

## DÔVODOVÁ SPRÁVA

### A. Všeobecná časť

Ministerstvo vnútra SR predkladá návrh zákona o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov, ktorého cieľom je transpozícia a implementácia právnych predpisov Európskej únie. V prvom rade ide o transpozíciu smernice Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES (ďalej len „smernice (EÚ) 2022/2557“). Zároveň sa zabezpečuje implementácia delegovaného nariadenia Komisie (EÚ) 2023/2450 zo 25. júla 2023, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 stanovením zoznamu základných služieb (Ú. v. EÚ L, 2023/2450, 30.10.2023).

Doterajšia smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu bola transponovaná do zákona č. 45/2011 Z. z. o kritickej infraštruktúre.

Cesta kreovania legislatívnych a koncepčných dokumentov na úseku kritickej infraštruktúry bola ovplyvnená medzinárodnými bezpečnostnými udalosťami, najmä sériou koordinovaných útokov na Svetové obchodné centrum v New Yorku v roku 2001, následné teroristickými akciami na železnice v Madride v roku 2004 a útokmi na dopravu v Londýne 2005. Preto sa v dokumentoch spája ochrana kritickej infraštruktúry v prvom rade s obranou proti terorizmu. Ďalší vývoj koncepčných a strategických dokumentov, ako je Bezpečnostná stratégia SR z roku 2005, považuje za najväčšiu hrozbu použitie zbraní hromadného ničenia a niektorých ich nosičov teroristickými skupinami, prípadne tzv. „zlyhávajúcimi štátmi“. Terorizmus predstavuje pre Slovenskú republiku (ďalej len „SR“) strategickú globálnu hrozbu. Prioritám dominuje boj proti terorizmu aj v Európskej bezpečnostnej stratégii z roku 2009. Téma globalizácie ustupuje do úzadia a do popredia sa dostávajú témy ako je zmena klímy a kybernetická bezpečnosť. Následná obsahová terminológia ako terorizmus, kybernetické alebo informačné operácie sa spojili do termínu asymetrické hrozby. Z terminologického významu existuje množstvo definícií asymetrických hrozieb, ktoré sa snažia zachytiť špecifickú povahu nových druhov hrozieb pre bezpečnosť a stabilitu štátu, ktoré koordinovane a plánovito využívajú rôzni aktéri. V tejto súvislosti sa najčastejšie hovorí o hybridných hrozbách (hybrid threats) a hybridných spôsoboch vedenia vojny (hybrid warfare).

Na pôde Európskej únie sa problematike hybridných hrozieb venuje značná pozornosť a od roku 2016 bolo prijatých viacero verejných politík a dokumentov dotýkajúcich sa tejto oblasti. Na Slovensku vznikol prvý koncepčný dokument v roku 2017 s názvom Koncepcia pre boj SR proti hybridným hrozbám. Tento koncepčný dokument ako prvý spojil boj proti hybridným hrozbám s ochranou kritickej infraštruktúry. Okrem kritickej infraštruktúry dokument používa aj termín kľúčová infraštruktúra, ktorou definuje akúkoľvek infraštruktúru, ktorá má zásadný význam pre štát a spoločnosť. Aktuálna Bezpečnostná stratégia SR z roku 2021 zahrňuje medzi strategické bezpečnostné záujmy Slovenskej republiky, ktorých ochrana a presadzovanie podporuje aj realizáciu životne dôležitých bezpečnostných záujmov (mimo iných aj);

- ochranu kritickej infraštruktúry štátu a
- zaistenie funkčného systému kybernetickej, informačnej a komunikačnej bezpečnosti.

V rámci dokumentu Správa o bezpečnosti SR za rok 2020 medzi najzávažnejšie bezpečnostné hrozby asymetrického charakteru naďalej patril terorizmus vykonávaný teroristickými (džihádistickými) skupinami. K zhoršeniu bezpečnostnej situácie došlo počas druhej polovice roka 2020 po prechodnom uvoľnení viacerých protipandemických opatrení.

Oblasťou možnej konfrontácie podľa Správy o bezpečnosti SR za rok 2023 sa stal vzdušný priestor, vesmír, medzinárodné vody a kybernetický priestor. Príčinou je prebiehajúca exponenciálna technologická zmena, osobitne v technológiách využívajúcich umelú inteligenciu. Ďalším významným faktorom, ktorý ovplyvňuje bezpečnostné prostredie, je široké používanie hybridných stratégií vrátane aktívneho šírenia dezinformácií a škodlivých aktivít v kybernetickom priestore. Dôsledky klimatických zmien vplývajúce na potravinovú bezpečnosť, energetickú bezpečnosť, infraštruktúru, udržateľný rozvoj štátov spolu s chudobou a etnickými konfliktmi predstavovali aj v roku 2023 výzvy.

V súčasnom geopolitickom kontexte, ktorý sa vyznačuje rastúcou nestabilitou, najmä v dôsledku vojny na Ukrajine a rastúcej zložitosti bezpečnostných hrozieb, ako aj následkami zmeny klímy, ako je nárast nezvyčajných klimatických udalostí alebo nedostatok vody, musí Slovenská republika zostať ostrážitá a neustále sa prispôsobovať. Z týchto dôvodov je zákon č. 45/2011 Z. z. o kritickej infraštruktúre, ktorý vymedzoval ochranu len prvkov kritickej infraštruktúry už prekonaný.

Súčasný zákon sa zaoberá len problematikou identifikácie kritickej infraštruktúry z hľadiska hospodárskych záujmov SR. Ustanovuje organizáciu a pôsobnosť iba orgánov štátnej správy na úseku kritickej infraštruktúry. Neustanovuje nástroje na ochranu prvkov. Nezaoberá sa problematikou odolnosti prvkov, čo je v súčasnosti jednou z hlavných problematík, ktorou by sa mala právna úprava zákona zaoberať, pretože sa nachádzame v dobe, kedy sa frekvencia výskytu mimoriadnych udalostí a incidentov výrazne zvýšila a tým sa priamoúmerne zintenzívnilo možné ohrozenie nielen života, zdravia, bezpečnosti a majetku obyvateľov, životného prostredia, ale aj fungovania štátu. Proces určovania neustanovuje jednoznačné postupy identifikácie prvkov či záväzné kritériá pre určenie prvkov. Ďalej proces posudzovania neustanovuje jednotnú metodiku hodnotenia rizík a postupy odolnosti, proces zabezpečenia neustanovuje opatrenia na zvládanie rizika a opatrenia na posilňovanie odolnosti. Neustanovuje pravidelnosť termínov týkajúci sa napr. aktualizácie koncepcie a analýzy rizík sektora (ústredný orgán ju spravidla vykoná, keďže nie je presne definované, v akých prípadoch je daná aktualizáciu potrebné vykonať) a pod.

V roku 2020 na základe údajov z Analýzy územia SR a konzultácií s príslušnými ústrednými orgánmi štátnej správy bol vytvorený Register hrozieb SR 2020 v kontexte civilnej ochrany. Obsahuje 62 hrozieb, ktoré boli identifikované spravidla na lokálnej alebo regionálnej úrovni. Každá hrozba má priradeného gestora a prípadného spolugestora. Spravidla ide o ústredné orgány štátnej správy, ktoré v rozsahu svojej pôsobnosti vedú prehľady zdrojov rizík majúcich tendenciu spôsobiť krízovú situáciu, analyzujú tieto riziká a prijímajú opatrenia na odstránenie ich príčin. Register hrozieb SR 2020 bol nahradený Národným registrom hrozieb, ktorý tvorí prílohu č. 1 k Národnej stratégii riadenia rizík bezpečnostných hrozieb Slovenskej republiky, schválenej uznesením vlády Slovenskej republiky č. 65/2022.

Dokument Národná stratégia riadenia rizík bezpečnostných hrozieb SR považuje v rámci hodnotenia súčasných a dlhodobých hrozieb a krízových situácií zraniteľnosť kritickej infraštruktúry v spojení s hrozbami v oblasti energetiky, informačnej a komunikačnej infraštruktúry za závažné nebezpečenstvo. Stratégia navrhuje v súvislosti s potenciálnou

zraniteľnosťou infraštruktúry, dodávkami potravín, liekov a základných služieb pre občanov komunikovať s gestorm hrozieb kybernetickej bezpečnosti, najmä s Národným bezpečnostným úradom. Dokument používa termín kritická infraštruktúra, ktorý dopĺňa terminológiou strategická a kľúčová infraštruktúra. Vo význame sa však jedná o jednotlivé prvky kritickej infraštruktúry podľa vymedzenia pojmov v zákone č. 45/2011 Z. z. o kritickej infraštruktúre. V zhrnutí prognózovania hrozieb z hľadiska dlhodobých rizík stratégia konštatuje, že v súvislosti so zmenou klímy budú riziká ohrozenia obyvateľstva a kritickej infraštruktúry len narastať. Stratégia akcentuje na potrebu investovať do systémov prognózy a analýzy trendov a do zabezpečenia včasného varovania a vyrozumienia obyvateľstva, do opatrení, ochranných a typových plánov a záchranných a monitorovacích modulov. Vzhľadom na vyššie uvedené je zrejmé, že týmto kľúčovým hrozbám je nutné venovať zvýšenú pozornosť na všetkých stupňoch verejnej správy, vertikálnej aj horizontálnej úrovni, a pri prijímaní opatrení na znižovanie rizika ich výskytu je potrebné zapájať výkonné zložky, súkromný sektor, akademickú obec, občiansku spoločnosť vrátane mimovládnych organizácií, dobrovoľníkov, médií a samotného obyvateľstva.

