# Svaz průmyslu a dopravy České republiky

# PŘIPOMÍNKY

## k návrhu vyhlášky o portálu kritické infrastruktury

## Doporučující připomínky

### K návrhu vyhlášky

#### 1. Obecně

**K Důvodové zprávě, I. Obecná část, 1. Popis obsahu návrhu právního předpisu s uvedením důvodů, které k jeho předložení vedou, a shrnutí základních zásad a nejdůležitějších změn, které oproti stávající právní úpravě zavádí, a zhodnocení platného právního stavu**

V části *hlavní principy navrhované právní úpravy, efektivní a bezpečný přenos informací* požadujeme, aby bylo postaveno na jisto, jakým způsobem má být „bezpečnosti" technicky dosaženo. Zcela absentuje popis bezpečnostního řešení a přenosu informací ze strany subjektu kritické infrastruktury.

#### 2. Obecně

**K Důvodové zprávě, I. Obecná část, 1. Popis obsahu návrhu právního předpisu s uvedením důvodů, které k jeho předložení vedou, a shrnutí základních zásad a nejdůležitějších změn, které oproti stávající právní úpravě zavádí, a zhodnocení platného právního stavu**

V posledním odstavci zákonodárce uvažuje o použití portálu kritické infrastruktury jako platformy umožňující jednotný postup pro hlášení incidentů relevantním orgánům státní správy, **avšak z navrhované úpravy nevyplývá, že by tímto postupem mělo být nahrazeno nebo sjednoceno plnění ohlašovacích povinností podle jednotlivých právních předpisů**.

**Subjekt kritické infrastruktury tedy bude mít povinnost hlásit jednotlivé incidenty samostatně, podléhají-li různým právním předpisům, i přesto, že se jedná o incident, který je společný.** Takto nastavený mechanismus popírá deklarovaný cíl jednotného a efektivního hlášení incidentů a vede k duplicitní administrativní zátěži dotčených subjektů.

#### 3. Obecně

**K Důvodové zprávě, I. Obecná část, 8.8. Dopad na bezpečnost nebo obranu státu**

V důvodové zprávě je uvedeno, že návrh vyhlášky má jednoznačně pozitivní dopady na bezpečnost a obranu státu, zejména s ohledem na centralizaci hlášení incidentů prostřednictvím portálu kritické infrastruktury a dostupnost aktualizovaných dat. Tento závěr však není možné považovat za dostatečně podložený, neboť z předloženého materiálu nelze jednoznačně dovodit, jakým způsobem má být zajištěna odpovídající úroveň technického a organizačního zabezpečení portálu.

Bez adekvátního zabezpečení portálu může mít navrhované řešení naopak negativní dopad na bezpečnost státu, jelikož soustředění rozsáhlé a citlivé dokumentace a informací o subjektech kritické infrastruktury a incidentech do jednoho informačního systému představuje zvýšené bezpečnostní riziko a potenciální cíl útoku. Absence bližší specifikace bezpečnostního řešení znemožňuje posoudit, zda deklarované pozitivní dopady návrhu na bezpečnost a obranu státu skutečně převyšují související rizika.

## 4. Obecně

**K Důvodové zprávě, I. Obecná část, 8.9. Dopad ve vztahu k ochraně soukromí a osobních údajů, Základní parametry navrhovaného zpracování osobních údajů, tabulka**

V předložené tabulce vymezující účely zpracování osobních údajů, subjekty údajů a druh (rozsah) zpracovávaných údajů nejsou v rozsahu zpracovávaných osobních údajů uvedeny některé údaje, které mohou být v souvislosti s fungováním portálu kritické infrastruktury relevantní nebo nezbytné. Konkrétně se jedná zejména o údaje o státní příslušnosti, přihlašovací údaje do portálu, dobu pověření oprávněné osoby k přístupu do portálu a případně číslo dokladu totožnosti.

