



KATEDRA  
INFORMAČNÍCH  
TECHNOLOGIÍ  
PEF ČZU V PRAZE

# Nové povinnosti tisíců obcí v oblasti bezpečnosti po novele ZoISVS

Proč se § 5b zákona o ISVS může stát klíčovým bezpečnostním pravidlem pro obce.

Ing. Miroslav Pavelka, doc. Ing. Jan Jarolímek, Ph.D.



Česká  
zemědělská  
univerzita  
v Praze

ISSS 2026 | Hradec Králové



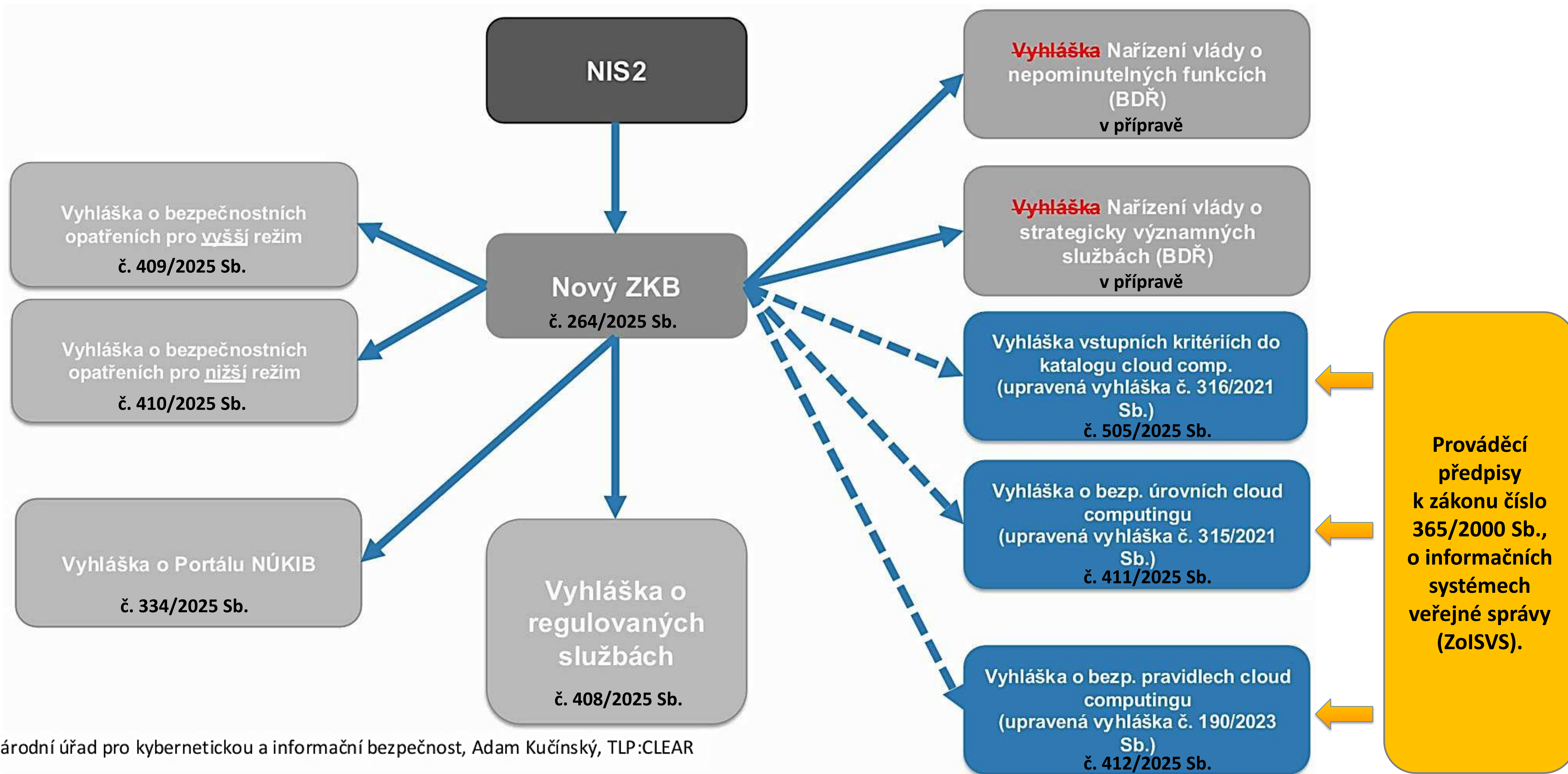
## Legislativní rámec kybernetické bezpečnosti



KATEDRA  
INFORMAČNÍCH  
TECHNOLOGIÍ  
PEF ČZU V PRAZE



# Ekosystém nového zákona o kybernetické bezpečnosti



## ➤ **Zákon č. 264/2025 Sb., o kybernetické bezpečnosti**

- Nový rámec kybernetické bezpečnosti v ČR
- Účinný od 1. 11. 2025; ruší původní zákon 181/2014 Sb.

## ➤ **Zákon č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti**

- Účinný od 1. 11. 2025
- V souvislosti s přijetím nového ZKB **mění 8 zákonů**: *Zákon o prověřování zahraničních investic; Zákon o Celní správě České republiky; Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, Zákon o provádění mezinárodních sankcí, Zákon o elektronických komunikacích, **Zákon o informačních systémech veřejné správy**, Zákon o poštovních službách, Zákon o bankách)*

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

- Účinný od 19. 8. 2025
- Stanoví působnost státu, práva a povinnosti k zajištění poskytování „základních služeb“ a k posilování odolnosti subjektů kritické infrastruktury
- Zavádí vládní Strategii pro posílení odolnosti a vymezuje věcnou působnost rezortů, přičemž klade důraz na koordinaci s orgány dle zákona o kybernetické bezpečnosti

# Prováděcí předpisy

## **1. Vyhláška o regulovaných službách → č. 408/2025 Sb.**

- Upravuje kritéria pro určení regulovaných osob a kritéria pro stanovení režimu regulace (vyšší/nížší).

## **2. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností → č. 409/2025 Sb.**

- Upravuje v detailu bezpečnostní opatření pro povinné osoby ve vyšším režimu.

## **3. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností → č. 410/2025 Sb.**

- Upravuje v detailu bezpečnostní opatření pro povinné osoby v nižším režimu.
- Upravuje způsob identifikace incidentů s významným dopadem (pro účely hlášení incidentů).

## **4. Vyhláška o Portálu NÚKIB → č. 334/2025 Sb.**

- Upravuje procesní a technické náležitosti řešení automatizace a elektronizace procesů NÚKIB, náležitosti pro hlášení údajů, incidentů, přístupu k informacím a elektronickým službám poskytovaným NÚKIB a plněním vůči NÚKIB ze strany povinných subjektů.