Vychádzajúc z doterajších skúseností, dostupných informácií a zaznamenaných trendov je možné predpokladať, že v nasledujúcom období bude celkové dianie ovplyvnené doznením pandémie COVID-19, ako aj neistotou vyplývajúcou z vojny na Ukrajine a na to nadväzujúcej vysokej miery inflácie a dôsledkami ekonomickej stagnácie, ktorá bude mať negatívny dopad na celkovú finančnú situáciu. V tomto slede udalostí vzniká vyššia miera konzistentnosti po potrebe, že občania spoločnosti a aj orgány štátnej správy sa spoliehajú na kritickú infraštruktúru z dôvodu zabezpečenia základných služieb, ktoré poskytujú subjekty prevádzkujúce takúto infraštruktúru. Takéto služby sú kľúčové pre zachovanie životne dôležitých spoločenských funkcií, hospodárskych činností, verejného zdravia, bezpečnosti alebo životného prostredia a na vnútornom trhu majú byť poskytované nerušeným spôsobom. Preto vzhľadom na význam týchto základných služieb pre vnútorný trh a z toho vyplývajúcu potrebu zvýšiť odolnosť kritickej infraštruktúry, v širšom zmysle zabezpečiť odolnosť kritických subjektov poskytujúcich tieto služby, musí Slovenská republika prijať opatrenia na posilnenie takejto odolnosti a zmiernenie akýchkoľvek narušení pri poskytovaní takýchto základných služieb. Takéto narušenia môžu mať inak vážne dôsledky nielen pre občanov Slovenskej republiky, ale aj Európskej únie, nášho hospodárstva a dôveru v náš demokratický systém, kde hrozby môžu ovplyvniť fungovanie vnútorného trhu, najmä v kontexte rastúcej vzájomnej závislosti medzi sektormi vnútri štátu aj cezhranične.

V čoraz viac prepojenom svete sa stala odolnosť voči hrozbám pre bezpečnostné prostredie prvoradou. Bezpečnostné prostredie zahŕňa rôzne kritické aspekty vrátane fyzickej infraštruktúry, informačných systémov, personálu a citlivých údajov. Ochrana tohto prostredia si vyžaduje komplexný prístup, ktorý rieši potenciálne hrozby a zraniteľnosti. V predkladanom návrhu zákona sa posudzujú rizika a význam odolnosti kritických subjektov, ktoré prostredníctvom ochrany svojich kritických infraštruktúr kontinuálne zabezpečujú poskytovanie základných služieb.

Bezpečnostné prostredie a posudzovanie rizík zahŕňa všetky prvky, ktoré prispievajú k odolnosti kritických subjektov a stabilite poskytovania základných služieb. Patria sem fyzické aktíva, ako sú budovy, zariadenia a vybavenie, ako aj nehmotné aktíva, ako sú informácie, údaje a personál. Uvedomenie si vzájomnej prepojenosti týchto prvkov je kľúčové pre vypracovanie účinných bezpečnostných opatrení.

To zahŕňa vykonanie komplexného hodnotenia rizík s cieľom posúdiť vnútorné aj vonkajšie faktory, ktoré môžu predstavovať riziká. Hrozby môžu siahať od fyzických narušení, kybernetických útokov a prírodných katastrof až po vnútorné hrozby a neoprávnený prístup. Medzi zraniteľnosti môžu patriť zastarané bezpečnostné systémy, slabé kontroly prístupu a nedostatočné školenia.

Fyzické bezpečnostné opatrenia zohrávajú dôležitú úlohu pri ochrane bezpečnostného prostredia pôsobnosti kritických subjektov. Systémy kontroly prístupu, monitorovacie kamery a bezpečné skladovacie priestory pomáhajú zabrániť neoprávnenému prístupu a odradiť potenciálne hrozby. Pravidelná údržba a kontroly fyzickej infraštruktúry sú potrebné na včasnú identifikáciu a riešenie zraniteľných miest. Vypracovanie komplexných bezpečnostných plánov je kľúčové na minimalizovanie vplyvu narušenia bezpečnosti alebo neočakávaných udalostí. Mali by sa zaviesť minimálne sektorové opatrenia na zabezpečenie odolnosti kritických subjektov, najmä postupy reakcie na incidenty, plány zálohovania a obnovy, stratégie kontinuity poskytovania základných služieb, ktoré by sa mali pravidelne testovať z dôvodu zabezpečenia ich účinnosti.

Navrhovaný zákon má priame väzby a je v súlade s ostatnými legislatívnymi zámermi v oblasti zvýšenia odolnosti civilnej ochrany, priamych zahraničných investícií, kybernetickej bezpečnosti, *acquis* v oblasti finančných služieb a posilnenia odolnosti a zníženia zraniteľností na zmenu klímy. Návrh je predovšetkým v úzkom súlade a vytvára úzke synergie s navrhovanou smernicou o kybernetickej bezpečnosti, ktorej cieľom je zvýšiť odolnosť informačných a komunikačných technológií „kľúčových subjektov“ a „dôležitých subjektov“, ktoré spĺňajú konkrétne prahové hodnoty vo veľkom počte odvetví, proti všetkým nebezpečenstvám. Cieľom tohto návrhu je zabezpečiť, aby ústredné orgány určené podľa tohto zákona a orgány určené podľa zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti prijali doplnkové opatrenia a podľa potreby si vymieňali informácie, pokiaľ ide o kybernetickú a nekybernetickú odolnosť, a aby subjekty, ktoré sa podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti považujú za „kľúčové“, takisto podliehali povinnostiam súvisiacim so všeobecnejším zvyšovaním odolnosti s cieľom riešiť nekybernetické riziká. Fyzická bezpečnosť sietí a informačných systémov subjektov v sektore digitálnej infraštruktúry sa komplexne rieši v smernici Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) ako súčasť povinností týchto subjektov v oblasti riadenia kybernetických rizík a oznamovania. Návrh okrem toho vychádza z existujúceho *acquis* v oblasti finančných služieb, v ktorom sa stanovujú komplexné požiadavky na finančné subjekty, pokiaľ ide o riadenie prevádzkových rizík a zaistenie kontinuity činností. Preto by sa so subjektmi pôsobiacimi v sektore digitálnej infraštruktúry a financií malo na účely povinností a činností zaobchádzať ako so subjektmi, ktoré sú rovnocenné kritickým subjektom podľa tejto smernice (EÚ) 2022/2557, pričom z tejto smernice by pre tieto subjekty nevyplývali dodatočné povinnosti.

V závislosti od jednotlivých sektorov je potrebné v rámci sektora energetiky zdôvodniť špecifiká podsektora jadrová energetika a to konkrétne metód výroby a prenosu elektrickej energie (pokiaľ ide o dodávku elektrickej energie). Rozumie sa, že ak je to vhodné, výroba elektrickej energie môže zahŕňať časti jadrových elektrární, ktoré slúžia na prenos elektrickej energie, ale výslovne sú z nej vylúčené jadrové prvky, na ktoré sa vzťahujú zmluvy a právo Únie vrátane príslušných právnych aktov Únie týkajúcich sa jadrovej energie.“ Takýmito právnymi predpismi je jednak Zmluva o založení európskeho spoločenstva pre atómovú energiu

(Zmluva Euratom) a smernice vydané na jej základe. Smernice sú plne transponované do slovenskej legislatívy. A práve preto zastávame názor, že je dôležité, aby jadrové zariadenia boli explicitne zaradené aj ako kategórie subjektov kritickej infraštruktúry a vzťahovala sa na nich časť povinností vyplývajúcich z navrhovaného zákona. Tieto povinnosti majú za cieľ zvyšovať úroveň odolnosti a povinnosť informovať o všetkých incidentoch v týchto zariadeniach. Na prevádzku jadrových zariadení sa plne vzťahuje aj znenie § 2 písm. b) tohto návrhu zákona, ako na kritický subjekt s poskytovaním základnej služby.