Absence těchto údajů v přehledu rozsahu zpracovávaných osobních údajů ztěžuje posouzení úplnosti a přiměřenosti navrhovaného zpracování osobních údajů, a tím i vyhodnocení dopadů návrhu vyhlášky na ochranu soukromí a osobních údajů.

## 5. Obecně

**K Důvodové zprávě, Obecná část, 8.9 (Rozsah zpracování osobních údajů – rozpor se zásadou minimalizace)**

Požadujeme upravit rozsah vyžadovaných osobních údajů v tabulce v bodě 8.9 Důvodové zprávy i v samotných procesech portálu tak, aby odpovídal zásadě minimalizace dat.

*Žádáme tedy z*cela vypustit sběr údajů „datum narození“ a „akademický titul“ u členů statutárních orgánů, pověřených pracovníků, manažerů kritické infrastruktury a kritických pracovníků. V obecné části zprávy rovněž vypustit sběr "adresy bydliště" u fyzických osob.

Odůvodnění:

Pro plnění účelů zákona o kritické infrastruktuře a přístupu do portálu postačují běžné identifikační a kontaktní údaje (jméno, příjmení, pracovní zařazení/role, telefon a e-mail), jak je ostatně správně definováno pro oprávněné osoby v samotném § 4 odst. 3 vyhlášky. Sběr akademických titulů a dat narození představuje nadbytečný a neospravedlnitelný zásah do soukromí zaměstnanců. Zajištění odolnosti subjektu nevyžaduje tyto citlivé osobní údaje.

## 6. Obecně

**K Důvodové zprávě, I. Obecná část, 8.9**

**Navrhujeme doplnit výslovnou zmínku o potřebě chránit i citlivé obchodní a bezpečnostní informace vložené do portálu.**

Odůvodnění:

Vedle ochrany osobních údajů je nutné zohlednit i ochranu údajů obchodně a bezpečnostně citlivých.

## 7. Obecně

**K vyhlášce - Návaznost na další hlásicí povinnosti**

**Doporučujeme zvážit doplnění vyhlášky o obecné zakotvení možnosti budoucího využití portálu kritické infrastruktury jako jednotného vstupního místa (Single Entry Point) pro hlášení incidentů vůči dalším relevantním orgánům veřejné moci (např. NÚKIB, Česká národní banka).** Takový přístup by do budoucna mohl snížit duplicitu hlášení a administrativní zátěž regulovaných subjektů.

## 8. Obecně

**K vyhlášce - Podpora testovacího a cvičného režimu**

**Doporučujeme zvážit možnost využití portálu také pro účely testování a cvičení** (např. cvičná hlášení incidentů, ověřování funkčnosti datových toků). Takové využití by přispělo ke zvýšení připravenosti subjektů kritické infrastruktury i příslušných orgánů veřejné moci a k celkovému posilování odolnosti systému.

## 9. Obecně

**Považujeme za nezbytné, aby technické nastavení portálu kritické infrastruktury odpovídalo praktickému fungování společností s rozsáhlou sítí provozoven, např. v oblasti maloobchodu. Portál by měl být koncipován způsobem, který povede ke skutečnému snížení administrativní zátěže a zefektivnění komunikace se státní správou.**

## 10. Obecně

**Připomínka k plánu odolnosti – seznam kritických pracovníků**

Doporučujeme výkladově potvrdit, že seznam kritických pracovníků v plánu odolnosti může být veden na úrovni rolí nebo pozic, přičemž jmenovitá identifikace osob je vedena operativně mimo plán.

Odůvodnění:

Vyhláška o plánu odolnosti předpokládá identifikaci kritických pracovníků prostřednictvím pozic nebo kategorií pracovníků s ohledem na jejich funkci při poskytování základní služby. Tento přístup reflektuje provozní realitu subjektů s vyšším počtem provozoven a personální fluktuací a zároveň umožňuje zachování aktuálnosti a funkčnosti plánu odolnosti.