## **5. Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy → č. 411/2025 Sb.**

- Úprava existující vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci
- V souvislosti s přesunem zmocnění ze zákona o kybernetické bezpečnosti do zákona o informačních systémech veřejné správy dojde ke zrušení stávající vyhlášky č. 315/2021 Sb. a je tedy nutné vydat vyhlášku znovu i s úpravami, které reflektují změny definic v zákoně apod.

## **6. Vyhláška o bezpečnostních pravidlech pro orgány VS využívající služby poskytovatelů cloud computingu → č. 412/2025 Sb.**

- Úprava existující vyhlášky č. 190/2023 Sb.
- V souvislosti s přesunem zmocnění ze zákona o kybernetické bezpečnosti do zákona o informačních systémech veřejné správy dojde ke zrušení stávající vyhlášky č. 190/2023 Sb. a je tedy nutné vydat vyhlášku znovu i s úpravami, které reflektují změny definic v zákoně apod.

## **7. Vyhláška o některých požadavcích pro zápis do katalogu cloud computingu → č. 505/2025 Sb.**

- Úprava existující vyhlášky č. 316/2021 Sb.

## **8. Nařízení vlády o nepominutelných funkcích stanoveného rozsahu → stále v přípravě**

- Upravuje, které funkce strategicky významných služeb jsou vždy zahrnuty v mechanismu prověřování bezpečnosti dodavatelského řetězce.

## **9. Nařízení vlády o strategicky významných službách → stále v přípravě**

*(Nařízení vlády o regulovaných službách, které splňují podmínky strategicky významné služby a o částech strategicky významných služeb tvořících nezbytný rozsah zajištění dostupnosti strategicky významných služeb (nařízení o strategicky významných službách))*

- Upravuje, koho se bude mechanismus prověřování bezpečnosti dodavatelského řetězce týkat.





## Režimy regulace

V ČR máme dvě úrovně regulace kybernetické bezpečnosti



# Režimy regulace v ČR – nižší / vyšší režim

**Směrnice NIS2 (EU 2022/2555) zavádí dvě kategorie regulovaných subjektů:**

- Essential entities
- Important entities

→ Cílem je proporcionalita požadavků – podle velikosti, sektoru a významu služby

**Česká transpozice (zákon č. 264/2025 Sb.) zavádí dvě úrovně regulace:**

- Režim nižších povinností (vyhláška č. 410/2025 Sb.)
- Režim vyšších povinností (vyhláška č. 409/2025 Sb.)



# Struktura vyhlášek o bezpečnostních opatřeních

## Vyšší režim (v. č. 409/2025 Sb.)

### Bezpečnostní opatření - organizační (§ 3–16):

- Systém řízení bezpečnosti informací
- Požadavky na vrcholné vedení
- Stanovení bezpečnostních rolí
- Řízení bezpečnostní politiky a bezpečnostní dokumentace
- Řízení aktiv
- Řízení rizik
- Řízení dodavatelů
- Bezpečnost lidských zdrojů
- Řízení změn
- Akvizice, vývoj a údržba
- Řízení přístupu
- Zvládání kybernetických bezpečnostních událostí a incidentů
- Řízení kontinuity činností
- Provádění auditu kybernetické bezpečnosti

### Bezpečnostní opatření - technická (§ 17–28):

- Fyzická bezpečnost
- Bezpečnost komunikačních sítí
- Správa a ověřování identit
- Řízení přístupových práv a oprávnění
- Detekce kybernetických bezpečnostních událostí
- Zaznamenávání událostí
- Vyhodnocování kybernetických bezpečnostních událostí
- Aplikační bezpečnost
- Kryptografické algoritmy
- Zajišťování dostupnosti regulované služby
- Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

## Nižší režim (v. č. 410/2025 Sb.)

### Bezpečnostní opatření (§ 3–13):

- Systém zajišťování minimální kybernetické bezpečnosti
- Požadavky na vrcholné vedení
- Bezpečnost lidských zdrojů
- Řízení kontinuity činností
- Řízení přístupu
- Řízení identit a jejich oprávnění
- Detekce a zaznamenávání kybernetických bezpečnostních událostí
- Řešení kybernetických bezpečnostních incidentů
- Bezpečnost komunikačních sítí
- Aplikační bezpečnost
- Kryptografické algoritmy

### Stanovení významnosti dopadu kybernetického bezpečnostního incidentu (§ 14)

# Oblasti regulovaných služeb dle v. č. 408/2025 Sb. – 22 skupin (102 služeb)

## 1. **Veřejná správa**

2. Energetika – Elektřina
3. Energetika – Ropa a ropné produkty
4. Energetika – Zemní plyn
5. Energetika – Teplárenství
6. Energetika – Vodík
7. Výrobní průmysl
8. Potravinářský průmysl
9. Chemický průmysl
10. Vodní hospodářství
11. Odpadové hospodářství

12. Letecká doprava
13. Drážní doprava
14. Námořní vodní doprava
15. Silniční doprava
16. Digitální infrastruktura a služby
17. Finanční trh
18. Zdravotnictví
19. Věda, výzkum a vzdělávání
20. Poštovní a kurýrní služby
21. Obranný průmysl
22. Vesmírný průmysl



# Regulovaná služba → 1. Veřejná správa → 1.1 Výkon svěřených pravomocí

## I. Poskytovatelem regulované služby v režimu vyšších povinností je

- a) ústřední orgán státní správy,
- b) jiný správní úřad s celostátní působností neuvedený v písmeni a),
- c) ústředí, generální nebo ústřední inspektorát, generální nebo ústřední ředitelství nebo obdobná součást správního úřadu, kterým jsou podřízeny součásti správního úřadu s krajskou, okresní nebo jinou územní působností,
- d) Kancelář prezidenta republiky,
- e) Kancelář Senátu,
- f) Kancelář Poslanecké sněmovny,
- g) Česká národní banka,
- h) Policejní prezidium České republiky,
- i) krajské ředitelství Policie České republiky,
- j) útvar Policie České republiky s celostátní působností, který zajišťuje speciální policejní činnosti v oblasti odhalování nelegální migrace, letecké služby, pyrotechnické služby, kriminalistických expertíz, ochrany ústavních činitelů České republiky, dalších určených osob a chráněných objektů nebo boje proti organizovanému zločinu, terorismu a kybernetické kriminalitě,

- k) Generální inspekce bezpečnostních sborů,
- l) součást Hasičského záchranného sboru České republiky podle § 5 písm. a) až c) zákona o hasičském záchranném sboru,
- m) Kancelář veřejného ochránce práv a ochránce práv dětí,
- n) Nejvyšší kontrolní úřad,
- o) Úřad pro zastupování státu ve věcech majetkových,
- p) Správa úložišť radioaktivních odpadů,
- q) Ústavní soud,
- r) zdravotní pojišťovna,
- s) **kraj**, nebo
- t) **hlavní město Praha**.

## II. Poskytovatelem regulované služby v režimu nižších povinností je

- a) správní úřad nebo jeho součást s krajskou, okresní nebo jinou územní působností,
- b) profesní komora,
- c) vysoká škola,
- d) Akademie věd České republiky,
- e) **obec s rozšířenou působností**, nebo
- f) **městská část Praha 1 až Praha 22**.

