

# Nový zákon o kybernetické bezpečnosti

Aktuální vývoj – obce s rozšířenou působností a věda a výzkum



2. prosince 2024

TLP: CLEAR

Klasifikace informací: Neveřejné

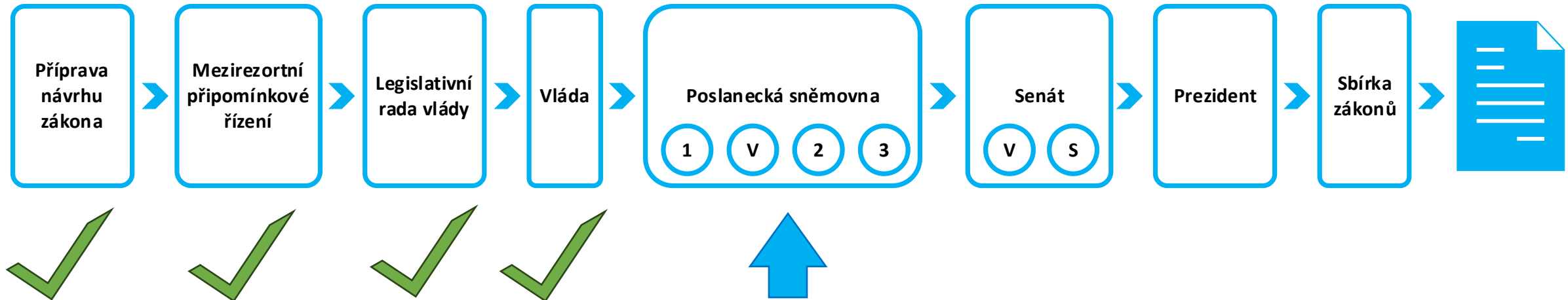
Daniela Procházková  
Vedoucí oddělení regulace veřejného sektoru



## **UPOZORNĚNÍ:**

Transpozice NIS2 do českého právního řádu není finalizována.  
Informace obsažené v této prezentaci se mohou změnit v rámci legislativního procesu.

<https://portal.nukib.gov.cz/>



**Vláda předložila Poslanecké sněmovně návrh zákona 25. července 2024.**

Návrh zákona rozeslán poslancům jako **sněmovní tisk 759/0**.

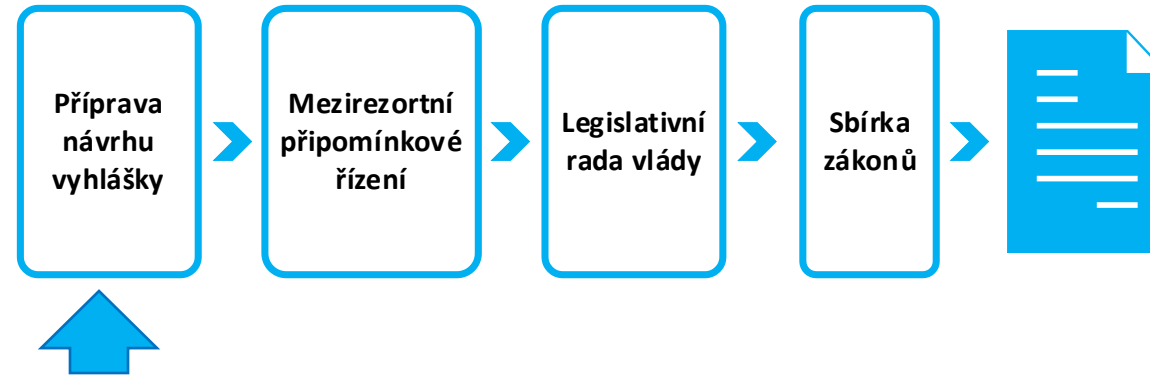
Předsedkyně sněmovny **projednání zákona doporučila**, určila **zpravodaje** a navrhla přikázat návrh zákona k projednání **Výboru pro bezpečnost** (později doplněn také Hospodářský výbor a výbor pro obranu).