Ďalším opatrením na zabezpečenie odolnosti kritických subjektov je otázka personálnej bezpečnosti. Kvalifikovaný personál môže byť v kritických subjektoch prínosom a zároveň potenciálnou zraniteľnosťou. Zavedenie opatrení personálnej bezpečnosti, ako sú napríklad preverenie zamestnancov, protokoly kontroly prístupu a školenia o bezpečnostnom povedomí, zabezpečuje, že osoby zapojené do systému sú dôveryhodné a spoľahlivé. Personál, ktorý má zabezpečený priamy alebo diaľkový prístup do priestorov kritického subjektu ku kritickej infraštruktúre, k limitovaným informáciám alebo ku kontrolným systémom musí byť preverený a bezúhonný. Za bezúhonnú osobu sa na účely tohto zákona považuje fyzická osoba, ktorá nebola právoplatne odsúdená za úmyselný trestný čin.

Zraniteľnosť, ktorá na úseku kritickej infraštruktúry nebola niekoľko rokov riešená je ochrana citlivých informácií zavedená v § 12 zákona č. 45/2011 Z. z. o kritickej infraštruktúre. Zákonné normy SR chránia oprávnené záujmy prostredníctvom ochrany určitých kategórií informácií. Pokrytá je oblasť utajovaných skutočností, oblasť ochrany osobných údajov, obchodného tajomstva, no ochrana citlivých informácií nie je dostatočne rozpracovaná. Tento nedokonalý stav problematiky citlivých informácií, zapríčinil zvýšený stupeň latentného pohľadu na význam a obsah informácií, čo má v danom prípade priamy vplyv na bezpečnosť. Keďže zákonné normy SR neobsahujú zoznamy explicitne vyjadrených skutočností, ktoré sú citlivou informáciou (s výnimkou zoznamov utajovaných skutočností predpísaných zákonom č. 215/2004 Z. z. v znení neskorších predpisov), v predkladanom návrhu zákona zavádzame pojem limitovanej informácie, ktorý nahrádza práve opomínaný rozsah citlivých informácií.

Ďalším aspektom reakcie na bezpečnostné prostredie je vytvorenie systému zdieľania informácií a spolupráce. Návrh zákona zavádza povinnosť nahlasovania incidentov na úseku kritickej infraštruktúry kritickými subjektmi a následne zdieľania informácií s príslušnými sektorovými ministerstvami, ministerstvom vnútra a ďalšími bezpečnostnými zložkami štátu. Ministerstvo vnútra SR ako predkladateľ tohto návrhu zákona bude plniť úlohy jednotného kontaktného bodu pre kritickú infraštruktúru SR a zároveň notifikačné a komunikačné povinnosti voči Európskej komisii. Vytvorenie komunikačných kanálov na nahlasovanie bezpečnostných incidentov podporuje proaktívny a koordinovaný prístup k celkovej odolnosti.

Tieto kroky sú nevyhnutné na udržiavanie aktuálnych informácií o nových hrozbách a osvedčených postupoch. Odolnosť v bezpečnostnom prostredí je nepretržitý proces. Pravidelné monitorovanie, kontroly a revízie bezpečnostných opatrení a postupov sú potrebné na identifikáciu oblastí, ktoré je potrebné zlepšiť, a na prispôsobenie sa novým hrozbám. Kľúčom k udržaniu spoľahlivého bezpečnostného prostredia je zostať proaktívny a reagovať na vyvíjajúce sa bezpečnostné výzvy.

Na dosiahnutie vyššie uvedených cieľov sa preto navrhuje v zákone o kritickej infraštruktúre a doplnení niektorých zákonov stanovenie priorít celkovej odolnosti, ktorými

môžu kritické subjekty zmierniť riziká, ochrániť kritické aktíva a udržať bezpečné a stabilné prevádzkové prostredie.

Návrh zákona je v súlade s Ústavou Slovenskej republiky, s ústavnými zákonmi a nálezmi Ústavného súdu Slovenskej republiky, so zákonmi a ostatnými všeobecne záväznými právnymi predpismi platnými v Slovenskej republike, s medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, ako aj s právom Európskej únie.

Prijatie navrhovaného zákona nemá negatívne vplyvy na rozpočet verejnej správy, nemá vplyvy na životné prostredie, vplyvy na služby verejnej správy pre občana, vplyvy na informatizáciu spoločnosti, vplyvy na manželstvo, rodičovstvo a rodinu, ale bude mať pozitívne vplyvy a negatívne vplyvy na podnikateľské prostredie a pozitívne sociálne vplyvy.

Návrh zákona nie je predmetom vnútrokomunitárneho pripomienkového konania.

## **DÔVODOVÁ SPRÁVA**

### **B. Osobitná časť**

#### **Čl. I**

#### **K § 1**

Jednotlivé ustanovenia upravujú predmet a pôsobnosť zákona, kde sa vymedzuje najmä organizácia, pôsobnosť a povinnosti orgánov štátnej správy na úseku kritickej infraštruktúry. Určuje sa postup pri identifikovaní kritických subjektov a kritických subjektov osobitného európskeho významu, ako aj postavenie a povinnosti kritických subjektov pri zabezpečovaní odolnosti kritickej infraštruktúry a zabezpečovaní nepretržitého poskytovania základných služieb.

Zákon ďalej pojednáva o povinnostiach a opatreniach na zabezpečenie odolnosti kritickej infraštruktúry, čo znamená schopnosť týchto systémov a služieb odolávať incidentom a udalostiam s cieľom zabezpečiť nepretržité poskytovanie nevyhnutných základných služieb, ktoré sú životne dôležité a majú zásadný význam pre spoločnosť a hospodárstvo.

Ďalším dôležitým aspektom je stanovenie zodpovednosti za porušenie povinností podľa tohto zákona. V jednotlivých ustanoveniach sa jasne vymedzujú sankcie za nedodržiavanie opatrení a povinností stanovených pre kritické subjekty, čo má za cieľ zabezpečiť dodržiavanie potrebných noriem bezpečnosti, aby dosiahli vysokú mieru odolnosti týchto subjektov.

V neposlednom rade zákon rieši aj funkciu kontroly a dohľadu vo vzťahu k dodržiavaniu zákona. Stanovujú sa mechanizmy, ktoré príslušným orgánom umožňujú vykonávať pravidelný dohľad prostredníctvom rôznych kontrolných činností, a to aj formou auditov s cieľom

zabezpečiť transparentnosť a dodržiavanie všetkých príslušných predpisov a noriem týkajúcich sa kritickej infraštruktúry.

V zákone sú uvedené aj výnimky, na ktoré sa jeho pôsobnosť nevzťahuje. Predkladaný zákon sa nevzťahuje na kritické subjekty v sektore vesmír, ktoré prevádzkujú infraštruktúru, ktorú vlastní, spravuje alebo prevádzkuje Európska únia alebo v jej mene v rámci svojho vesmírneho programu. Výnimkou sú subjekty verejnej správy v oblasti obrany Slovenskej republiky, vyšetrovanie, odhaľovanie a stíhanie trestných činov. Ďalšou výnimkou sú aj platobné systémy a systémy zúčtovania a vyrovnaní cenných papierov a ich infraštruktúry dohliadané alebo prevádzkované Európskou centrálnou bankou alebo Eurosystemom.

## K § 2

V § 2 zákona, ktorý sa zaoberá definíciou základných pojmov, sa uvádza, čo presne sa rozumie pod pojmami uvedenými v zákone, aby sa zabezpečil jasný a jednotný výklad pojmov, ktorých sa zákon týka. Toto rozsiahle a podrobné vymedzenie kľúčových pojmov a definícií odráža snahu o dôkladné vypracovanie právnych predpisov na základe správnej transpozície smernice (EÚ) 2022/2557.

Transponovaná smernica (EÚ) 2022/2557 zrušuje smernicu Rady 2008/114/ES, ktorá charakterizuje kritickú infraštruktúru ako zložku, systém alebo ich časť, ktorá je nevyhnutná pre zachovanie základných funkcií spoločnosti, zdravia, ochrany, bezpečnosti, kvality života obyvateľov z ekonomického a sociálneho hľadiska, a ktorej narušenie alebo zničenie by malo závažné dôsledky v členskom štáte z dôvodu nemožnosti zachovať tieto nevyhnutné funkcie. Podľa § 2 zákona č. 45/2011 Z. z. o kritickej infraštruktúre pri ochrane prvku kritickej infraštruktúry tohto zákona sa prvkom kritickej infraštruktúry rozumie najmä inžinierska stavba, služba vo verejnom záujme a informačný systém v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé, dokonca až devastačné dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým následne aj priamo na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia.

Nový pojem kritická infraštruktúra podľa smernice (EÚ) 2022/2557 predstavuje odklon od fyzickej ochrany prvku k zaisteniu kontinuálneho poskytovania základnej služby. Nový pojem tak predstavuje aktívum, zariadenie, vybavenie a systém (alebo ich časti), ktoré sú nevyhnutné na poskytovanie základnej služby.