## 11. K § 2

Navrhujeme doplnit závazek správce portálu k primárnímu užití komunikačního kanálu Portálu a pravidla komunikace ve směru od MV k regulovaný subjektům.

Odůvodnění:

Je nezbytné promítnout i deklaraci MV k tomu, že bude směrem na regulované subjekty komunikovat pomocí Portálu. Jednostranná komunikace by jinak ztrácela smysl. Tato komunikace by měla mít současně jasně stanovená pravidla, tak jak jsou stanovena pro komunikaci směrem regulovaných subjektů směrem k Portálu.

## 12. K § 2

Navrhuje se vložit do § 1 nový odstavec obsahující slovník pojmů a současně vypustit definiční část z § 2 tak, aby § 2 upravoval výlučně vlastní úpravu portálu.

Návrh nového znění:

**Navrhované znění § 1 (doplnění):**

§ 1 Předmět úpravy

(1) Tato vyhláška stanoví

a) formu a způsob zpracování informací, dat, údajů a evidencí (dále jen „informace“) vkládaných do portálu kritické infrastruktury (dále jen „portál“) a jejich strukturu a

b) technické a organizační podmínky používání portálu.

**(2) Pro účely této vyhlášky se rozumí:**

**a) portálem kritické infrastruktury informační systém určený ke zpracování informací podle zákona o kritické infrastruktuře,**

**b) oprávněným uživatelem subjekt nebo orgán oprávněný využívat portál podle zákona o kritické infrastruktuře,**

**c) oprávněnou osobou fyzická osoba oprávněná jednat za oprávněného uživatele v portálu.**

Současně se navrhuje **v § 2 vypustit definiční část**, a § 2 ponechat pouze jako ustanovení upravující fungování portálu.

Odůvodnění:

Návrh vyhlášky v současném znění neobsahuje samostatné definiční ustanovení, přestože pracuje s pojmy, které jsou pro aplikaci právního předpisu klíčové. Tyto pojmy jsou částečně vymezeny v rámci § 2 „Portál“, který má podle svého názvu i systematiky upravovat věcnou regulaci fungování portálu, nikoli obecné pojmy.

Takové řešení není v souladu s legislativními zvyklostmi, podle nichž mají být pojmy používané v právním předpisu vymezeny přehledně a systematicky, zpravidla na jeho počátku, a odděleně od ustanovení upravujících vlastní práva a povinnosti. Soustředění definičních ustanovení do § 1 přispívá k jednoznačnosti výkladu, přehlednosti právní úpravy a ke zvýšení právní jistoty adresátů právní normy.

Navržená změna má výlučně systematický a legislativně-technický charakter a nemění věcný obsah navrhované právní úpravy.

## 13. K § 2

Ustanovení § 2 návrhu vyhlášky neobsahuje dostatečné vymezení portálu kritické infrastruktury jako informačního systému, ani základní rámec jeho fungování. Ze znění ustanovení není zřejmé, o jaký typ informačního systému se jedná, zejména zda je portál provozován jako webová aplikace umožňující dálkový přístup, jiná forma aplikace, nebo jiný technický model.

Návrh dále zcela opomíjí systematické vymezení procesu přístupu do portálu, zejména jakým způsobem jsou získávány přihlašovací údaje, jakým způsobem je ověřováno, že za oprávněného uživatele jedná skutečně osoba k tomu oprávněná, v jaké právní formě oprávněný uživatel prostřednictvím oprávněných osob jedná.

Současně není nijak popsán základní rámec zabezpečení portálu jako informačního systému, ani principy řízení přístupových práv oprávněných osob. Zejména není zřejmé, v jakém rozsahu budou jednotlivým oprávněným osobám přidělována oprávnění k nahlížení, vkládání či editaci informací, ani jak bude regulován přístup k informacím z hlášení incidentů.

V důsledku uvedeného není zřejmé, v jakém rozsahu a vůči jakému okruhu subjektů a osob mohou být zpřístupněny konsolidované informace a dokumenty strategického a bezpečnostního významu, které mají být prostřednictvím portálu shromažďovány.