**Projednávání tisku proběhlo v prvním čtení na 112. schůzi Poslanecké sněmovny.**

**Očekávaná účinnost 1.7.2025**



[Sněmovní tisk 759 \(psp.cz\)](https://psp.cz)



S návrhem zákona se připravují také teze jeho vyhlášek. Ty čeká samostatný legislativní proces.

Legislativní proces vyhlášek bude zahájen potom, co zákon projde druhým čtením a bude jasné, že jeho podoba je více méně finální – leden 2025.

1. Vyhláška o regulovaných službách
2. Vyhláška o bezpečnostních opatřeních pro vyšší režim
3. Vyhláška o bezpečnostních opatřeních pro nižší režim
4. Portálová vyhláška
5. Vyhláška o nepominutelných funkcích (BDŘ)
6. Vyhláška o bezpečnostních úrovních (cloud)
7. Vyhláška o bezpečnostních pravidlech (cloud)



## 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

13/28 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 protioopatření

Vydá a doručí NÚKIB

Reaktivní protioopatření/varování

Lhůty dané protioopatřením



## 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

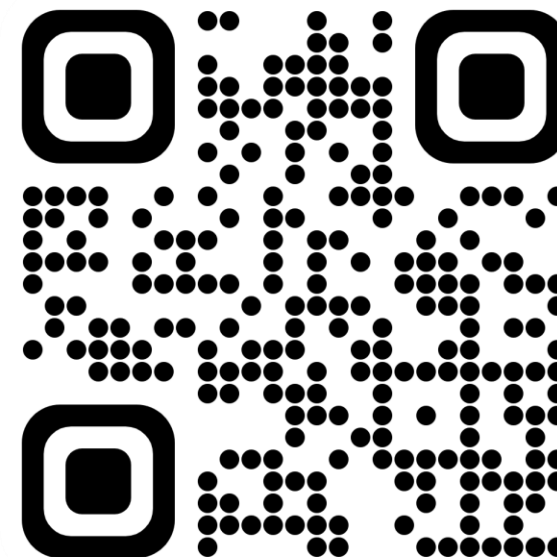


## Portál NÚKIB

<https://portal.nukib.gov.cz/>

Hlavní komunikační platforma týkající se nového ZKB

- Podpůrné materiály
- Aktuality
- Otázky & odpovědi





## 1. Veřejná správa

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby a jeho režim pro tuto službu
1.1. Výkon svěřených pravomocí	<p>Orgán nebo osoba je</p> <p>I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je</p> <ul style="list-style-type: none"><li>a) ústředním orgánem státní správy,</li><li>b) jiným správním úřadem s celostátní působností neuvedeným v písm. a), a to včetně ústředí a generálního ředitelství územně <u>dekoncentrovaných</u> (specializovaných) orgánů státní správy,</li><li>c) Kanceláří prezidenta republiky,</li><li>d) Kanceláří Senátu,</li><li>e) Kanceláří Poslanecké sněmovny,</li><li>f) Českou národní bankou,</li><li>g) Policejním prezidiem,</li><li>h) útvarem policie s celostátní působností,</li><li>i) Generální inspekcí bezpečnostních sborů</li><li>j) Generálním ředitelstvím hasičského záchranného sboru,</li><li>k) krajským ředitelstvím hasičského záchranného sboru,</li><li>l) Kanceláří Veřejného ochránce práv,</li><li>m) Nejvyšším kontrolním úřadem,</li><li>n) Úřadem pro zastupování státu ve věcech majetkových</li><li>o) Správou úložišť radioaktivních odpadů,</li><li>p) orgánem soudní moci,</li><li>q) státním zastupitelstvím,</li><li>r) zdravotní pojišťovnou,</li><li>s) krajem, nebo</li><li>t) hlavním městem Praha.</li></ul> <p>II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je</p> <ul style="list-style-type: none"><li>a) územně <u>dekoncentrovaným</u> (specializovaným) orgánem státní správy,</li><li>b) profesní komorou<sup>2</sup>,</li><li>c) vysokou školou,</li><li>d) Akademií věd České republiky, nebo</li><li>e) obcí s rozšířenou působností,</li><li>f) městským obvodem nebo městskou částí, která vykonává rozšířenou působnost.</li></ul>