Smernicou (EÚ) 2022/2557 z dôvodu previazanosti kritickej infraštruktúry<sup>1</sup> na základnú službu, na rozdiel od súčasného určenia prvkov, dochádza k posunu určenia a ochrany kritickej infraštruktúry samotným kritickým subjektom. Samotný kritický subjekt vymedzí kritickú infraštruktúru pri prijímaní (vlastných) opatrení na zabezpečenie odolnosti kritickej infraštruktúry podľa § 10.

Zameranie sa presúva z ochrany kritickej infraštruktúry na širšiu koncepciu odolnosti kritických subjektov prevádzkujúcich takúto kritickú infraštruktúru, ktorá sa vzťahuje na obdobie pred incidentom, počas neho a aj po ňom.

---

<sup>1</sup> Okrem toho by sa pojem „kritická infraštruktúra“ mal chápať rovnakým spôsobom, ako sa uvádza v odôvodnení 7 odporúčania 2023/C 20/01, t. j. ako pojem, ktorý zahŕňa relevantnú kritickú infraštruktúru identifikovanú členským štátom na vnútroštátnej úrovni alebo označenú za európsku kritickú infraštruktúru podľa smernice 2008/114/ES, ako aj kritické subjekty, ktoré sa identifikujú podľa smernice (EÚ) 2022/2557.

Pojem „odolnosť“, vymedzený v článku 2 bode 2 smernice (EÚ) 2022/2557, by sa mal chápať aj ako schopnosť kritickej infraštruktúry predchádzať udalostiam, ktoré výrazne narušajú alebo môžu významne narušiť poskytovanie základných služieb kritickým subjektom, t. j. služieb, ktoré sú kľúčové pre zachovanie nevyhnutných spoločenských a hospodárskych funkcií, verejnú bezpečnosť a ochranu, zdravie obyvateľstva alebo životné prostredie, chrániť pred takýmito udalosťami, reagovať na ne, odolávať im, zmierňovať ich, absorbovať ich, prispôbovať sa im alebo zotaviť sa z nich.

Základná služba<sup>2</sup> je nový pojem, ktorý prináša/zavádza smernica (EÚ) 2022/2557 do národnej legislatívy. Základné služby sú podľa smernice (EÚ) 2022/2557 kľúčové pre zachovanie životne dôležitých spoločenských funkcií, hospodárskych činností, verejného zdravia a bezpečnosti alebo životného prostredia a musia sa poskytovať neprerušeným spôsobom. Preto vzhľadom na význam týchto základných služieb pre trh a z toho vyplývajúcu potrebu zvýšiť odolnosť kritickej infraštruktúry je nevyhnutné zabezpečiť odolnosť kritických subjektov poskytujúcich tieto služby. Je potrebné prijať opatrenia na posilnenie takejto odolnosti a zmiernenie akýchkoľvek narušení pri poskytovaní takýchto základných služieb. V opačnom prípade môžu mať takéto narušenia vážne dôsledky pre občanov, naše hospodárstvo, dôveru v demokratický systém a môžu ovplyvniť fungovanie trhu, najmä v kontexte rastúcej vzájomnej závislosti medzi sektormi a aj cezhranične. Základné služby sú uvedené v prílohe č. 1. Nie každý poskytovateľ základnej služby bude aj kritickým subjektom, ale len taký, ktorý bude na základe zákona identifikovaný ako kritický subjekt a to priamo ústredným orgánom. Zákon neustanovuje ohlasovaciu povinnosť ani povinnosť pre kritické subjekty, aby sa „samoidentifikovali“.

Smernica (EÚ) 2022/2557 stanovuje do legislatívy určité povinnosti oznamovania incidentov v prípade, že incident<sup>3</sup> má alebo by mohol mať významný vplyv na kritické subjekty a kontinuitu poskytovania základných služieb. Incidenty, ktoré narušajú kritickú infraštruktúru alebo poskytovanie základných služieb kritickými subjektmi, podľa návrhu dosahujú prahovú hodnotu významného incidentu, ktorú si určia (a v prípade potreby aktualizujú) ústredné orgány v posúdení rizika ústredným orgánom podľa § 8 ods. 3 písm. e), pre každý sektor a podsektor. Kritický subjekt bude oboznámený s týmito prahovými hodnotami za účelom hlásenia incidentov. Spôsob a rozsah hlásenia incidentov ústrednému orgánu je bližšie upravený v § 14.

Ďalším pojmom je definícia posúdenia rizika podľa smernice (EÚ) 2022/2557. Aby boli kritické subjekty schopné zabezpečiť svoju odolnosť, mali by mať prehľad a znalosti o všetkých relevantných rizikách, ktorým sú vystavené, a mali by tieto riziká analyzovať. Na tento účel by mali vykonávať posúdenie rizík vždy, keď je to potrebné vzhľadom na ich osobitnú situáciu a vývoj predmetných rizík, v každom prípade však každé štyri roky. Posúdenia rizík, ktoré vykonávajú kritické subjekty, budú vychádzať z posúdenia rizika, ktoré vykonali ústredné orgány a ministerstvo vnútra.

---

<sup>2</sup> Pojem základná služba bol doteraz definovaný len v zákone č. 69/2018 Z.z. o kybernetickej bezpečnosti, kde Zákon identifikuje tri druhy základnej služby: Základná služba v zmysle transpozície smernice NIS - služba, ktorá je uvedená v prílohe č. 1 zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a ktorá spĺňa identifikačné kritériá podľa tohto zákona. Základná služba ako informačný systém verejnej správy – identifikuje sa na základe dohody s ústredným orgánom, do pôsobnosti ktorého sektor informačných systémov verejnej správy spadá. Základná služba ako prvok kritickej infraštruktúry.

<sup>3</sup> Incident je v smernici NIS 2 vymedzený ako „udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôverynosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov“ („kybernetický incident“).



Právna úprava pojmu limitovanej informácie bola inšpirovaná používaním neverejných informácií vo vzťahu k Európskej únii a Organizácii Severoatlantickej zmluvy, v ktorých majú pre tieto informácie zavedené označenie „EU LIMITÉ“, resp. „NATO UNCLASSIFIED“. Základným princípom, na ktorom je navrhovaná limitovaná informácia založená, je zásada „potreba poznať“ (z angličtiny „need-to-know“), schopnosť zachovať mlčanlivosť, znalosť pravidiel manipulácie a schopnosť ich dodržania. V dôsledku toho citlivú informáciu na úseku kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre nahradila limitovaná informácia, ktorá je plne implementovaná novelou zákona č. 215/2004 Z. z. Cieľom je poskytnúť jasné usmernenia na ochranu limitovaných informácií.

V časti o vymedzení pojmov orgán verejnej moci a oprávnená osoba sa vymedzujú úlohy a právomoci jednotlivých orgánov verejnej moci a jednotlivých oprávnených osôb v procese ochrany kritickej infraštruktúry. Tieto definície rozširujú rámec zákona o organizácii činnosti vlády a organizácii ústrednej štátnej správy, kde poskytujú ďalšie podrobnosti o povinnostiach subjektov a právnych podmienkach.

Terminológia ponúka dôkladný opis mechanických a technických bezpečnostných opatrení, ktoré zohrávajú kľúčovú úlohu pri ochrane kritickej infraštruktúry. Tie sú aktualizované podľa súčasnej odbornej literatúry a zahŕňa aj nové trendy v oblasti bezpečnostných zabezpečovacích prostriedkov. V rámci aktualizácie právnych predpisov a pravidiel na zabezpečenie odolnosti kritických subjektov sa preto kladie dôraz na integráciu nových technológií do systémov fyzicko-objektovej ochrany. Tento prístup podporuje smernica (EÚ) 2022/2557, ktorá od nás vyžaduje, aby sme neustále rozširovali a aktualizovali naše kapacity a technológie na odhaľovanie hrozieb. Konkrétne bezpečnostné opatrenia si určujú samotné kritické subjekty podľa § 10, pričom ústredné orgány môžu odporúčať minimálne opatrenia.

V rámci vymedzenia základných pojmov v zákone sa kladie osobitný dôraz na technické bezpečnostné zariadenia, ktoré zahŕňajú nielen tradičné elektronické bezpečnostné systémy, ale aj špecializované zariadenia na detekciu bezpilotných lietadiel. Tieto zariadenia sú dôležitou súčasťou ekosystému bezpečnosti kritickej infraštruktúry, keďže neoprávnený prienik bezpilotných lietadiel môže predstavovať významné riziko pre poskytovanie nevyhnutných základných služieb a ochranu limitovaných informácií.

Zahrnutie zariadení na detekciu bezpilotných lietadiel do právnych predpisov a bezpečnostných noriem týkajúcich sa kritickej infraštruktúry preto odráža rastúcu potrebu primerane reagovať na dynamicky sa vyvíjajúce hrozby a predstavuje významný krok k zaisteniu väčšej odolnosti kritických infraštruktúr a služieb, ktoré sú nevyhnutné pre fungovanie spoločnosti, hospodárstva a štátu.