Odůvodnění:

Portál kritické infrastruktury má podle návrhu vyhlášky plnit roli centrální platformy pro shromažďování, zpracování a sdílení informací zásadního významu z hlediska bezpečnosti státu. Na tomto základě požadujeme doplnit do návrhu vyhlášky a důvodové zprávy informace na základě výše uvedených slabých a bílých míst.

## 14. K § 2 odst. 5

Doporučujeme nahradit text „Správce nebo oprávněný uživatel“ formulací „ministerstvo vnitra (dále jen správce)“.

## 15. K § 2 odst. 6

**Návrh změny:**

„(6) Pokud prostřednictvím portálu nelze vložit informace a tyto byly správci doručeny jiným způsobem v souladu se zákonem o kritické infrastruktuře, správce zajistí jejich vložení do portálu bez zbytečného odkladu. **Oprávněný uživatel nenese odpovědnost za prodlení nebo nesoulad vzniklý výlučně v důsledku technické nedostupnosti portálu nebo postupu správce při následném vložení informací do portálu.“**

Odůvodnění:

Máme za to, že je nutné výslovně upravit odpovědnost pro případy výpadku portálu. Bez této úpravy vzniká právní nejistota na straně povinných subjektů.

## 16. K § 3 odst. 2 písm. b)

**Návrh změny:**

„b) údaje o kritických dodavatelích, manažerovi kritické infrastruktury a dalších osobách, mají-li tyto osoby přístup do portálu, **v rozsahu nezbytném pro plnění povinností podle zákona o kritické infrastruktuře a s ohledem na zásadu minimalizace údajů**.“

Odůvodnění:

Rozsah evidovaných údajů by měl být výslovně omezen zásadou minimalizace, aby nedocházelo k nepřiměřenému sběru údajů o pracovnících a dodavatelích jednotlivých subjektů.

## 17. K § 3 odst. 2 písm. b)

Požadujeme výkladové upřesnění, že uvedení kritických pracovníků a kritických dodavatelů v rámci identifikačních informací nezakládá povinnost zřizovat těmto osobám nebo subjektům přístup do portálu kritické infrastruktury.

Odůvodnění:

Z vyhlášky o portálu kritické infrastruktury ani z její důvodové zprávy nevyplývá, že by kritičtí pracovníci nebo kritičtí dodavatelé měli být automaticky považováni za oprávněné osoby s přístupem do portálu. Přístup do portálu je dle § 4 vyhlášky určen výlučně osobám, které prostřednictvím portálu vkládají informace nebo jednají za oprávněného uživatele, a má být omezen podle zásady minimalizace. Nejednoznačný výklad by u rozsáhlých retailových subjektů

s vysokým počtem provozních pracovníků a přirozenou fluktuací vedl k neúměrné administrativní zátěži, která není předvídána zákonem ani vyhláškou.

## 18. K § 3 odst. 2 písm. b)

**K ustanovení § 3 odst. 2 písm. b) a Důvodové zprávě 8.9 (Rozsah evidence kritických dodavatelů)**

Žádáme o upřesnění a omezení vyžadovaných informací o kritických dodavatelích.

● *Žádáme z*rušit v důvodové zprávě povinnost vkládat kontaktní „telefonní číslo“ a „e-mail“ na kritické dodavatele (pokud nemají přímý přístup do portálu).

Odůvodnění:

Udržovat trvale aktuální telefonní čísla a e-maily na třetí strany (dodavatele) v externím státním portálu je v praxi velkých firem téměř neproveditelné. Pro základní identifikaci dodavatele plně postačuje název právnické osoby, identifikační číslo a adresa sídla. V případě potřeby detailnější komunikace si orgány krizového řízení mohou kontaktní údaje třetích stran vyžádat u poskytovatele základní služby ad hoc.