# Přímá regulace samospráv

Vyhláška č. 408/2025 Sb. řeší veřejnou správu podle typu subjektu a režimu povinností.

## 14

krajů včetně hl. m. Prahy  
v režimu vyšších povinností

## 205

obcí s rozšířenou působností  
v režimu nižších povinností

## 22

městských částí Prahy  
v režimu nižších povinností

**Obce I. a II. typu nejsou přímo poskytovatelem regulované služby podle nového ZoKB.**

To ale neznamená, že stojí mimo nový bezpečnostní rámec.



# Skrytý most: § 5b zákona č. 365/2000 Sb., o ISVS

Pokud je obec správcem alespoň jednoho ISVS, do hry vstupuje nepřímý dopad přes zákon č. 365/2000 Sb.



**Zákon výslovně počítá s přiměřeností: dopad na důvěrnost, integritu a dostupnost konkrétního ISVS + vhodnost a proveditelnost opatření.**

**metodicky: začít plnit nejpozději do 1. 11. 2026**



## § 2 ZoISVS

### 1) Pro účely tohoto zákona se rozumí

- a) informační činností získávání a poskytování informací, reprezentace informací daty, shromažďování, vyhodnocování a ukládání dat na nosiče a uchovávání, vyhledávání, úprava nebo pozměňování dat, jejich předávání, šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace dat ukládaných na nosičích. **Informační činnost je prováděna správci, provozovateli a uživateli informačních systémů veřejné správy prostřednictvím technických a programových prostředků,**
- b) **informačním systémem veřejné správy funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy nebo plnění jiných funkcí státu anebo dalších veřejnoprávních korporací.** Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále technické a programové prostředky, případně jiné nástroje umožňující výkon informačních činností,
- c) **správce** informačního systému veřejné správy osoba nebo její součást, která poskytuje služby informačního systému veřejné správy a **za informační systém veřejné správy odpovídá,**
- d) **provozovatelem** informačního systému veřejné správy osoba nebo její součást, která **zajišťuje funkčnost technických a programových prostředků** tvořících informační systém veřejné správy. Provozováním informačního systému veřejné správy může správce pověřit jiné osoby nebo jejich součásti, pokud to jiný zákon nevyklučuje,

## § 5b ZoISVS

→ po novele zákonem č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

**Správci informačních systémů veřejné správy, kteří nejsou poskytovateli regulované služby podle zákona o kybernetické bezpečnosti, jsou povinni na jimi spravované informační systémy veřejné správy zavádět bezpečnostní opatření pro poskytovatele regulované služby v režimu nižších povinností podle § 8, 13 a 14 zákona o kybernetické bezpečnosti, a to přiměřeně s ohledem na možné dopady narušení důvěrnosti, integrity a dostupnosti konkrétního informačního systému veřejné správy na činnost jeho správce a jeho schopnost poskytovat své služby občanům, a dále vhodnost a proveditelnost těchto opatření.**



## § 5b ZoISVS

→ po novele zákonem č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

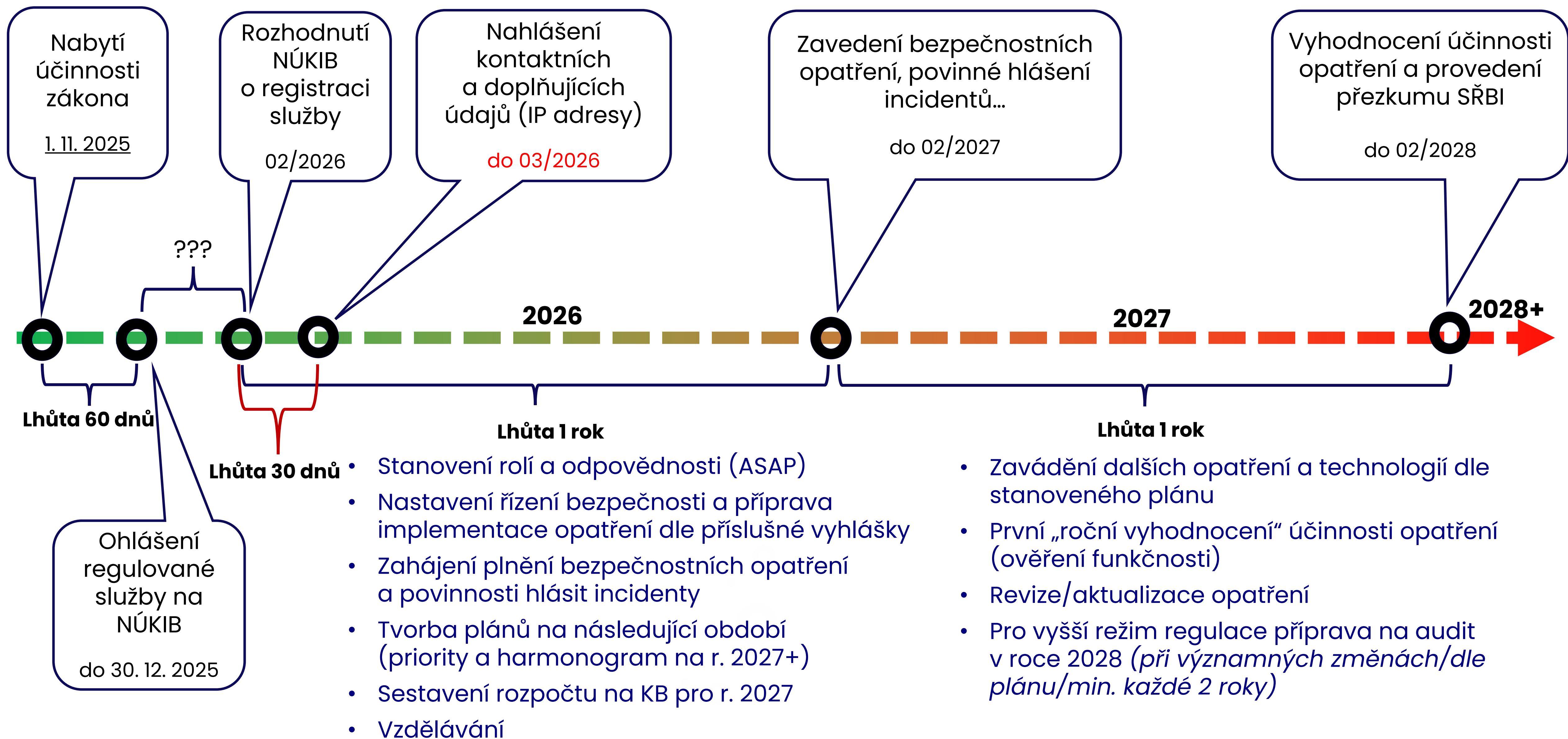
**zavádět bezpečnostní opatření pro poskytovatele regulované služby v režimu nižších povinností podle § 8, 13 a 14 zákona o kybernetické bezpečnosti**

## § 14 zákona 264/2025 Sb., o kybernetické bezpečnosti

- a) systém zajišťování minimální kybernetické bezpečnosti,
- b) požadavky na vrcholné vedení,
- c) řízení aktiv,
- d) řízení rizik,
- e) bezpečnost lidských zdrojů,
- f) řízení kontinuity činností,
- g) řízení přístupu,
- h) řízení identit a jejich oprávnění,
- i) detekce a zaznamenávání kybernetických bezpečnostních událostí,
- j) řešení kybernetických bezpečnostních incidentů,
- k) bezpečnost komunikačních sítí,
- l) aplikační bezpečnost a
- m) kryptografické algoritmy.