## K § 3

Kompetencie orgánov štátnej správy v oblasti kritickej infraštruktúry, ako sú upravené v § 3, sú kľúčovým prvkom pre zabezpečenie kontinuálneho a bezpečného fungovania základných služieb a ich infraštruktúr potrebných pre spoločnosť a hospodárstvo. V tejto súvislosti vláda Slovenskej republiky, Ministerstvo vnútra SR spolu s niektorými ústrednými orgánmi štátnej správy, tvoria základ organizácie a riadenia kritickej infraštruktúry. Ich kompetencie a zodpovednosti v tomto sektore umožňujú integrovaný prístup k riadeniu a

ochrane kritických infraštruktúr a základných služieb, čo je nevyhnutné pre celkovú odolnosť všetkých sektorov voči potenciálnym hrozbám a výzvam.

V rámci vytvorenej štruktúry orgánov štátnej správy sa navrhuje, aby zodpovednosti za sektory kritickej infraštruktúry boli zverené predovšetkým ústredným orgánom vo svojej pôsobnosti. Táto skupina orgánov verejnej moci má za úlohu zabezpečiť primeranú ochranu všetkých sektorov kritickej infraštruktúry a zároveň využiť synergie medzi rôznymi sektormi a zabezpečiť ich odolnosti. Oproti zákonu č. 45/2011 Z. z. o kritickej infraštruktúre dochádza k decentralizácii úloh a povinností na decentralizovanú sektorovú úroveň. Ústredné orgány budú zaraďovať a vyradovať kritické subjekty, navrhovať prahové hodnoty pre identifikáciu kritických subjektov, určovať prahové hodnoty incidentov vo svojom sektore a podsektore bez koordináčnej zodpovednosti ministerstva vnútra. Ministerstvo vnútra sa v predkladanom návrhu zákona stane ústredným orgánom a zároveň bude pokrývať komunikačné úlohy. Vláda bude zohrávať rozhodovaciu úlohu v procese nastavovania kritérií pri identifikácii kritických subjektov prostredníctvom pravidelne aktualizovanej stratégie.

Navrhovaný legislatívny rámec preto považuje pôsobnosť a organizáciu orgánov štátnej správy v oblasti kritickej infraštruktúry za základné piliere, na ktorých stojí celý systém zvyšovania odolnosti a riadenia kritickej infraštruktúry. Táto navrhnutá komplexná organizácia zabezpečuje, aby Slovenská republika bola schopná čeliť súčasným a budúcim výzvam v oblasti bezpečnosti a ochrany kritickej infraštruktúry, pričom sa kladie dôraz na spoluprácu všetkých kľúčových aktérov a zapojenie rôznych úrovní štátnej správy s cieľom optimálne a efektívne riešiť potenciálne riziká a hrozby.

#### K § 4

Navrhovaná pôsobnosť vlády zodpovedá jej ústavnému postaveniu vrcholného orgánu výkonnej moci. Vláda Slovenskej republiky bude každé 4 roky schvaľovať stratégiu odolnosti kritických subjektov (ďalej len „stratégia“), ktorá je ďalej definovaná v § 7. V tejto stratégii sa stanovujú hlavné ciele, priority a úlohy na určené obdobie, ako aj určujú metódy a opatrenia na ich realizáciu a zabezpečí sa financovanie úloh vyplývajúcich z tohto zákona. Tento proces vedie k včasnému a účinnému plánovaniu na zabezpečenie odolnosti kritickej infraštruktúry voči rôznym hrozbám a incidentom, čo je nevyhnutné na zachovanie kontinuity poskytovania nevyhnutných základných služieb.

Stratégia bude obsahovať aj prahové hodnoty pre jednotlivé kritériá na identifikáciu kritických subjektov a zaradenie kritických subjektov do sektorov kritickej infraštruktúry. Rozhodnutie o tom, či sa subjekt považuje za kritický, a jeho zaradenie do príslušného sektora kritickej infraštruktúry alebo jeho vyradenie, ak už nespĺňa stanovené kritériá, bude v kompetencii ústredných orgánov štátnej správy.

Zákon preto kladie dôraz na prípravu a schvaľovanie stratégií, ktoré sú kľúčovými krokmi na zvýšenie odolnosti kritických infraštruktúr a zabezpečenie ich funkčnosti voči potenciálnym hrozbám.

#### K § 5

V ustanovujúcich odsekoch zákon podrobne a taxatívne špecifikuje, čo všetko spadá do pôsobnosti ministerstva vnútra a jeho postavenia ako jednotného kontaktného miesta pre zabezpečenie odolnosti kritickej infraštruktúry na národnej a európskej úrovni.

Vedenie verejného a neverejného zoznamu kritických subjektov má význam pre potreby ďalšej podrobnejšej úpravy počas krízových stavov vrátane financovania potrebných výziev a programov. Pandémia spôsobená vírusom COVID-19 odhalila medzery v reakčných schopnostiach štátu aj na úseku kritickej infraštruktúry. Na tento účel slúži vedenie verejných a neverejných zoznamov kritických subjektov. Verejný zoznam umožňuje transparentnosť a poskytuje cenné informácie o odvetviach a subjektoch, ktoré sa považujú za kritické pre štát a jeho občanov. Na druhej strane neverejný zoznam obsahuje limitované informácie, ktorých odtajnenie by mohlo ohroziť bezpečnosť štátu alebo príslušnej infraštruktúry. Táto dualita zabezpečuje, aby štát mohol účinne chrániť kritické subjekty a infraštruktúry a reagovať na ich potreby.

Pandémia COVID-19 však poukázala na nemožnosť vytvoriť selektívne opatrenia na úseku kritickej infraštruktúry, pretože celý jej zoznam a údaje boli neverejné a v rámci existujúcej legislatívy citlivých informácií sa táto skutočnosť ukázala ako dvojsečná v súvislosti so zabezpečením ochrany a prioritizácie kritických zamestnancov v jednotlivých sektoroch.

V dôsledku uvedených skúseností je potrebné prehodnotiť a optimalizovať proces vedenia zoznamov a údajov kritických subjektov. To zahŕňa nielen revíziu limitovaných informácií do zoznamov, ale aj zabezpečenie toho, aby bol systém flexibilný a dynamický, čo mu umožní rýchlo sa prispôbiť meniacim sa podmienkam a výzvam.

Prioritou by malo byť zavedenie a prispôbenie výziev na kritickú infraštruktúru, ako aj financovanie programov zameraných na zvýšenie odolnosti kritických subjektov. To si vyžaduje koordinovaný prístup medzi prioritami vlády a sektormi súkromného sektora, ako aj medzinárodnú spoluprácu.

Pandémia tak poskytla dôležitú lekciu o význame pripravenosti a flexibility pri riadení kritickej infraštruktúry a zdôraznila potrebu pružnej reakcie na krízy a efektívneho využívania verejných a neverejných zoznamov kritických subjektov.

Ďalej sa v tomto paragrafe podrobne uvádzajú úlohy a povinnosti ministerstva vnútra s dôrazom na spoluprácu s ústrednými orgánmi pri vypracúvaní stratégie kritickej infraštruktúry, identifikáciu a rozsah potrebných limitovaných informácií. Osobitná pozornosť je venovaná správe a aktualizácii verejného a neverejného zoznamu kritických subjektov, ktorý zahŕňa nielen identifikáciu subjektov a základných služieb podľa prílohy č. 1, ale aj proces nahlasovania incidentov, ktoré môžu alebo majú významný vplyv na poskytovanie základnej služby.

V nadväznosti na túto podrobnú úpravu úseku kritickej infraštruktúry získava ministerstvo vnútra dôležitú úlohu vo výkonnej štruktúre štátnej správy a rovnako nemenej dôležitá je jeho spolupráca s Európskou komisiou a členskými štátmi EÚ, výmena informácií o schválených stratégiách, realizovaných opatreniach či incidentoch. Takýto prístup umožňuje lepšiu pripravenosť na možné mimoriadne situácie a vytvára priestor pre medzinárodnú spoluprácu a koordináciu pri riešení potenciálnych hrozieb. V súlade s článkom 19 Smernice (EÚ) 2022/2557 sa zriaďuje Skupina pre odolnosť kritických subjektov, ktorá podporuje

Komisiu a uľahčuje spoluprácu a výmenu informácií medzi členskými štátmi o otázkach týkajúcej sa Smernice (EÚ) 2022/2557. Skladá sa zo zástupcov Komisie a členských štátov, pričom môže vyzvať zainteresované strany, aby sa zúčastnili na jej práci, a rovnako ak o to požiada Európsky parlament sa na jej práci môžu podieľať aj experti Európskeho parlamentu. Jednotlivé úlohy Skupiny pre odolnosť kritických subjektov bližšie upravuje Smernica (EÚ) 2022/2557, najmä jej článok 19.