## 19. K § 3 odst. 3

Navrhujeme doplnit propojení Portálu s Portálem NÚKIB a systémem pro hlášení kyberbezpečnostních incidentů podle jiných právních předpisů a vyjmout hlášení těch incidentů, které jsou již hlášeny NÚKIB podle jiných právních předpisů.

Odůvodnění

Logickým ze strany MV by mělo být propojení systémů a portálů pro hlášení incidentů podle dalších právních předpisů tak, aby nedocházelo ke zdvojení povinnosti hlášení takových incidentů, tedy typicky s obdobným portálem NÚKIB. Podnikatelům a povinným subjektům tak vzniká neúměrná zátěž ve zdvojené povinnosti.

## 20. K § 3 odst. 4

Ustanovení § 3 odst. 4 stanoví, že identifikační informace se do portálu vkládají pouze v rozsahu údajů, které nejsou portálem automaticky generovány. Ze zvláštní části důvodové zprávy k § 3 vyplývá, že smyslem tohoto ustanovení je rozlišit údaje aktivně vkládané oprávněným uživatelem od údajů vznikajících systémově v rámci fungování portálu kritické infrastruktury.

Předložený právní předpis však neobjasňuje, jakým konkrétním způsobem má automatické generování těchto údajů fungovat. Není zřejmé, které identifikační údaje jsou portálem automaticky generovány, z jakých zdrojů tyto údaje vznikají nebo jsou přebírány, jaký je proces jejich vzniku, aktualizace a vazby na údaje vkládané oprávněným uživatelem.

Současně zcela chybí popis komunikačního schématu portálu kritické infrastruktury, tedy jakým způsobem portál komunikuje s oprávněnými uživateli, správcem portálu a případně dalšími informačními systémy veřejné správy. Z textu není patrné, zda a v jakém rozsahu dochází k výměně dat s jinými systémy ani jaké jsou základní datové toky v rámci portálu.

Odůvodnění:

Nejasnost ohledně geneze automaticky generovaných údajů a komunikačního schématu portálu snižuje právní jistotu adresátů a ztěžuje posouzení proveditelnosti a odpovědnosti za správnost a

aktuálnost identifikačních informací. Proto požadujeme doplnit do návrhu vyhlášky a důvodové zprávy zmiňované informace.

## 21. K § 4

Požadujeme doplnit možnost komunikace přes API.

Odůvodnění:

S ohledem na zvyšování digitalizace procesů nejen státní správy a samosprávy dochází k digitalizaci procesů také v soukromém sektoru, proto je nezbytné umožnit automatizované propojení s Portálem, aby mohlo být hlášení prováděno automaticky.

## 22. K § 4

Doporučujeme doplnit nový odst. 8) „Po zařazení poskytovatele základní služby na seznam subjektů kritické infrastruktury obdrží každý subjekt kontaktní údaje na správce, mimo jiné pro případ výpadku portálu“.

## 23. K § 4 odst. 1

Požadujeme reflektovat status informačního systému veřejné správy, kterým Portál bezesporu je a v souvislosti s tím nastavit bezpečnostní pravidla a opatření dle příslušných právních předpisů.

Odůvodnění:

Vyhláškou definovaný „Portál kritické infrastruktury“ bezpochyby bude Informačním systémem veřejné správy a měl by tak respektovat požadavky na funkčnost, stanovené platnými právními předpisy, včetně odpovídajících částí NAPu, zejména pak z pohledu realizace digitálních úkonů v prostředí portálu. Základní pravidla (např. autentizace, autorizace, jednání v zastoupení) jsou v NAP jednoznačně definována a není proto z našeho pohledu možné stanovovat odchylnou úpravu. Tím spíš, že NAP obsahuje i dispozice i pro komunikaci ISVS v krizovém stavu.