II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je

- a) územně dekoncentrovaným (specializovaným) orgánem státní správy,
- b) profesní komorou<sup>2</sup>,
- c) vysokou školou,
- d) Akademií věd České republiky nebo
- e) obcí s rozšířenou působností,
- f) městským obvodem nebo městskou částí, která vykonává rozšířenou působnost.



## 1. Veřejná správa

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby a jeho režim pro tuto službu
1.1. Výkon svěřených pravomocí	Orgán nebo osoba je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je a) ústředním orgánem státní správy, b) jiným správním úřadem s celostátní působností neuvedeným v písm. a), a to včetně ústředí a generálního ředitelství územně <u>dekoncentrovaných</u> (specializovaných) orgánů státní správy, c) Kanceláří prezidenta republiky, d) Kanceláří Senátu, e) Kanceláří Poslanecké sněmovny, f) Českou národní bankou,



## 1. Veřejná správa

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby a jeho režim pro tuto službu
1.1. Výkon svěřených pravomocí	<p>Orgán nebo osoba je</p> <p>I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je</p> <ul style="list-style-type: none"><li>a) ústředním orgánem státní správy,</li><li>b) jiným správním úřadem s celostátní působností neuvedeným v písm. a), a to včetně ústředí a generálního ředitelství územně <u>dekoncentrovaných</u> (specializovaných) orgánů státní správy,</li><li>c) Kanceláří prezidenta republiky,</li><li>d) Kanceláří Senátu,</li><li>e) Kanceláří Poslanecké sněmovny,</li><li>f) Českou národní bankou,</li><li>g) Policejním prezidiem,</li><li>h) útvarem policie s celostátní působností,</li><li>i) Generální inspekcí bezpečnostních sborů</li><li>j) Generálním ředitelstvím hasičského záchranného sboru,</li><li>k) krajským ředitelstvím hasičského záchranného sboru,</li><li>l) Kanceláří Veřejného ochránce práv,</li><li>m) Nejvyšším kontrolním úřadem,</li><li>n) Úřadem pro zastupování státu ve věcech majetkových</li><li>o) Správou úložišť radioaktivních odpadů,</li><li>p) orgánem soudní moci,</li><li>q) státním zastupitelstvím,</li><li>r) zdravotní pojišťovnou,</li><li>s) krajem, nebo</li><li>t) hlavním městem Praha.</li></ul> <p>II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je</p> <ul style="list-style-type: none"><li>a) územně <u>dekoncentrovaným</u> (specializovaným) orgánem státní správy,</li><li>b) profesní komorou<sup>2</sup>,</li><li>c) vysokou školou,</li><li>d) Akademií věd České republiky, nebo</li><li>e) obcí s rozšířenou působností,</li><li>f) městským obvodem nebo městskou částí, která vykonává rozšířenou působnost.</li></ul>

## Obcí zřizované organizace:

- **Nespadají automaticky „protože obec“**
  - **Typicky tedy ne základní a mateřské školy či městské knihovny**
- Spadají jen ty zřizované organizace, které samy naplní kritéria v jiném odvětví
  - **Obce se ale k nim v rámci počítání velikosti podniků nepřiřítávají**
  - *Příklad: Do počtu zaměstnanců pro posouzení velikosti podniku např. vodárny, která je zřízena obcí, ale má samostatné IČO, se počet zaměstnanců obce nepřiřítává.*



## Přenesená působnost obcí

- Evidence obyvatel
- Matrika
- Vidimace a legalizace
- Poskytování informace
- Stavební a silniční správní úřad
- Dopravní agenda
- Životní prostředí
- Přestupky
- Místní poplatky
- Právo shromažďování
- Sociální agenda
- Krizové řízení