Zákon hovorí aj o dôležitosti vytvárania partnerstiev na národnej a medzinárodnej úrovni, ktoré by mali významne prispieť k zabezpečeniu vyššej odolnosti kritickej infraštruktúry a jej kritických subjektov. Partnerský prístup a spolupráca medzi rôznymi orgánmi a inštitúciami poskytuje príležitosti na výmenu osvedčených postupov, skúseností a doplnkových kapacít, ktoré môžu pomôcť pri rýchlej reakcii v reálnom čase na vznikajúce situácie a hrozby.

Navrhovaný paragraf celkovo predstavuje kľúčové legislatívne opatrenia a povinnosti ministerstva vnútra zamerané na ochranu a zabezpečenie odolnosti kritickej infraštruktúry a jej kritických subjektov.

## K § 6

V § 6 zákona je taxatívne vymedzená pôsobnosť príslušných ministerstiev a ostatných ústredných orgánov štátnej správy na úseku kritickej infraštruktúry. Tieto ústredné orgány štátnej správy budú vykonávať štátnu správu vrátane kontrolnej činnosti v oblasti kritickej infraštruktúry v rámci svojej pôsobnosti, najmä vo vzťahu k opatreniam na zabezpečenie odolnosti kritických subjektov. Ústredný orgán štátnej správy pre kritickú infraštruktúru sa v rámci sektora a podsektora, pre ktorý je príslušný, podieľa na vypracovaní stratégie, navrhuje kritériá pre identifikáciu kritických subjektov po vykonaní konzultácií so združeniami podnikateľov, hodnotí riziká v sektore a podsektore podľa prílohy č. 1, vrátane určovania prahových hodnôt pre hlásenie incidentov. Posudzuje riziká kritických subjektov pre príslušné sektory a podsektory podľa tej istej prílohy, ktoré priamo súvisia s poskytovaním základnej služby, a svoje závery predkladá ministerstvu vnútra s cieľom vypracovať, sumarizovať, posúdenie rizík na národnej úrovni a koncipovať návrh stratégie.

Ústredné orgány štátnej správy v rámci tzv. decentralizácie zároveň identifikujú kritické subjekty a ich zaradenie alebo vyradenie zo sektora a podsektora podľa prílohy č. 1 a informujú kritický subjekt o tom, že bol identifikovaný ako kritický subjekt resp. vyradený zo sektora a podsektora podľa prílohy č. 1. O identifikácii kritického subjektu a jeho zaradení a vyradení zo sektora a podsektora podľa prílohy č. 1 informuje ústredný orgán ministerstvo vnútra. Zároveň vedie neverejnú časť zoznamu identifikovaných kritických subjektov v stanovenom rozsahu.

Ústredný orgán priebežne kontroluje zoznam kritických subjektov a bezodkladne oznamuje každú zmenu v zozname kritických subjektov ministerstvu vnútra. Odporúča minimálne bezpečnostné opatrenia na zvýšenie odolnosti kritických subjektov vo svojom sektore a podsektore, ako je uvedené v prílohe č. 1, vrátane používania noriem a technických špecifikácií vhodných pre kritické subjekty. Posudzuje a vyhodnocuje prijaté bezpečnostné plány kritických subjektov na zabezpečenie odolnosti kritických subjektov pri zohľadnení rizík kritického subjektu a rizík ústredného orgánu. Zúčastňuje sa na vytváraní národných a medzinárodných partnerstiev v oblasti kritickej infraštruktúry a podporuje ich s cieľom

zabezpečiť ochranu a tým aj zvýšenú odolnosť kritickej infraštruktúry a jej kritických subjektov.

Pri odporúčaní minimálnych opatrení na zabezpečenie odolnosti kritického subjektu ústredným orgánom podľa § 6 písm. i) budú ústredné orgány dbať o primerané prehlbovanie povinností vlastníka len vo vzťahu k jeho kritickej infraštruktúre z dôvodu zabezpečenia odolnosti kritickej infraštruktúry a zabezpečenia poskytovania základnej služby.

## K § 7

Smernica (EÚ) 2022/2557 zaväzuje členské štáty Európskej únie, aby prijali stratégiu zameranú na zvýšenie odolnosti kritických subjektov. Cieľom tejto stratégie je zabezpečiť ochranu kontinuity poskytovania nevyhnutných základných služieb a odolnosť kritických subjektov, ktoré ich prevádzkujú cez svoje infraštruktúry. Predkladaný návrh zákona ustanovuje do stratégie najdôležitejší mechanizmus a to proces, ktorým sa kritické subjekty identifikujú, vrátane určenia prahových hodnôt významnosti vplyvu (podľa § 14 ods. 3 pre každý sektor a podsektor a pre každú základnú službu podľa prílohy č. 1). Jednotlivé prahové hodnoty, kritéria významnosti vplyvu, v procese tvorby stratégie navrhujú ústredné orgány samy, pričom ale ústredné orgány budú vykonávať konzultácie so združeniami podnikateľov. Tie sa vykonajú za účelom kvalitného nastavenia kritérií, získania postojov a stanovísk od dotknutých subjektov. Vybrané kritéria s údajmi o prahovej hodnote tvoria limitovanú informáciu a môžu tvoriť utajovanú skutočnosť. Tieto údaje sa budú aktualizovať spoločne so stratégiou.

V nadväznosti na historický vývoj v oblasti kritickej infraštruktúry, ktorá bola v minulosti na Slovensku často okrajovým záujmom, predstavuje súčasný rámec výrazný posun. Pravidelné aktualizácie, ktoré sú už stanovené v právnych predpisoch, každé štyri roky zabezpečujú, že stratégia pružne reaguje na meniace sa hrozby a potreby.

V stratégii vypracovanej na základe smernice sa kľúčové body podrobne vymedzujú ako strategické ciele a priority na zvýšenie odolnosti, a to aj pri zohľadnení cezhraničnej a sektorovej závislosti. Rámec riadenia, opatrenia na posilnenie odolnosti kritických subjektov, proces identifikácie kritických subjektov, podpora kritických subjektov a zapojenie verejného a súkromného sektora sú kľúčovými prvkami na zabezpečenie odolnosti. Okrem toho sa v stratégii bude popisovať systém koordinácie medzi rôznymi štátnymi orgánmi na výmenu informácií o kybernetických a nekybernetických rizikách a opatreniach na podporu malých a stredných podnikov definovaných ako potenciálne budúce kritické subjekty.

Porovnanie s históriou koncepcie kritickej infraštruktúry na Slovensku ukazuje, že súčasné legislatívne zmeny zamerané na posilnenie odolnosti kritických infraštruktúr majú za cieľ prekonať predchádzajúci pasívny prístup a zaviesť dynamický systém plánovania a reakcie na hrozby. Tento posun odráža nielen rastúci význam ochrany a obrany na úseku kritickej infraštruktúry v globálne prepojenom prostredí, ale tiež demonštruje zvýšené povedomie o potrebe komplexnej odolnosti poskytovania nevyhnutných základných služieb a ich kritickú infraštruktúru.

Definíciu malých a stredných podnikov v § 7 ods.1 písm. h) obsahuje Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmov mikro, malé a stredné podniky (Ú. v. EÚ L 124, 20.5.2003).

Stratégiu vypracováva ministerstvo vnútra v spolupráci s ústrednými orgánmi. Obsah stratégie je vymedzený v odseku 1 tak, aby korešpondoval s obsahovým vymedzením smernice (EÚ) 2022/2557.

## K § 8

Opatrenia odkazované v § 10 zamerané na identifikáciu a pomoc pri zabezpečovaní odolnosti kritických subjektov by sa mali riadiť prístupom založeným na riziku. Tento prístup umožňuje efektívne zameranie úsilia na tie kritické subjekty, ktoré sú najdôležitejšie z hľadiska zabezpečovania životne dôležitých spoločenských funkcií alebo hospodárskych činností. Kľúčovým krokom k zabezpečeniu takéhoto cieleného prístupu je vykonávanie posúdení rizík zo strany ústredných orgánov vo svojich sektorových pôsobnostiach, pričom zohľadňujú všetky relevantné prírodné javy a riziká spojené s ľudskou činnosťou - ako sú nehody, prírodné katastrofy, hrozby pre verejné zdravie typu pandémie a antagonistické hrozby vrátane teroristických činov. Dôležitou súčasťou tohto procesu je tiež zohľadnenie existujúcich sektorových alebo všeobecných posúdení rizík, ktoré boli vykonané na základe iných právnych aktov EÚ.