Portál by dle našeho názoru měl pro autentizaci využívat výhradně kvalifikované prostředky elektronické identifikace s úrovní důvěry „vysoká“, konzumovat služby RPP / ReZa na podporu jednání v zastoupení za právnické osoby (pro zástupce OVM správu účtu v CAAIS), autorizovat úkony (včetně následného vystavení Osvědčení o provedení digitálního úkonu) a zajistit i podporu obousměrné zabezpečené komunikace.

## 24. K § 4 odst. 1

**Návrh změny:**

„(1) Správce portálu zveřejňuje způsob autentizace, základní rozsah uživatelských oprávnění a technické požadavky pro používání portálu způsobem umožňujícím dálkový přístup, **včetně informací o plánovaných odstávkách, změnách technických parametrů, kontaktní podpory a postupu při řešení nedostupnosti portálu**.“

Odůvodnění:

Povinné subjekty musí mít včas k dispozici i provozní informace o fungování portálu, aby mohly řádně plnit své zákonné povinnosti.

## 25. K § 4 odst. 2

**K § 4 odst. 2 a 4**

Ustanovení § 4 odst. 2 stanoví, že přístupová oprávnění do portálu se zřizují jako individuální, nepřenosná a jedinečná pro každou oprávněnou osobu. Ze znění tohoto ustanovení však není zřejmé, zda právní úprava počítá také s možností zřízení přístupových oprávnění pro zástupce osoby oprávněné za oprávněného uživatele do portálu vkládat informace nebo prostřednictvím portálu za oprávněného uživatele jednat.

Není tedy jasné, zda může mít oprávněná osoba svého zástupce (např. v případě nepřítomnosti, organizačního zajištění nebo rozdělení rolí), zda má být takový zástupce považován za samostatnou oprávněnou osobu s vlastním individuálním přístupem, nebo zda právní úprava tuto možnost nepředpokládá.

Odůvodnění:

Nejasnost ohledně možnosti zastupování oprávněné osoby v kombinaci se zásadou individuálních, nepřenosných a jedinečných přístupových oprávnění vyvolává výkladové pochybnosti a snižuje právní jistotu adresátů právní normy. Bez výslovného vyjasnění není zřejmé, zda a za jakých podmínek lze zajistit kontinuitu plnění povinností oprávněného uživatele (např. při nepřítomnosti oprávněné osoby), aniž by docházelo k porušení uvedených zásad. Požadujeme doplnit do návrhu vyhlášky a důvodové zprávy, zda mohou být zřizována přístupová oprávnění pro zástupce osoby oprávněné jednat za oprávněného uživatele, případně zda je takový zástupce považován za samostatnou oprávněnou osobu s vlastním individuálním přístupem.

## 26. K § 4 odst. 2

Ustanovení § 4 odst. 2 stanoví, že přístupová oprávnění do portálu se zřizují jako individuální, nepřenosná a jedinečná pro každou oprávněnou osobu. Z návrhu však není zřejmé, jakou konkrétní formu mají tato přístupová oprávnění, zejména zda se jedná o přístupové údaje ve formě přihlašovacího jména a hesla, případně jiného obdobného autentizačního prostředku.

V případě, že jsou přístupová oprávnění realizována prostřednictvím přihlašovacích údajů, jedná se o údaje, které v kombinaci s dalšími identifikačními údaji oprávněné osoby představují osobní údaje ve smyslu obecného nařízení o ochraně osobních údajů. Tato skutečnost však není v návrhu ani v důvodové zprávě nijak reflektována.

Odůvodnění:

Z návrhu vyhlášky ani z důvodové zprávy není zřejmé, jakou konkrétní formu mají přístupová oprávnění do portálu, zejména zda jsou realizována prostřednictvím přihlašovacích údajů (např. přihlašovací jméno a heslo). V případě, že tomu tak je, jedná se o údaje, které v kombinaci s dalšími údaji oprávněné osoby představují osobní údaje ve smyslu GDPR.

Z tohoto důvodu požadujeme vyjasnit, jaká forma přístupových údajů je předpokládána a zda je s nimi nakládáno jako s osobními údaji, včetně odpovídajícího zohlednění z hlediska ochrany osobních údajů.