## Samostatná působnost obcí

- Správa vlastního majetku
- Místní referenda
- Vyřizování petic a stížností
- Poskytování dotací
- Odpadové hospodářství
- Poskytování informací
- Zřizování příspěvkových organizací a obecní policie
- Vydávání obecně závazných vyhlášek



Regulovaná služba	
Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
1. Výzkum a vývoj	<p>Veřejná výzkumná instituce<sup>[1]</sup>, výzkumná organizace podle přímo použitelného předpisu Evropské unie<sup>[2]</sup>, vysoká škola nebo výzkumná instituce dle § 2 této vyhlášky je</p> <p>I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že</p> <ol style="list-style-type: none"> <li>1. v posledních 5 kalendářních letech prováděla a alespoň 2 kalendářní roky citlivou výzkumnou činnost, nebo</li> <li>2. v posledních 5 kalendářních letech prováděla a alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU<sup>[3]</sup>:             <ol style="list-style-type: none"> <li>a. technologie pokročilých polovodičů,</li> <li>b. technologie umělé inteligence,</li> <li>c. kvantové technologie, nebo</li> <li>d. biotechnologie.</li> </ol> </li> </ol> <p>II. poskytovatelem regulované služby v režimu nižších povinností v případě, že v posledních 5 kalendářních letech prováděla a alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje dle doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU<sup>[4]</sup>:</p> <ol style="list-style-type: none"> <li>1. pokročilá konektivita, navigace a digitální technologie,</li> <li>2. technologie pokročilého snímání,</li> <li>3. vesmírné technologie a technologie pohonu,</li> <li>4. energetické technologie,</li> <li>5. robotika a autonomní systémy, nebo</li> <li>6. pokročilé materiály, výrobní a recyklační technologie.</li> </ol> <p>Výzkumná instituce podle § 2 této vyhlášky je poskytovatelem regulované služby v režimu nižších povinností v případě, že je velkým podnikem.</p>



Regulovaná služba	
Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
<b>1. Výzkum a vývoj</b>	<p>Veřejná výzkumná instituce<sup>[1]</sup>, výzkumná organizace podle přímo použitelného předpisu Evropské unie<sup>[2]</sup>, vysoká škola nebo <b>výzkumná instituce dle § 2 této vyhlášky</b> je</p> <p>I. poskytovatelem regulované služby v režimu <b>vyšších povinností</b> v případě, že</p> <ol style="list-style-type: none"><li>1. v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky <b>citlivou výzkumnou</b> činnost, nebo</li><li>2. v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU<sup>[3]</sup>:</li></ol> <ol style="list-style-type: none"><li>a. technologie pokročilých polovodičů,</li><li>b. technologie umělé inteligence,</li><li>c. kvantové technologie, nebo</li><li>d. biotechnologie.</li></ol> <p>II. poskytovatelem regulované služby v režimu nižších povinností v případě, že v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje dle doporučení Komise o</p>



Regulovaná služba	
Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
1. Výzkum a vývoj	<p>Veřejná výzkumná instituce<sup>[1]</sup>, výzkumná organizace podle přímo použitelného předpisu Evropské unie<sup>[2]</sup>, vysoká škola nebo výzkumná instituce dle § 2 této vyhlášky je</p> <p>I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že</p> <ol style="list-style-type: none"> <li>1. v posledních 5 kalendářních letech prováděla a alespoň 2 kalendářní roky citlivou výzkumnou činnost, nebo</li> <li>2. v posledních 5 kalendářních letech prováděla a alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU<sup>[3]</sup>: <ol style="list-style-type: none"> <li>a. technologie pokročilých polovodičů,</li> <li>b. technologie umělé inteligence,</li> <li>c. kvantové technologie, nebo</li> <li>d. biotechnologie.</li> </ol> </li> </ol> <p>II. poskytovatelem regulované služby v režimu nižších povinností v případě, že v posledních 5 kalendářních letech prováděla a alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje dle doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU<sup>[4]</sup>:</p> <ol style="list-style-type: none"> <li>1. pokročilá konektivita, navigace a digitální technologie,</li> <li>2. technologie pokročilého snímání,</li> <li>3. vesmírné technologie a technologie pohonu,</li> <li>4. energetické technologie,</li> <li>5. robotika a autonomní systémy, nebo</li> <li>6. pokročilé materiály, výrobní a recyklační technologie.</li> </ol> <p>Výzkumná instituce podle § 2 této vyhlášky je poskytovatelem regulované služby v režimu nižších povinností v případě, že je velkým podnikem.</p>