Výsledky posúdení rizík poskytujú podstatný základ nielen pre identifikáciu kritických subjektov, ale aj pre usmerňovanie týchto subjektov v procese plnenia ich legislatívnych povinností. Ide o to, že kritické subjekty by mali byť informované o všetkých relevantných rizikách, s ktorými sa môžu stretnúť, a mali by tieto riziká pravidelne posudzovať, ideálne minimálne každé štyri roky, alebo vždy, keď to vyžaduje zmena v ich osobitnej situácii alebo v príslušných rizikách.

Zároveň, podľa § 8, ústredné orgány majú povinnosť predkladať ministerstvu vnútra správy o posúdení rizík v rámci svojich sektorov a podsektorov, pričom tieto posúdenia majú byť vykonávané podľa potreby a aspoň raz za štyri roky. V prípade rizika s významným vplyvom na poskytovanie základných služieb ústredný orgán správy o posúdení rizika predloží ministerstvu vnútra bezodkladne a rovnako jej relevantné časti sprístupní kritickému subjektu s povinnou lehotou aktualizovania bezpečnostného plánu. Tieto analýzy musia zohľadniť široké spektrum potenciálnych hrozieb a rizík vrátane tých, ktoré majú cezhraničný či medzisektorový charakter. Aj na základe týchto posúdení rizík ústredné orgány identifikujú kritické subjekty a pomáhajú im pri implementácii adekvátnych opatrení na zabezpečenie odolnosti voči identifikovaným rizikám.

V tomto kontexte, sprístupnenie relevantných častí posúdenia rizík kritickým subjektom umožňuje týmto subjektom lepšie pochopiť potenciálne riziká a zároveň ich motivuje k adekvátnej príprave a reakcii na možné hrozby. Prístup založený na riziku, jeho implementácia a následné hodnotenie sú kľúčové pre posilnenie odolnosti na úseku kritickej infraštruktúry a kritických subjektov, čím sa zabezpečuje kontinuita základných služieb nevyhnutných pre spoločnosť a hospodárstvo.

Z tohto procesu je nesmierne dôležité navrhnúť ústredným orgánom aj ďalší typ prahových hodnôt, ktoré zohľadnia kedy je incident významný pre povinnosť nahlasovania. Údaje prahových hodnôt incidentov, zohľadnia najmä počet a podiel používateľov dotknutých narušením základnej služby, ktorú kritický subjekt poskytuje, trvanie narušenia a geografické územie dotknuté narušením s prihliadnutím na to, či je toto územie geograficky izolované, a akékoľvek informácie o incidentoch oznámených podľa § 14. Ústredný orgán pri oznámení identifikovania kritického subjektu je povinný tieto údaje o prahových hodnotách incidentu

písomne oznámiť kritickému subjektu a informovať o procese hlásenia incidentov. Údaje o prahových hodnotách významnosti vplyvu pri identifikácii kritických subjektov podľa § 14 ods.3 a prahové hodnoty pre nahlasovanie incidentov podľa § 8 ods. 3 písm. e) môžu, ale aj nemusia byť totožné. Pri posúdení rizík je potrebné vziať do úvahy jednotlivé sektorové asymetrie. Prahové hodnoty incidentov v priebežnom procese posúdení rizika ústredným orgánom podliehajú režimu limitovanej informácie.

Posudzovanie rizík je kľúčovým procesom v rámci národnej stratégie riadenia rizík bezpečnostných hrozieb Slovenskej republiky. Jeho dôležitosť je dvojnásobne zvýraznená v kontexte stratégií a akčných plánov schvaľovaných na vládnej úrovni, akým je napríklad Akčný plán k Národnej stratégii riadenia rizík bezpečnostných hrozieb do roku 2025. Tento dokument predstavuje komplexný prístup k identifikácii, hodnoteniu a znižovaniu potenciálnych rizík a hrozieb, ktoré môžu ohroziť bezpečnosť a ochranu občanov Slovenskej republiky.

Bez hĺbkového pochopenia potenciálnych rizík nemôže byť akýkoľvek bezpečnostný program alebo stratégia účinná. V kontexte národnej bezpečnosti umožňuje posúdenie rizika určiť priority bezpečnostných opatrení, alokovať zdroje tam, kde sú najpotrebnejšie, a zároveň plánovať ochranu kritických infraštruktúr a dôležitých spoločenských funkcií.

Akčný plán k Národnej stratégii riadenia rizík bezpečnostných hrozieb do roku 2025 signalizuje záväzok vlády SR systematicky a komplexne pristupovať k zaistieniu bezpečnosti svojich občanov. Strategická iniciatíva zahŕňa rozvoj a implementáciu mechanizmov na znižovanie rizík vrátane kybernetických útokov, terorizmu, prírodných katastrof či hybridných hrozieb. Zaväzuje sa k nepretržitému zlepšovaniu systému civilnej ochrany a krízového riadenia, čo reflektuje integrovaný prístup k rizikám a ich riadeniu cez multisektorovú spoluprácu.

Posúdenie rizika teda v kontexte Národnej stratégie pre Slovenskú republiku predstavuje základný kameň jej snaženia vybudovať odolnú a bezpečnú spoločnosť schopnú čeliť rôznym typom hrozieb a vyvíjajúcich sa bezpečnostných výziev.

Na účely zabezpečenia úrovne a funkčnosti fyzickej ochrany jadrových zariadení a posudzovania rizík na účely opatrení na úseku fyzickej ochrany existuje od roku 2009 pracovná skupina „Hrozba jadrovým zariadením a pre jadrové materiály a jadrové zariadenia v rámci projektového ohrozenia štátu“, ktorá je zložená zo zástupcov ÚJD SR, MV SR, MO SR a SIS. Pravidelná ročná aktualizácia sa predkladá na Bezpečnostnú radu SR. Táto skupina vznikla na základe uznesenia vlády SR č. 229/2009 a pravidelne v ročnom intervale aktualizuje vyhodnotenie hrozby a v intervale cca 3 rokov pripravuje/aktualizuje projektové ohrozenie pre jadrové materiály a jadrové zariadenia, ktoré je vstupným dokumentom pre plány fyzickej ochrany jadrových materiálov a jadrových zariadení. Dokumenty sú v režime „D“.

## K § 9

Ustanovenia sa týkajú identifikácie kritických subjektov a kritických subjektov osobitného európskeho významu. Zákon nezavádza povinnosť hlásiť ústrednému orgánu začatie poskytovania základnej služby, ani samoidentifikáciu kritickým subjektom. Označenie kritických subjektov a kritických subjektov osobitného európskeho významu zahŕňa postup ústredného orgánu, ktorým sa identifikuje kritický subjekt, ktorý splní všetky kritériá uvedené v odseku 1. Na tento účel je najprv potrebné stanoviť v stratégii presné prahové hodnoty kritérií významnosti vplyvu na poskytovanie základnej služby podľa § 14 ods. 3, na základe ktorých

sa kritické subjekty identifikujú a zaradzujú do sektorov, ako aj sa z nich vyradujú. Podmienkou identifikácie kritického subjektu podľa § 9 ods. 1 písm. c) a jeho zaradenia v sektore je skutočnosť, že spĺňa aspoň jedno kritérium významnosti vplyvu, ktorý by mal incident, ak by skutočne nastal. Celý proces sa nezaobíde bez zapojenia všetkých dotknutých ústredných orgánov, ktoré na základe svojich odborných a sektorových znalostí posudzujú relevantnosť informácií a údajov potrebných na identifikovanie kritického subjektu. Ústredný orgán bude oprávnený vyžadovať od subjektov o ktorých možno dôvodne predpokladať, že budú identifikované podľa tohto zákona ako kritické subjekty alebo kritické subjekty osobitného európskeho významu súčinnosť a poskytnutie potrebných údajov, dokladov a vysvetlení podľa § 11 ods. 4 písm. e).

Ak sú splnené kritériá na identifikáciu kritického subjektu, po zohľadnení stratégie a posúdení rizika je ústredný orgán povinný oznámiť kritickému subjektu najneskôr do 30 dní od identifikácie subjektu ako kritického subjektu, že bol identifikovaný ako kritický subjekt a zaradený v sektore a podsektore podľa prílohy č. 1. Ústredný orgán vo svojom oznámení uvedie, deň, ku ktorému bol subjekt identifikovaný ako kritický subjekt, ktorú základnú službu alebo základné služby poskytuje, do ktorého sektora a podsektora kritický subjekt zaraďuje a deň od ktorého je identifikovaný kritický subjekt povinný plniť povinnosti podľa zákona. Osobitne je upravená povinnosť vykonať posúdenie rizika v § 11 a prijať opatrenia na zabezpečenie odolnosti v § 10, pri ktorých zákon vychádza z lehôt stanovených priamo v smernici (EÚ) 2022/2557. Posledným krokom v procese identifikácie kritických subjektov je zaradenie do zoznamu kritických subjektov.