# Kroky po účinnosti nZoKB

Tento harmonogram ilustruje obecný postup implementace požadavků nového zákona o kybernetické bezpečnosti (nZoKB) pro oba režimy regulace (nižší i vyšší), při respektování rozdílného rozsahu bezpečnostních opatření.



# Metodický pokyn k aplikaci § 5b zákona č. 365/2000 Sb., o informačních systémech veřejné správy

## Preambule

Digitální a informační agentura vydává na základě § 4 odst. 1 písm. c) zákona č. 365/2000 Sb., o informačních systémech veřejné správy (dále také „Zákon“) tento metodický pokyn pro výkon odborných činností spojených s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy.

Účelem metodického pokynu je výklad § 5b Zákona, pokud jde o okamžik, kdy je nutné jej začít plnit.

## Problematika

Ustanovení § 5b Zákona, ve znění účinném od 1. listopadu 2026, zní:

### § 5b

*„Správci informačních systémů veřejné správy, kteří nejsou poskytovateli regulované služby podle zákona o kybernetické bezpečnosti, jsou povinni na jimi spravované informační systémy veřejné správy zavádět bezpečnostní opatření pro poskytovatele regulované služby v režimu nižších povinností podle § 8, 13 a 14 zákona o kybernetické bezpečnosti, a to přiměřeně s ohledem na možné dopady narušení důvěrnosti, integrity a dostupnosti konkrétního informačního systému veřejné správy na činnost jeho správce a jeho schopnost poskytovat své služby občanům, a dále vhodnost a proveditelnost těchto opatření.“*

## Pokyn

**Správce informačního systému veřejné správy je povinen začít plnit povinnosti podle § 5b Zákona do 1 roku ode dne, kdy se stal správcem informačního systému veřejné správy, nejdříve však do 1 roku ode dne nabytí účinnosti § 5b Zákona, tj. do 1. listopadu 2026.**

[https://www.dia.gov.cz/media/3158/download/Metodicky\\_pokyn\\_k\\_5b\\_zoisvs-FINAL%283967109514%29.pdf](https://www.dia.gov.cz/media/3158/download/Metodicky_pokyn_k_5b_zoisvs-FINAL%283967109514%29.pdf)

### Kontrola dodržování povinností orgánů veřejné správy

**3) Realizace programů** obsahujících **pořízení nebo architektonické změny určených\* informačních systémů**, investičních záměrů akcí pořízení nebo architektonických změn určených informačních systémů anebo projektů určených informačních systémů nebo jejich architektonických změn **bez souhlasného vyjádření Agentury nebo** souhlasného rozhodnutí **vlády**, jsou-li vyžadovány, se považuje za **porušení rozpočtové kázně**.

\* *určeným informačním systémem je informační systém veřejné správy, který:*

- 1. využívá služby referenčního rozhraní nebo poskytuje služby referenčnímu rozhraní,*
- 2. má vazby na informační systém veřejné správy podle bodu 1, nebo*
- 3. je určený k poskytování služby informačního systému veřejné správy fyzickým nebo právnickým osobám s předpokládaným počtem uživatelů, kteří využívají přístup se zaručenou identitou, alespoň 5000 ročně.*

# § 11 v. č. 360/2023 Sb., o dlouhodobém řízení ISVS

## Struktura provozní dokumentace

- (1) Provozní dokumentaci každé etapy životního cyklu informačního systému tvoří sady dokumentací
- a) plánování vytvoření a rozvoje informačního systému,
  - b) zadání a smluv pro vytvoření a rozvoj informačního systému,
  - c) stavu informačního systému při uvedení do produkčního provozu po jeho vytvoření nebo rozvoji,
  - d) plánu a zajišťování provozu,
  - e) změn informačního systému a
  - f) hodnocení informačního systému, včetně hodnocení ekonomické výhodnosti.

...

- (3) Orgán veřejné správy zveřejňuje sady dokumentací podle odstavce 1 **způsobem umožňujícím dálkový přístup**; ...

# § 12 v. č. 360/2023 Sb., o dlouhodobém řízení ISVS

## Náležitosti provozní dokumentace

(1) Provozní dokumentace obsahuje

- a) charakteristiku informačního systému,
- b) popis architektury informačního systému,
- c) podrobný popis informačního systému,
- d) bezpečnostní dokumentaci,**
- e) provozní řád,
- f) postupy a procesy související s provozem informačního systému,
- g) protokoly související s provozem informačního systému a
- h) smluvní a licenční dokumentaci.



# § 12 v. č. 360/2023 Sb., o dlouhodobém řízení ISVS

## Náležitosti provozní dokumentace

- (5) Orgán veřejné správy, kterému **nejsou** uloženy povinnosti v oblasti kybernetické **bezpečnosti** podle zákona upravujícího kybernetickou bezpečnost, **stanovuje** v bezpečnostní dokumentaci alespoň **postupy pro**
- a) **hodnocení** dopadů narušení **dostupnosti**, **důvěrnosti** a **integrity** informací v informačním systému,
  - b) způsob řešení a **reakce na bezpečnostní události** a **bezpečnostní incidenty**, **sběr** a **vyhodnocování** kybernetických bezpečnostních událostí a incidentů,
  - c) zajištění provozu informačních systémů a **bezpečnosti informací** v informačních systémech,
  - d) **rozvoj bezpečnostního povědomí** a způsob jeho kontroly,
  - e) zajištění **bezpečnosti komunikační sítě** a
  - f) zajištění **řízení kontinuity činnosti**.