**Citlivá výzkumná činnost** = aplikovaný výzkum vojenského materiálu dle seznamu vojenského materiálu podle zákona o zahraničním obchodu s vojenským materiálem

**Výzkumná instituce podle § 2 vyhlášky** = výzkumná organizace dle NIS2 - orgán nebo osoba, jejímž hlavním cílem je provádět aplikovaný výzkum za účelem využití výsledků tohoto výzkumu pro komerční účely, který ovšem nezahrnuje vzdělávací instituce

**Výzkum a vývoj** = regulovaná služba – to stanovuje okruh aktiv, které by měl poskytovatel regulované služby evidovat a následně chránit



Regulovaná služba	
Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
1. Výzkum a vývoj	<p>Veřejná výzkumná instituce<sup>[1]</sup>, výzkumná organizace podle přímo použitelného předpisu Evropské unie<sup>[2]</sup>, vysoká škola nebo výzkumná instituce dle § 2 této vyhlášky je</p> <p>I. poskytovatelem regulované služby v režimu <b>vyšších</b> povinností v případě, že</p> <ol style="list-style-type: none"><li>1. v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky citlivou výzkumnou činnost, nebo</li><li>2. v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje <b>doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU</b> <sup>[3]</sup>:</li></ol> <ol style="list-style-type: none"><li>a. technologie pokročilých polovodičů,</li><li>b. technologie umělé inteligence,</li><li>c. kvantové technologie, nebo</li><li>d. biotechnologie.</li></ol> <p>II. poskytovatelem regulované služby v režimu nižších povinností v případě, že v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje dle doporučení Komise o</p>



Regulovaná služba	
Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
1. Výzkum a vývoj	<p>Veřejná výzkumná instituce<sup>[1]</sup>, výzkumná organizace podle přímo použitelného předpisu Evropské unie<sup>[2]</sup>, vysoká škola nebo výzkumná instituce dle § 2 této vyhlášky je</p> <p>I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že</p> <ol style="list-style-type: none"> <li>1. v posledních 5 kalendářních letech prováděla a alespoň 2 kalendářní roky citlivou výzkumnou činnost, nebo</li> <li>2. v posledních 5 kalendářních letech prováděla a alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU <sup>[3]</sup>:             <ol style="list-style-type: none"> <li>a. technologie pokročilých polovodičů,</li> <li>b. technologie umělé inteligence,</li> <li>c. kvantové technologie, nebo</li> <li>d. biotechnologie.</li> </ol> </li> </ol> <p>II. poskytovatelem regulované služby v režimu nižších povinností v případě, že v posledních 5 kalendářních letech prováděla a alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje dle doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU <sup>[4]</sup>:</p> <ol style="list-style-type: none"> <li>1. pokročilá konektivita, navigace a digitální technologie,</li> <li>2. technologie pokročilého snímání,</li> <li>3. vesmírné technologie a technologie pohonu,</li> <li>4. energetické technologie,</li> <li>5. robotika a autonomní systémy, nebo</li> <li>6. pokročilé materiály, výrobní a recyklační technologie.</li> </ol> <p>Výzkumná instituce podle § 2 této vyhlášky je poskytovatelem regulované služby v režimu nižších povinností v případě, že je velkým podnikem.</p>

**2 kalendářní roky za posledních 5 kalendářních let = v souvislosti s grantovou povahou fungování výzkumu – stabilizační podmínka**

**doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU = dokument převedený pro řízení rizik ve vědě a výzkumu do národní metodiky od MŠMT a AVČR; má být do budoucna převeden do podoby závazného legislativního aktu unie**

- a. technologie pokročilých polovodičů,**
- b. technologie umělé inteligence,**
- c. kvantové technologie, nebo**
- d. biotechnologie.**

= 4 odvětví, které doporučení Komise vydefinovalo jako nejvíce ohrožené z pohledu ochrany dat



Regulovaná služba	
Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
1. Výzkum a vývoj	<p>Veřejná výzkumná instituce<sup>[1]</sup>, výzkumná organizace podle přímo použitelného předpisu Evropské unie<sup>[2]</sup>, vysoká škola nebo výzkumná instituce dle § 2 této vyhlášky je</p> <p>I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že</p> <ol style="list-style-type: none"> <li>1. v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky citlivou výzkumnou činnost, nebo</li> <li>2. v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU <sup>[3]</sup>:             <ol style="list-style-type: none"> <li>a. technologie pokročilých polovodičů,</li> <li>b. technologie umělé inteligence,</li> <li>c. kvantové technologie, nebo</li> <li>d. biotechnologie.</li> </ol> </li> </ol> <p>II. poskytovatelem regulované služby v režimu nižších povinností v případě, že v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje dle doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU <sup>[4]</sup>:</p> <ol style="list-style-type: none"> <li>1. <b>pokročilá konektivita, navigace a digitální technologie,</b></li> <li>2. <b>technologie pokročilého snímání,</b></li> <li>3. <b>vesmírné technologie a technologie pohonu,</b></li> <li>4. <b>energetické technologie,</b></li> <li>5. <b>robotika a autonomní systémy, nebo</b></li> <li>6. <b>pokročilé materiály, výrobní a recyklační technologie.</b></li> </ol> <p>Výzkumná instituce podle § 2 této vyhlášky je poskytovatelem regulované služby v režimu nižších povinností v případě, že je <b>velkým podnikem</b>.</p>



## 1. Výzkum a vývoj

II. poskytovatelem regulované služby v režimu **nižších povinností** v případě, že v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje dle doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU [\[4\]](#):

1. **pokročilá konektivita, navigace a digitální technologie,**
2. **technologie pokročilého snímání,**
3. **vesmírné technologie a technologie pohonu,**
4. **energetické technologie,**
5. **robotika a autonomní systémy, nebo**
6. **pokročilé materiály, výrobní a recyklační technologie.**

Výzkumná instituce podle § 2 této vyhlášky je poskytovatelem regulované služby v režimu **nižších povinností** v případě, že je **velkým podnikem**.



Regulovaná služba	
Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
1. Výzkum a vývoj	<p>Veřejná výzkumná instituce<sup>[1]</sup>, výzkumná organizace podle přímo použitelného předpisu Evropské unie<sup>[2]</sup>, vysoká škola nebo výzkumná instituce dle § 2 této vyhlášky je</p> <p>I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že</p> <ol style="list-style-type: none"><li>1. v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky citlivou výzkumnou činnost, nebo</li><li>2. v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU<sup>[3]</sup>:<ol style="list-style-type: none"><li>a. technologie pokročilých polovodičů,</li><li>b. technologie umělé inteligence,</li><li>c. kvantové technologie, nebo</li><li>d. biotechnologie.</li></ol></li></ol> <p>II. poskytovatelem regulované služby v režimu nižších povinností v případě, že v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky aplikovaný výzkum v některém z níže uvedených oborů výzkumu a vývoje dle doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU<sup>[4]</sup>:</p> <ol style="list-style-type: none"><li>1. <b>pokročilá konektivita, navigace a digitální technologie,</b></li><li>2. <b>technologie pokročilého snímání,</b></li><li>3. <b>vesmírné technologie a technologie pohonu,</b></li><li>4. <b>energetické technologie,</b></li><li>5. <b>robotika a autonomní systémy, nebo</b></li><li>6. <b>pokročilé materiály, výrobní a recyklační technologie.</b></li></ol> <p>Výzkumná instituce podle § 2 této vyhlášky je poskytovatelem regulované služby v režimu nižších povinností v případě, že je <b>velkým podnikem</b>.</p>

