Nejedná se o klasicky dodavatelský vztah. Mezi správci těchto centrálních systémů a jejich uživateli zpravidla nejsou uzavírány smlouvy. Neuplatní se tedy požadavky na obsah smluv s dodavateli, ať už jde o režim vyšších či nižších povinností (viz příloha č. 2 vyhlášky č. 410/2025 Sb. a příloha č. 5 vyhlášky č. 409/2025 Sb.). Poskytovatel regulované služby Výkon svěřených pravomocí nemusí v těchto případech evidovat správce centrálního systému jako svého významného dodavatele a jakkoli jej řídit či informovat.

Povinnost zavádět bezpečnostní opatření ve vztahu k těmto systémům dopadá na jejich správce. Poskytovatel regulované služby Výkon svěřených pravomocí v pozici uživatele tedy nemá povinnost, ani možnost, přímo zabezpečovat například Informační systém datových schránek nebo další centrální registry. Správce daného systému však může stanovit určité bezpečnostní požadavky, kterými se uživatelé musí řídit.

Poskytovatel služby Výkon svěřených pravomocí v pozici uživatele každopádně musí zavést bezpečnostní opatření, aby nedocházelo např. k neoprávněným přístupům do těchto centrálních systémů nebo k neoprávněným zásahům do údajů vedených v daném systému (tato povinnost vyplývá mj. ze zákona č. 111/2009 Sb., o základních registrech).

Do stanoveného rozsahu řízení KB tak budou typicky spadat podpůrná aktiva, prostřednictvím kterých poskytovatel k centrálním systémům přistupuje.

3.6 Je možné stanovený rozsah řízení KB rozdělit na dílčí rozsahy?

Stanovený rozsah řízení KB podle § 12 nového ZKB není možné dělit na dílčí stanovené rozsahy v rámci jednoho poskytovatele regulované služby. Rozdělení stanoveného rozsahu na dílčí části je možné provést v rámci řízení primárních a podpůrných aktiv. Tímto způsobem je možné v organizaci interně rozdělit odpovědnosti a povinnosti v rámci systému řízení bezpečnosti informací. Z pohledu NÚKIB jde však stále o jednu organizaci.

V materiálu Kybernetická bezpečnost obcí je popsáno, že např. obecní policie nemá vlastní IČO a je formálně součástí obce, která ji zřizuje. Obě tyto složky mohou teoreticky řídit svou kybernetickou bezpečnost samostatně tím způsobem, že si interně rozdělí odpovědnosti a povinnosti za jednotlivá aktiva ve stanoveném rozsahu. Poskytovatelem regulované služby Výkon svěřených pravomocí je v tomto případě pouze obec s rozšířenou působností, nikoliv samotná obecní policie. Případně vydaná rozhodnutí či uložené sankce tak dopadají na samotnou obec, nikoliv obecní policii.

3.7 Kde lze najít další podrobnosti ke stanovení rozsahu řízení KB?

Existuje specifický podpůrný materiál Stanovení rozsahu řízení kybernetické bezpečnosti. Ten popisuje proces stanovení rozsahu obecně bez ohledu na konkrétní regulovanou službu.

Konkrétnější návod pro obce s rozšířenou působností je dostupný v materiálu Kybernetická bezpečnost obcí, kde se řeší specificky problematika městské policie či městských částí.

V případě nejasností se s dotazy obracejte na e-mail regulace@nukib.gov.cz.

4 Hlášení údajů

Povinnosti hlášení údajů podle § 11 nového ZKB se podrobně věnuje podpůrný materiál Hlášení údajů k regulovaným službám, kde je přesně popsáno, jaké údaje se musí a nemusí hlásit.

Důležité je připomenout, že poskytovatel regulované služby má povinnost údaje udržovat aktuální. Případné změny údajů, které nejsou referenčními údaji vedenými v základních registrech, je třeba hlásit nejpozději do 14 dnů ode dne, kdy došlo k jejich změně.

4.1 Je možné v rámci hlášení údajů rozlišit, k jakým informačním systémům se údaje hlásí?

Nahlášené údaje se vztahují k regulované službě jako celku. Nahlášené údaje tedy není možné v rámci Portálu NÚKIB třídit či rozlišovat podle konkrétních informačních systémů, se kterými souvisí. Poskytovatel regulované služby Výkon svěřených pravomocí si tuto problematiku řeší interně v rámci řízení aktiv (např. eviduje vztahy mezi veřejnými IP adresami či doménami a dalšími aktivy ve stanovém rozsahu řízení KB).

5 Přechodná ustanovení

5.1 Jak zajišťovat kybernetickou bezpečnost v přechodném období, pokud byla organizace dříve správcem VIS či KII?

Této problematice se věnuje shrnující materiál Přechodná ustanovení v zákoně o kybernetické bezpečnosti.

Poskytovatelé regulované služby v režimu vyšších povinností zabezpečují informační systémy regulované podle starého ZKB v rozsahu, ve kterém jsou služby a aktiva regulovány novým ZKB. V tomto rozsahu také hlásí během přechodného období kybernetické bezpečnostní incidenty.

Dříve regulované VIS a KII typicky budou spadat do stanoveného rozsahu řízení KB podle nového ZKB. Možnost „vypadnutí“ určité části dříve regulovaných aktiv ze stanoveného rozsahu řízení KB, a tedy působnosti nového ZKB, je spíš nepravděpodobná. Naopak může dojít k zachování původního rozsahu, případně k rozšíření množiny aktiv souvisejících s poskytováním regulované služby Výkon svěřených pravomocí.

V režimu vyšších povinností se poskytovatelé regulované služby řídí vyhláškou č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

Poskytovatelé regulované služby v režimu nižších povinností se soustředí pouze na bezpečnostní opatření podle vyhlášky č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností. Opatření, která jdou nad rámec požadavků stanovených pro režim nižších povinností, poskytovatel regulované služby v režimu nižších povinností **nemusí nadále plnit**. Dobrovolné plnění přísnějších požadavků není vyloučeno.

6 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**
9. února 2026	1.0	OREG	Vytvoření dokumentu