# ISVS v cloudu



KATEDRA  
INFORMAČNÍCH  
TECHNOLOGIÍ  
PEF ČZU V PRAZE

## § 6l zákona 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

→ po novele zákonem č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

### Základní pravidla využívání cloud computingu orgánem veřejné správy

(3) Orgán veřejné správy využívá cloud computing poskytovaný poskytovatelem cloud computingu na základě písemné smlouvy o poskytování cloud computingu orgánu veřejné správy. **Orgán veřejné správy je povinen před uzavřením smlouvy s poskytovatelem cloud computingu zařadit informační systém veřejné správy nebo jeho část, k zajištění jehož provozu má být cloud computing využíván, do bezpečnostní úrovně s ohledem na povahu dotčeného informačního systému veřejné správy podle prováděcího právního předpisu.** Orgán veřejné správy je dále povinen zajišťovat, že budou **po celou dobu využívání služeb cloud computingu dodržována bezpečnostní pravidla.**

## § 12 zákona 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

→ po novele zákonem č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

### Zmocňovací ustanovení

(2) Národní úřad pro kybernetickou a informační bezpečnost stanoví vyhláškou

- požadavky na zajištění základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6m odst. 1 písm. a) a § 6n písm. b),
- seznam certifikací a auditů pro oblast ochrany důvěrnosti, integrity a dostupnosti informací podle § 6q odst. 5 písm. c), § 6t odst. 6 písm. b) a § 6t odst. 7 písm. c), doklady o jejich splnění a intervaly pro předkládání těchto dokladů podle § 6y odst. 2,
- požadavky na strukturu a náležitosti zprávy o provedení penetračního testu podle § 6t odst. 6 písm. d) a § 6t odst. 7 písm. e) a intervaly pro její předkládání,
- požadavky na náležitosti auditní zprávy osvědčující existenci plánu zajištění kontinuity provozu nabízeného cloud computingu a plánu na obnovu poskytování nabízeného cloud computingu po havárii podle § 6t odst. 6 písm. e) a § 6t odst. 7 písm. f),

## § 6n zákona 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

→ po novele zákonem č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

### Požadavky na cloud computing využívaný orgánem veřejné správy

Orgán veřejné správy může **využívat** a poskytovatel cloud computingu může orgánu veřejné správy nebo poskytovateli státního cloud computingu poskytovat **pouze cloud computing,**

- který umožňuje splnění požadavků kladených na informační systém veřejné správy **informační koncepcí České republiky,**
- který umožňuje dosažení alespoň základní úrovně ochrany důvěrnosti, integrity a dostupnosti **informací** orgánu veřejné správy,
- který umožňuje orgánu veřejné správy **zajistit dodržování bezpečnostních pravidel stanovených prováděcím právním předpisem,**
- jehož **bezpečnostní úroveň je stejná nebo vyšší** než bezpečnostní úroveň informačního systému veřejné správy nebo jeho části, k zajištění jehož provozu je využíván,

## § 12 zákona 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

→ po novele zákonem č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

### Zmocňovací ustanovení

(2) Národní úřad pro kybernetickou a informační bezpečnost stanoví vyhláškou

- požadavky na strukturu a náležitosti dokladu o zhodnocení zdrojů rizik podle § 6t odst. 6 písm. f) a § 6t odst. 7 písm. g),
- požadavky na strukturu a náležitosti podkladů k ověření splnění požadavku na zajištění **důvěrnosti, integrity a dostupnosti informací** podle § 6t odst. 6 písm. g) a § 6t odst. 7 písm. h),
- bezpečnostní úrovně informačních systémů veřejné správy,
- obsah a rozsah bezpečnostních pravidel** pro orgány veřejné správy využívající služeb cloud computingu podle § 6l odst. 3.

*Jdeme do hloubky...*

*Toto téma a mnoho dalších bude detailně  
řešeno v rámci specializovaného semináře  
4. června 2026.*



KATEDRA  
INFORMAČNÍCH  
TECHNOLOGIÍ  
PEF ČZU V PRAZE





# Národní architektura veřejné správy ČR jako zdroj pravidel a povinností v oblasti správy a rozvoje IT a ISVS

# Informační koncepce ČR / Informační koncepce OVS

## Zákonná povinnost:

- **Každý orgán veřejné správy (OVS) – tedy i každá obec** – musí mít zpracovanou a **vydanou Informační koncepci** svého úřadu (IK OVS) podle ZoISVS.

## Obsah IK OVS:

- Stanovuje dlouhodobé **cíle úřadu v oblasti řízení a rozvoje ICT**, zejména **řízení kvality a bezpečnosti spravovaných systémů**.
- Vymezuje **zásady pro pořizování, vytváření a provozování ISVS**.

## Informační koncepce ČR (IK ČR):

- Vládou schválený strategický dokument (usnesení č. 629/2018) definující celostátní vize, cíle a principy digitalizace veřejné správy.
- Představuje rámec eGovernmentu ČR, ke kterému se musí přihlásit všechny úřady.

# Informační koncepce ČR / Informační koncepce OVS

## Soulad IK ČR a IK OVS:

- Každá **IK OVS musí vycházet z IK ČR** a být s ní v souladu – pro jednotlivé OVS platí povinnost uvést svou koncepci **do souladu s cíli, principy a zásadami IK ČR**.
- **Lokální ICT strategie obce** tedy **navazuje na národní koncepci** a podporuje naplnění jejích cílů.

## Národní architektonický plán (NAP):

- Klíčová **příloha IK ČR** – jedná se o soubor referenčních modelů a jednotných architektonických pravidel eGovernmentu.
- Vydává jej a průběžně aktualizuje Odbor hlavního architekta DIA jako navazující dokument k IK ČR
- **IK ČR spolu s NAP stanovují závazné principy a standardy**, které musí orgány veřejné správy respektovat při budování či **pořizování svých informačních systémů**  
*(NAP například popisuje sdílené služby, datové integrace, bezpečnostní standardy apod., čímž usměrňuje rozvoj ICT ve všech úřadech v souladu s národní architekturou.)*

# Web odboru Hlavního architekta eGovernmentu (OHA)

## Národní architektonický plán

Národní architektonický plán je přílohou Informační koncepce ČR dle zákona 365/2000 Sb. a toto je základní rozcestník na jeho jednotlivé kapitoly/stránky.

### Struktura NAP

1. Kapitola Úvod
2. Kapitola Architektonická vize eGovernmentu ČR
3. Kapitola Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury
4. Kapitola Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR
5. Kapitola Způsoby využívání sdílených služeb, funkčních celků a tematických oblastí úřady
6. Kapitola Modely NAP v centrálním úložišti a v OVS

Můžete se podívat i na [Náhled na celkový Národní architektonický plán složený ze všech kapitol](#)