**Velký podnik** = >250 zaměstnanců nebo 50 milionů EUR obrát a 43 milionů EUR rozvaha



## 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

## ➤ Redukovaná bezpečnostní opatření pro nižší režim



## NIŽŠÍ REŽIM

### § 7

#### Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

1. v rámci primárních aktiv stanoví jejich prioritu a pořadí a postupy jejich obnovy,
2. stanoví odpovědnosti a povinnosti při obnově podle písm. a),
3. vytváří pravidelné zálohy nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

## VYŠŠÍ REŽIM

### § 16

#### Řízení kontinuity činností

1. Povinná osoba v rámci řízení kontinuity činností
  - a) stanoví metodiku pro provedení analýzy dopadů,
  - b) pomocí analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a zohlední hodnocení rizik podle § 9, v rámci kterého posoudí možná rizika související s ohrožením kontinuity činností,
  - c) na základě výstupů analýzy dopadů a hodnocení rizik podle písmene b) stanoví cíle řízení kontinuity činností formou určení
    - i) minimální úroveň poskytovaných služeb, která je přijatelná pro užívání, provoz a správu regulované služby,
    - ii) doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby a
    - iii) bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,
  - d) stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c) a stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,
  - e) vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a plány obnovy související s poskytováním regulované služby a
  - f) realizuje bezpečnostní opatření pro zvýšení odolnosti podle § 27.
2. Cíle řízení kontinuity podle odst. 1 písm. c) tohoto ustanovení jsou stanoveným časem a kvalitou regulované služby podle § X [Zajištění dostupnosti strategicky významné služby] zákona. Stanoveným časem je doba obnovení chodu podle odst. 1 písm. c) bod ii) tohoto ustanovení a stanovenou kvalitou regulované služby je minimální úroveň poskytovaných služeb podle odst. 1 písm. c) bodu i) tohoto ustanovení.



- **Přiměřenost nákladů** – bezpečnostní opatření nemá být dražší, než jaké jsou náklady realizovaného incidentu (Součást obou vyhlášek jako princip)

## Cost of a Data Breach Report 2023 od IBM:.

- průměrné globální náklady na únik dat 4,45 milionu USD, tedy 103,5 milionu Kč
- nárůst o 15 % za poslední tři roky

## 123 SMB Cybersecurity Statistics

- 61 % malých a středně velkých podniků terčem kybernetického útoku
- průměrné náklady na řešení KBI v roce 2023 od 826 do 653 587 USD

## Nová zpráva Izraelské INCD: analýza nákladů KBI na izraelskou ekonomiku:

- nejméně 12 miliard NIS ročně = přes 76 miliard Kč
- základní opatření mohou snížit šance na útok o 30–50 %

Kybernetická kriminalita se v roce 2025 stane 3. největší ekonomikou světa



## Přehled v organizaci

- Jaké vykonávám agendy a poskytuji služby?
- Co pro výkon těchto agend 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 finanční a personální kapacity?
- Co je má prioritní služba?
- Provedu analýzy, stanovím plán se zohledněním kapacit a priorit.

## Zavádění opatření

- Určím osobu odpovědnou za KB.
- Priorita je vzdělávání zaměstnanců včetně vedení.
- Vytvořím bezpečnostní politiku, kterou lze fakticky používat.
- Pokračuji dle plánu.

## Zásada přiměřenosti:

- Náklady na zaváděné opatření by neměly převyšovat náklady na případnou realizaci kybernetického incidentu.
- Nechci všechno najednou, postupně se zlepšuji.



# Děkuji za pozornost.

<https://portal.nukib.gov.cz/>

[regulace@nukib.cz](mailto:regulace@nukib.cz)