## 27. K § 4 odst. 2

**Připomínka k § 4 odst. 2 a 3**

Navrhujeme jednoznačně vymezit, že oprávněnými osobami s přístupem do portálu jsou pouze osoby výslovně určené oprávněným uživatelem, typicky manažer kritické infrastruktury a omezený okruh pověřených osob, nikoliv kritičtí pracovníci obecně.

Odůvodnění:

Tento výklad odpovídá zásadě minimalizace přístupů, odpovědnosti konkrétních osob za správnost a aktuálnost údajů a je plně v souladu s vyhláškou o plánu odolnosti, která identifikaci kritických pracovníků váže primárně na stanovení pozic nebo kategorií pracovníků, nikoliv na jejich zapojení do systémových procesů nebo nárok na přístup do portálu.

## 28. K § 4 odst. 3

Doporučujeme doplnit text v písm. b) takto: „vymezení role **a rozsah oprávnění** při využívání portálu“.

## 29. K § 4 odst. 4

Navrhujeme nahradit vágní pojem „bez zbytečného odkladu“ přesnou lhůtou, která bude pro subjekty reálně splnitelná.

● *Návrh znění:* „...oprávněný uživatel zajistí **nejpozději do 15 dnů od vzniku změny** aktualizaci okruhu osob...“

Odůvodnění:

V maloobchodním a korporátním prostředí je přirozená fluktuace a interní přesuny zaměstnanců na denním pořádku. Termín „bez zbytečného odkladu“ zakládá právní nejistotu, neboť může být kontrolními orgány vykládán jako povinnost okamžité aktualizace v řádu hodin. Stanovení pevné, například patnáctidenní lhůty, poskytne společnostem dostatečný prostor pro standardní administrativní procesy (offboarding) a sníží riziko neúmyslného pochybení.

## 30. K § 4 odst. 5

Navrhujeme doplnit § 4 odst. 5 o možnost automatizovaného vkládání dat prostřednictvím aplikačního rozhraní (API).

● *Návrh znění:* „Informace se do portálu vkládají ve strukturované elektronické podobě prostřednictvím uživatelského rozhraní **nebo prostřednictvím automatizovaného programového rozhraní (API)**.“

Odůvodnění:

Návrh v současném znění omezuje vkládání informací pouze na uživatelské rozhraní. Pro velké subjekty kritické infrastruktury nebo poskytovatele základních služeb, jako jsou nadnárodní maloobchodní sítě, je manuální zadávání rozsáhlých objemů dat (např. seznamy desítek až stovek kritických pracovníků a dodavatelů) neefektivní. Důvodová zpráva přitom deklaruje jako hlavní princip efektivní a bezpečný přenos informací a snížení administrativní náročnosti. Bez možnosti systémového napojení (stroj-stroj) dojde u velkých společností k masivnímu nárůstu byrokracie, před čímž varuje i bod 1 důvodové zprávy u snahy o standardizaci postupů.

## 31. K § 4 odst. 6

Ustanovení § 4 odst. 6 stanoví, že dokumentace nebo jiné materiály se vkládají do portálu ve formátu stanoveném správcem. Avšak není zřejmé, zda a jakým způsobem bude verifikováno zabezpečení vložených dokumentů (např. zda budou kontrolovány bezpečnostní atributy souborů, škodlivý obsah, případně požadavky na ochranu dokumentů), ani jaké předepsané konfigurační a bezpečnostní požadavky budou na portál a vkládané soubory kladeny.

Odůvodnění:

Vkládání dokumentace a jiných materiálů do portálu může zahrnovat obsah bezpečnostně nebo strategicky citlivé povahy. Není však zřejmé, jak bude ověřováno zabezpečení vkládaných dokumentů ani jaké minimální bezpečnostní a konfigurační požadavky budou na portál a vkládané soubory kladeny. Z tohoto důvodu požadujeme doplnit tyto informace.