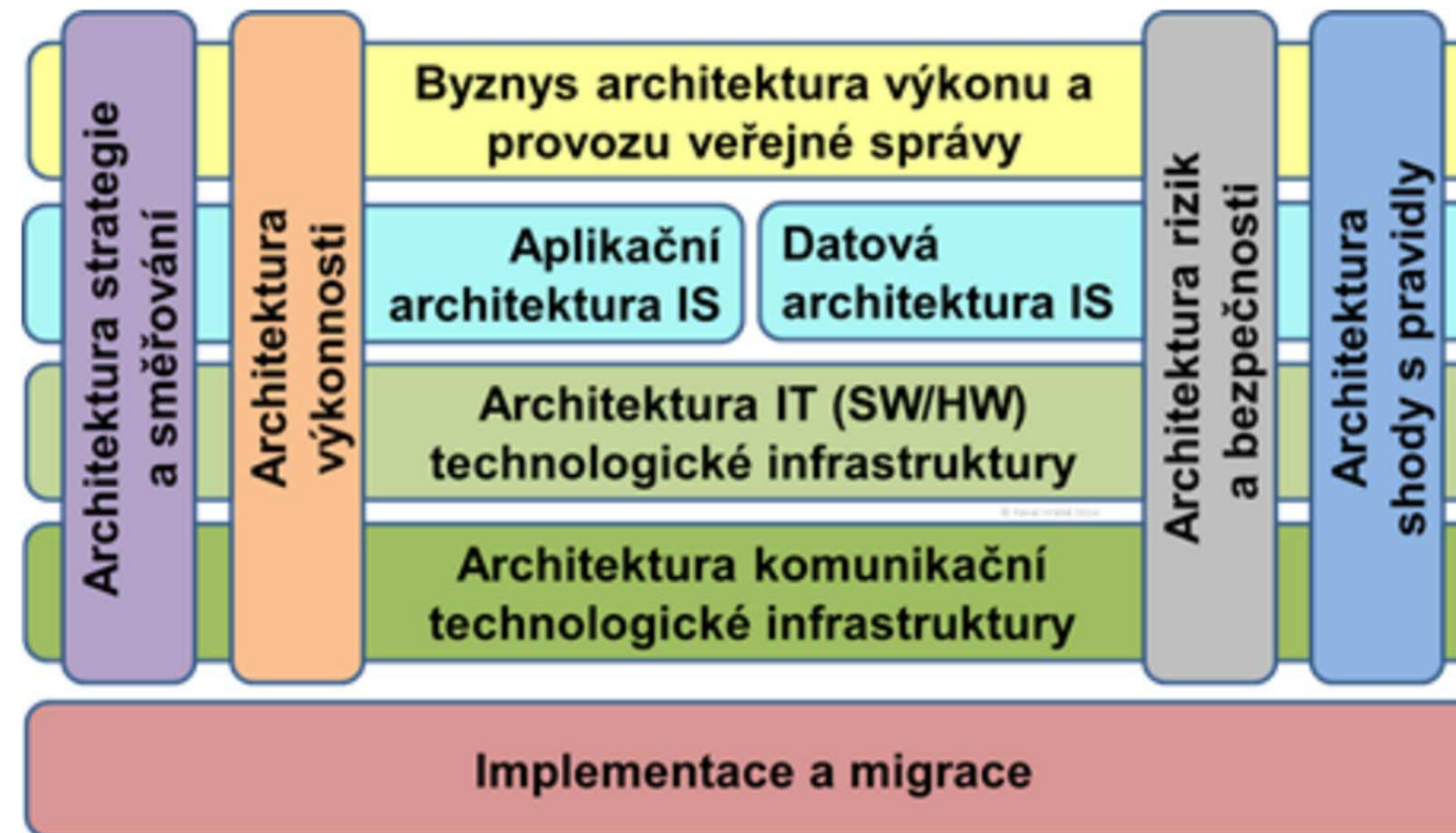
# Web odboru Hlavního architekta eGovernmentu (OHA)

## Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury



Tato kapitola popisuje architekturu úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu. Jde o jiný přístup k popisu požadavků na využívání systémů a služeb eGovernmentu než v části [Způsoby využívání sdílených služeb, funkčních celků a tematických oblastí jednotlivých úřadů](#), kde se požadavky popisují v celé šíři (v celé architektuře) sdílené služby, funkčního celky či tematické oblasti.

Skladba této kapitoly odpovídá doménám národní architektury





**Bylo záměrem, aby i malé obce plnily tolik povinností v oblasti správy ISVS a kybernetické bezpečnosti?**

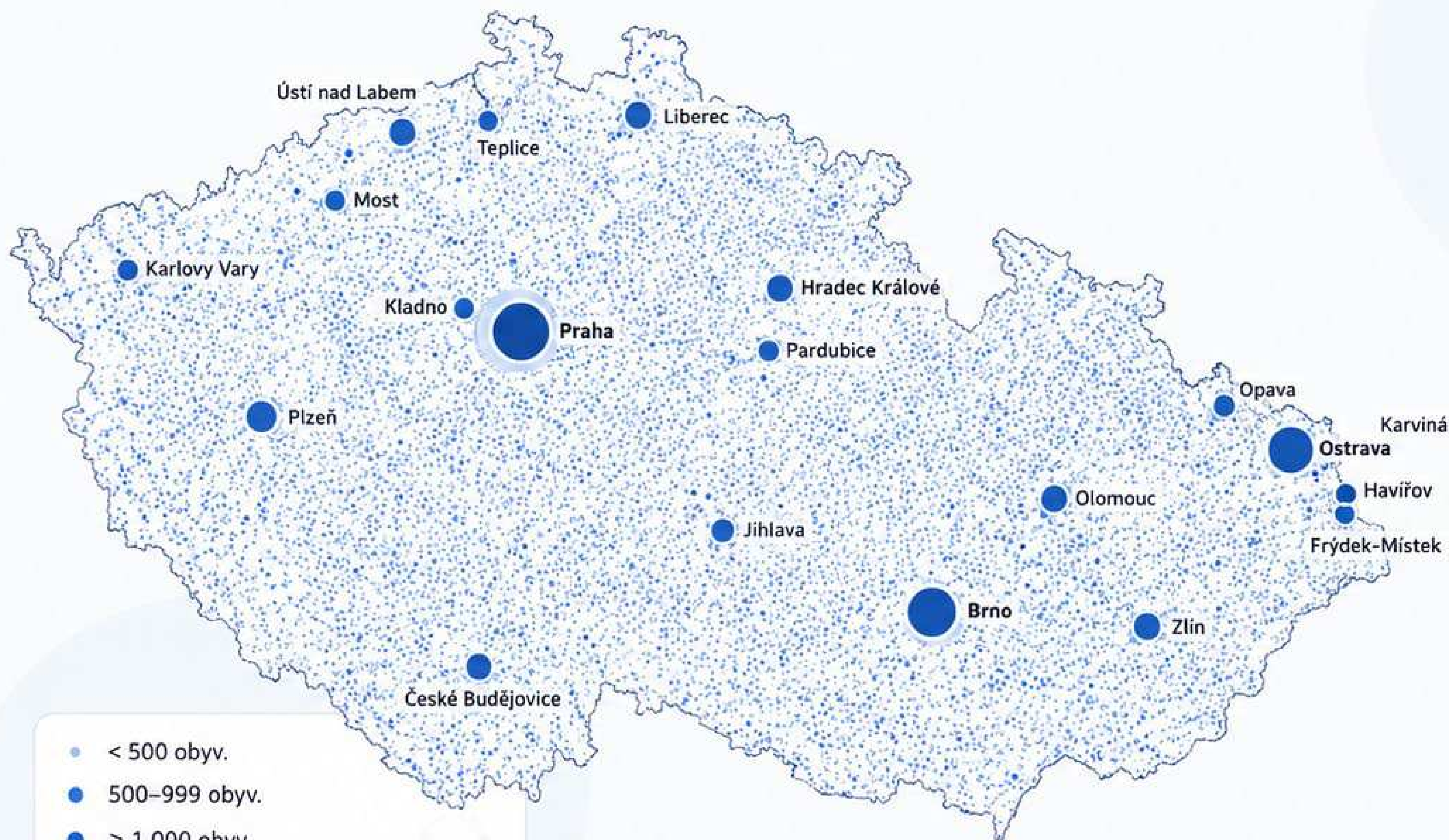


KATEDRA  
INFORMAČNÍCH  
TECHNOLOGIÍ  
PEF ČZU V PRAZE



# Roztříštěné územní uspořádání ČR

Skutečné bodové polohy obcí; velikost zvýrazněných piktogramů odpovídá počtu obyvatel



## Struktura obcí

Ověřeno z dat ČSÚ k 1. 1. 2025



**6 258**

obcí



**453**

medián obyvatel



**75,5 %**

obcí < 1 000  
obyvatel

4 723 obcí



**53,5 %**

obcí < 500  
obyvatel

7,6 % populace

### Poznámka k mapě

Velikost zvýrazněných piktogramů je škálována podle počtu obyvatel. Výpočty vycházejí z dat ČSÚ k 1. 1. 2025.

Mapa zobrazuje skutečný tvar ČR a bodové umístění obcí v přibližně reálné poloze.

# Výzvy a omezení pro malé obce v ICT

## Náročnost pro malé obce:

- Požadavky dlouhodobého plánování a řízení ICT podle IK ČR jsou pro **malé obce obtížně splnitelné** – vysoké nároky na odborné znalosti, kapacity personálu i finanční zdroje.
- Malé obecní úřady mívají jen omezený IT aparát.

## Omezené možnosti vývoje:

- **Malé obce nemají zdroje pro vývoj a rozvoj vlastních IS.**
- Většinou pořizují hotová řešení od externích dodavatelů (komerční software pro agendy, spisovou službu, webové portály apod.).



# Výzvy a omezení pro malé obce v ICT

## Povinnosti při pořízení IS:

- Nákup systému „na klíč“ obec nezbavuje odpovědností.
- Každý ISVS musí mít určeného věcného a technického správce (garanta) a také provozovatele (i externě).
- Obec odpovídá za **bezpečný provoz** systému (mj. splnění požadavků kybernetické bezpečnosti) a za **soulad s legislativou** (např. správa dat, archivace).
- K tomu patří i průběžná **aktualizace vlastní Informační koncepce** a plnění podmínek dlouhodobého řízení ICT.



# Výzvy a omezení pro malé obce v ICT

## Nutnost interních kompetencí:

- Národní koncepce – důraz na udržení **interních ICT kompetencí** v každém úřadu
- Vlastní odborné pozice pro klíčové role (ICT architekt, správce systému, projektový manažer apod.)
- **Snaha o nezávislost na dodavatelích** a o kontinuitu ICT
- Malé obce – obtížně zajistitelné interní kapacity, výrazná zátěž

## Využívání sdílené podpory:

- **sdílené služby** a sdílené informační systémy (např. prostřednictvím **ORP** nebo krajů)
- cloudové eGovernment služby (splní povinné standardy ICT)

# Národní architektonický plán – role KÚ a ORP

**Specifická pravidla pro architekturu úřadů** - Pravidla pro architekturu dle velikosti a možností úřadů

**Pro obce 1. a 2. typu má vize architektury veřejné správy následující podobu:**

Architekturu IT úřadu obce 1. a 2. typu (do určité velikosti, viz níže) tvoří pouze koncová zařízení pro uživatele, síťovou infrastrukturu jim jako sdílenou poskytuje kraj, aplikační služby pro státní správu v přenesené působnosti poskytnou ohlašovatelé agend a aplikační služby pro samosprávnou působnost poskytne vyšší stupeň územní samosprávy (ORP, kraj) jako sdílenou službu.

Pro oblast samosprávy tak vychází koncepce z následujících principů:

1. NAP je závazný pro všechny subjekty samosprávy, které mají více než 10 zařízení.
2. Informační systémy pro činnosti a agendy v přenesené působnosti přebírají v plném rozsahu od centrálních úřadů. Samosprávné činnosti si každý územněsprávní celek zajišťuje sám.
3. Subjekty s méně než 10 zařízeními si pořizují pouze uživatelský HW a SW, tj. tato koncová zařízení, SW produkty pro výkon veřejné správy jim jako službu zajišťují subjekty, v jejichž správním obvodu leží.

# Národní architektonický plán – role KÚ a ORP

Specifická pravidla pro architekturu úřadů - Pravidla pro architekturu dle velikosti a možností úřadů

- Zákon č. 129/2000 Sb., o krajích, výslovně upravuje některé povinnosti krajů v oblasti ICT/ISVS.
- Klíčový je § 67 odst. 1, který stanoví působnost krajského úřadu v přenesené působnosti.
- Krajský úřad mj. **„poskytuje odbornou a metodickou pomoc obcím“** a dále **„zabezpečuje koordinaci výstavby a provozu informačního systému kompatibilního s informačními systémy veřejné správy“**.

# Rozpor mezi architekturou a provozní realitou

NAP směřuje k sdíleným službám; praxe obcí je často odlišná.



## Logika NAP

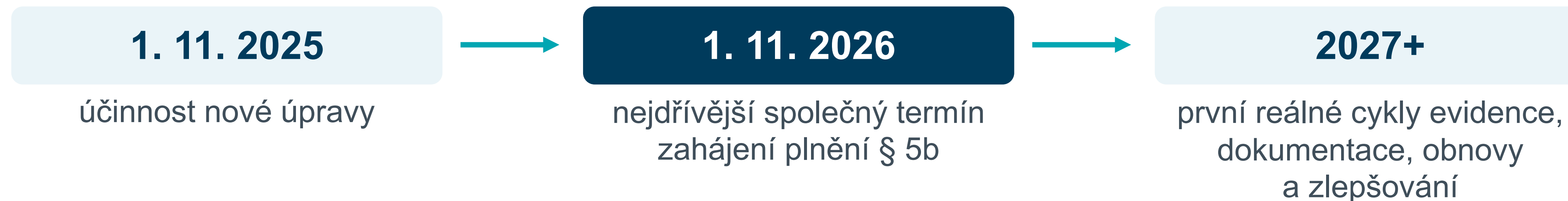
- malé obce: zejména koncová zařízení
- síťové a aplikační služby sdíleně
- ORP a kraje jako servisní uzly

## Provozní realita

- lokální i hostované systémy
- různá smluvní ujednání
- nejasná role správce / provozovatele



# Shrnutí nejdůležitějších informací



- 1) I malé obce mají povinnosti podle nZoKB, pokud („jelikož“) spravují ISVS.**
- 2) Malé obce (do 10 zařízení) nemají budovat vlastní ICT infrastrukturu.**
- 3) Bezpečnost je jen jedna a týká se všech, bez ohledu na zákony. Řešit bezpečnost je pudem sebezáchovy, ne dodržováním právních norem.**

Nečekat na konec přechodného období, první kroky jsou evidenční a organizační, nikoli investiční.