## 32. K § 4 odst. 6

**K § 4 odst. 6, věta „ve formátu stanoveném správcem“**

Ustanovení § 4 odst. 6 stanoví, že dokumentace nebo jiné materiály se vkládají do portálu ve formátu stanoveném správcem. Z uvedeného však není zřejmé, zda a jakým způsobem má být zajištěno zabezpečení vkládaných dokumentů, zejména v situaci, kdy dokumentace může obsahovat citlivé, bezpečnostně významné nebo interní informace.

Vzhledem k nejasnosti ohledně úrovně zabezpečení portálu a vkládaných souborů může v praxi vzniknout potřeba opatřovat dokumenty dodatečnými bezpečnostními opatřeními, například jejich ochranou heslem, aby nedošlo k porušení právních nebo interních předpisů jednotlivých subjektů.

Odůvodnění:

Neurčitost vymezení „formátu stanoveného správcem“ neumožňuje adresátům právní úpravy posoudit, zda je zabezpečení vkládané dokumentace zajištěno již na úrovni portálu, nebo zda je očekáváno, že odpovědnost za ochranu obsahu ponesou oprávnění uživatelé formou dodatečných opatření (např. zaheslováním dokumentů). Z toho důvodu požadujeme tuto skutečnost vyjasnit.

## 33. K § 4 odst. 6

Navrhujeme garantovat použití běžně dostupných formátů.

● *Návrh znění:* „Dokumentace nebo jiné materiály se vkládají do portálu ve **standardních a otevřených** formátech stanovených správcem.“

Odůvodnění:

Ustanovení dává správci (Ministerstvu vnitra) zcela volnou ruku diktovat jakékoliv datové formáty. Z důvodu předvídatelnosti a zamezení budoucích dodatečných nákladů na konverzi dat do případných proprietárních formátů doporučujeme omezit tuto pravomoc na běžné, mezinárodně uznávané a otevřené formáty dokumentů (např. PDF, DOCX, XLSX).

## 34. K § 4 odst. 7

Ustanovení § 4 odst. 7 ukládá oprávněnému uživateli povinnost zajistit správnost, úplnost a aktuálnost informací, dokumentace nebo materiálů vložených do portálu oprávněnou osobou. Takto formulovaná povinnost však nebere v dostatečné míře v úvahu povahu hlášení incidentů podle § 18 a § 19 zákona o kritické infrastruktuře. V průběhu šetření incidentu mohou vycházet najevo nové skutečnosti, které dodatečně mění nebo zpřesňují dříve poskytnuté informace, případně je činí neaktuálními nebo neúplnými k okamžiku jejich původního vložení do portálu.

Odůvodnění:

Bez bližšího vyjasnění může být povinnost zajistit „správnost, úplnost a aktuálnost“ vykládána příliš rigidně, aniž by zohledňovala, že informace o incidentech jsou poskytovány na základě aktuálně dostupných poznatků a mohou se v průběhu času měnit.

Z tohoto důvodu požadujeme vyjasnit předmětnou právní úpravu v tom smyslu, že uvedená povinnost se vztahuje k informacím v rozsahu a stavu poznání dostupném v době jejich vložení a

že následné zpřesňování nebo změny informací v průběhu vyšetřování incidentu nejsou porušením této povinnosti, ale jejím přirozeným naplněním.

## 35. K § 4 odst. 7

**Návrh změny:**

„(7) Oprávněný uživatel zajišťuje správnost, úplnost a aktuálnost informací, dokumentace nebo materiálů vložených do portálu oprávněnou osobou, **pokud mohl jejich správnost, úplnost a aktuálnost rozumně ověřit a pokud nesprávnost nevznikla v důsledku technického omezení portálu nebo chybného nastavení správcem**.“

Odůvodnění:

Odpovědnost oprávněného uživatele by měla být přiměřeně vymezena jen na skutečnosti, které mohl reálně ovlivnit a ověřit.