## Problém není bezpečnost, ale měřítko

Co je běžná provozní agenda pro velký úřad, může být pro malou obec neproveditelný balík dokumentů.

### Legitimní minimum

- Jaké systémy obec používá
- Jaká data se zpracovávají
- Kdo má přístup
- Kdo obnoví službu po incidentu

### Riziko formalismu

- Nic neříkající analýzy
- Dokumenty bez vazby na provoz
- Nedostupné odborné kapacity
- Náklady bez reálného zvýšení odolnosti

Řešení: jednoduché minimum + sdílená infrastruktura + nástrojová evidence.

## Důvěrnost, integrita, dostupnost: dopad na službu občanům

Bezpečnost ISVS není „IT navíc“ — přímo souvisí s výkonem veřejné správy.

### DŮVĚRNOST

Kdo vidí osobní údaje,  
spisy, rozhodnutí a účetní  
data?

### INTEGRITA

Jsou údaje správné,  
úplné a průkazné?

### DOSTUPNOST

Funguje spisová služba,  
účetnictví, portál,  
podatelna?

Přiměřené řízení začíná otázkou:

„Co se stane, když systém přestane fungovat nebo mu nemohu věřit?“

## Role musí být čisté: správce ≠ provozovatel ≠ dodavatel

Největší praktický problém bývá nejasnost, kdo odpovídá za co.

Role	Praktická otázka	Co má obec doložit
Správce ISVS	Kdo odpovídá za systém a službu?	evidence, vlastník, dopad na službu
Provozovatel	Kdo zajišťuje technický provoz?	smlouva, SLA, kontakty, zálohy
Uživatel	Kdo do systému vstupuje?	účty, oprávnění, pravidelná revize
Dodavatel	Kdo drží know-how a data?	incidenty, subdodavatelé, exit, audit

První úkol není nakoupit technologii. První úkol je vyčistit odpovědnosti.

## Bezpečnost zabudovaná do služeb, ne do šanonů

Cílový model má obcím odlehčit, nikoli vyrobit další stovky lokálních metodik.



### ORP / kraj

servisní uzel  
společné smlouvy  
bezpečný hosting  
zálohy a monitoring

### DIA / NÚKIB

metodické minimum  
vzory dokumentů  
podpora nižšího  
režimu  
praktické manuály

### Obec

evidence systémů  
role a kontakty  
řízení přístupů  
plán obnovy

## Systémová doporučení

Co musí vzniknout, aby § 5b nezůstal jen formální povinností.

- 1 Čistá evidence rolí** jednoduchý postup oprav v AIS RPP a ve smluvní dokumentaci
- 2 Sdílené balíčky služeb** správa stanic, identita, zálohy, hosting, spisová služba
- 3 Metodické minimum** vzor evidence ISVS, rizik, provozní dokumentace a obnovy
- 4 Nástrojová podpora** společná evidence, úkoly, důkazy plnění, kontrolní přehledy

Bez těchto čtyř prvků vznikne spíše compliance papír než skutečná odolnost.

## Závěr: odpovědnost ano, izolovaná implementace ne

Bezpečnost malých obcí musí být provozovatelná, sdílená a doložitelná.

**Malé obce nepotřebují výjimku z bezpečnosti.  
Potřebují bezpečnost, která je provozovatelná.**

- ✓ § 5b ZoISVS rozšiřuje dopad i na správce ISVS mimo přímou regulaci ZKB.
- ✓ Přiměřenost musí znamenat kratší, funkční a udržovatelné postupy.
- ✓ Cesta vede přes ORP/kraje, sdílené služby a nástroje řízení bezpečnosti.

## Právní mapa pro následné čtení

PODKLAD

Kontext, do kterého se problematika obcí jako správců ISVS skládá.

### ZKB

zákon č. 264/2025 Sb.  
vyhláška č. 408/2025 Sb.  
vyhláška č. 410/2025 Sb.  
vyhláška č. 334/2025 Sb.

### ZoISVS

zákon č. 365/2000 Sb.  
§ 5b – správci ISVS  
§ 6I – cloud computing  
vyhlášky č. 411/2025 a 412/2025 Sb.

### Dlouhodobé řízení

vyhláška č. 360/2023 Sb.  
informační koncepce OVS  
provozní dokumentace  
bezpečnostní dokumentace

## Výsledek, který chceme

Cílem není vyrobit složku dokumentů. Cílem je vědět, co máme udělat, když systém selže.

### Vím, co mám

evidence ISVS, dat, dodavatelů  
a kritických služeb

### Vím, kdo odpovídá

garant, provozovatel, dodavatel,  
kontakty a zastupitelnost

### Vím, jak obnovím

zálohy, postup obnovy, incidentní  
kontakt a ověřený test





# Vaše dotazy ?

## Odborný seminář na toto téma:

- 4. června 2026
- Hotel Akademie Naháč



KATEDRA  
INFORMAČNÍCH  
TECHNOLOGIÍ  
PEF ČZU V PRAZE

Ing. Miroslav Pavelka, pavelka@pef.czu.cz

# Zdroje a doporučené materiály

PODKLAD

Pro následné čtení a praktickou implementaci.

Pavelka, M.; Jarolímek, J.: Nové povinnosti tisíců obcí v oblasti bezpečnosti po novele ZoISVS. Sborník ISSS 2026.  
DIA: Metodický pokyn k aplikaci § 5b zákona č. 365/2000 Sb.  
NÚKIB: Manuál pro poskytovatele regulovaných služeb v režimu nižších povinností; podpůrné materiály pro obce.  
Vyhláška č. 410/2025 Sb. — bezpečnostní opatření v režimu nižších povinností.  
Vyhláška č. 360/2023 Sb. — dlouhodobé řízení ISVS; Národní architektonický plán.

Podklady pro právní a metodický kontext prezentace.

Pavelka, M.; Jarolímek, J.: Nové povinnosti tisíců obcí v oblasti bezpečnosti po novele ZoISVS. Sborník ISSS 2026.  
Zákon č. 264/2025 Sb., o kybernetické bezpečnosti; zákon č. 265/2025 Sb.; zákon č. 365/2000 Sb.  
Vyhlášky č. 408/2025 Sb., 410/2025 Sb., 411/2025 Sb., 412/2025 Sb.; vyhláška č. 360/2023 Sb.  
DIA: Metodický pokyn k aplikaci § 5b ZoISVS. NÚKIB: podpůrné materiály a manuál pro nižší režim.  
AIS RPP Působnostní / Katalog ISVS.  
Národní architektonický plán a [archi.gov.cz](http://archi.gov.cz).