Ústredný orgán na úseku kritickej infraštruktúry, priebežne podľa potreby a aspoň raz za štyri roky preskúmava a aktualizuje zoznam kritických subjektov. V rámci princípu reciprocity ak sa kritický subjekt domnieva, že nespĺňa aspoň jedno kritérium pre identifikáciu, môže písomne požiadať ústredný orgán o preverenie splnenia kritérií. Kritický subjekt v žiadosti poskytne ústrednému orgánu všetky relevantné údaje, doklady a vysvetlenia potrebné na posúdenie splnenia kritérií. Ústredný orgán je povinný preveriť takéto žiadosti a písomne sa k nim vyjadriť najneskôr do 60 dní od doručenia písomnej žiadosti kritického subjektu.

Kritické subjekty v digitálnej infraštruktúre a finančnom sektore sú vystavené jedinečným a veľmi dynamickým hrozbám, ktoré majú potenciál výrazne narušiť ich prevádzku a služby, čo má následne široký/významný vplyv/dopad na hospodárstvo a spoločnosť ako celok. Keďže tieto sektory majú význam pre udržanie stability a bezpečnosti štátu, je nevyhnutné zabezpečiť ich odolnosť voči kybernetickým útokom a technologickým narušeniam v osobitných predpisoch. Preto sa kladie dôraz na potrebu špecifikovať zodpovednosti týchto sektorov s cieľom čo najefektívnejšie chrániť kritické služby, zabezpečiť kontinuitu činností a minimalizovať potenciálne vplyvy na ostatné sektory a občanov.

Na tento účel je nevyhnutné, aby ústredný orgán informoval kritické subjekty v dotknutých sektoroch, že budú plniť povinnosti podľa ďalších regulačných rámcov, ktoré budú zohľadňovať špecifiká a riziká spojené s prevádzkou kritickej infraštruktúry v sektoroch finančnej a digitálnej infraštruktúry. Tento rámec zahŕňa špecifické opatrenia na posúdenie rizík, plánovanie odolnosti, postupy reakcie na incidenty a povinné hlásenie incidentov. Na tento účel ústredný orgán oznámi kritickým subjektom v sektore financie a v sektore digitálnej infraštruktúry, že sa na nich nevzťahujú povinnosti ustanovené v § 19 ods. 3 a budú postupovať podľa regulácie návrhov zákonov, ktorým sa mení a dopĺňa zákon č. 747/2004 Z. z. o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení neskorších



predpisov a návrhu zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Kritický subjekt, ktorý poskytuje základné služby šiestim alebo viacerým členským štátom, je povinný informovať o tejto skutočnosti ústredný orgán, ktorý v zmysle komunikačných úloh informuje ministerstvo vnútra. Ministerstvo vnútra oznámi Komisii podrobnosti týkajúce sa takéhoto kritického orgánu osobitného európskeho významu na účely uskutočnenia konzultácií. Ak Komisia dospeje k záveru, že príslušný kritický orgán sa považuje za kritický subjekt osobitného európskeho významu, oznámi to jednotnému kontaktnému miestu, v tomto prípade ministerstvu vnútra.

Ústredný orgán je na základe informácie poskytnutej ministerstvom vnútra povinný oznámiť dotknutému kritickému orgánu, že bol identifikovaný ako kritický subjekt osobitného európskeho významu a, že sa naň vzťahujú povinnosti ustanovené takémuto subjektu podľa tohto zákona.

## K § 10

Účinný nástroj na zabezpečenie odolnosti kritických subjektov v oblasti kritickej infraštruktúry predstavuje bezpečnostný plán. Každý kritický subjekt je povinný mať vypracovaný a implementovaný aktuálny bezpečnostný plán v praxi pre vlastnú a prevádzkovanú kritickú infraštruktúru. Kritický subjekt sám vymedzí svoju kritickú infraštruktúru, ktorá je nevyhnutná pre poskytovanie základnej služby alebo základných služieb podľa prílohy č. 1. Bezpečnostný plán musí obsahovať podrobný opis a lokalizáciu kritickej infraštruktúry pomocou GPS súradníc. Okrem toho musí zahŕňať širokú škálu opatrení naprieč technickými, organizačnými, personálnymi a kontrolnými aspektmi, aby sa zabezpečila väčšia odolnosť kritickej infraštruktúry. Kľúčom k plánu je špecifikácia opatrení, ktoré sú kriticky dôležité pre účinnú prevenciu incidentov, ochranu infraštruktúry, reakciu na incidenty, následné riadenie a zotavenie sa z týchto situácií. Kritický subjekt je povinný aktualizovať svoj bezpečnostný plán v určenej lehote ústredným orgánom podľa § 8 ods. 4, v prípade sprístupnenia posúdenia rizika s významným vplyvom.

Zabezpečenie odolnosti kritickej infraštruktúry je proces, ktorý si vyžaduje komplexný prístup a koordinovanú spoluprácu medzi kritickým subjektom a príslušnými ústrednými orgánmi. Tento proces sa začína dôkladným posúdením potenciálnych rizík, ktoré by mohli ohroziť bezpečnosť infraštruktúry.

Na účely posilnenia odolnosti kritického subjektu, kde je potrebné predchádzať a reagovať na incidenty je kľúčové aj využívanie kamerového systému ako nástroja na monitorovanie a ochranu kritickej infraštruktúry. V tomto prípade má kritický subjekt právo monitorovať nielen samotnú kritickú infraštruktúru, ale aj jej bezprostredné okolie, a to v rozsahu, ktorý považuje za potrebný na splnenie cieľov ochrany. Je dôležité, aby bol kamerový systém riadne začlenený do celkového bezpečnostného plánu a aby bola jeho inštalácia a používanie odôvodnené s prihliadnutím na konkrétne umiestnenie infraštruktúry a súvisiace riziká. Z prvej časti vety § 10 ods. 3 zákona vyplýva, že nie všetky kritické subjekty sa rozhodnú využiť kamerové systémy, preto nenastáva problém s formulovaním možnosti a povinnosti. V tomto bode tiež narážame na uvedenie konkrétnej zásady – minimalizácie údajov podľa čl. 5 ods. 1 písm. c) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane

údajov) v platnom znení, aby kritické subjekty vedeli, že musia pri zavádzaní systému zohľadniť a v bezpečnostnom pláne odôvodniť konkrétne túto zásadu.

Kritický subjekt musí zároveň zabezpečiť, aby sa záznam z kamerového systému uchovával sedem dní po jeho vyhotovení. Táto požiadavka je dôležitá pre prípad, že v prípade incidentu bude potrebná rekonštrukcia udalostí. Záznamy môžu byť neoceniteľným zdrojom informácií pri vyšetrowaní trestných činov týkajúcich sa závažných narušení alebo útokov na kritickú infraštruktúru. Kritický subjekt je povinný poskytovať tieto záznamy na iný účel ako zabezpečenie odolnosti kritického subjektu, len súdom, orgánom činným v trestnom konaní a spravodajskej službe, čím sa zabezpečí ochrana osobných údajov a zabráni sa zneužitiu záznamov.

Celkovo je proces zabezpečenia odolnosti kritickej infraštruktúry komplexným úsilím, ktoré si vyžaduje neustálu aktualizáciu a prispôsobovanie sa meniacim sa bezpečnostným hrozbám. Kritický subjekt spolu s ústrednými orgánmi musí neustále monitorovať vyvíjajúcu sa situáciu a byť pripravený aktualizovať potrebné bezpečnostné opatrenia na zabezpečenie ochrany kritickej infraštruktúry a predchádzať prípadným poruchám alebo útokom za účelom zvyšovania celkovej odolnosti. Pri odporúčaní minimálnych opatrení na zabezpečenie odolnosti kritického subjektu ústredným orgánom podľa § 6 písm. i) budú ústredné orgány dbať o primerané prehlbovanie povinností vlastníka len vo vzťahu k jeho kritickej infraštruktúre z dôvodu zabezpečenia odolnosti kritickej infraštruktúry a zabezpečenia poskytovania základnej služby.

## K § 11

Ustanovenia v § 11 sa zameriavajú a kladú dôraz na špecifikáciu zodpovedností kritických subjektov na úseku kritickej infraštruktúry, pričom kľúčovým aspektom je zodpovednosť kritických subjektov za proces zvyšovania ich odolnosti. Cieľom je dosiahnuť vysokú úroveň ochrany kritickej infraštruktúry stanovením konkrétnych povinností, ktoré musí kritický subjekt splniť.

Základnou charakteristikou týchto povinností je, že kritický subjekt, ktorý bol identifikovaný podľa kritérií, je povinný vykonať komplexné posúdenie všetkých relevantných rizík, ktoré by mohli ohroziť poskytovanie jeho základných služieb, a to do deviatich mesiacov od prijatia tohto oznámenia a potom opakovane podľa budúcich potrieb, najmenej však raz za štyri roky.

V tomto posúdení sa zohľadňuje široká škála rizík vrátane prírodných katastrof, nehôd a rizík súvisiacich s ľudskou činnosťou, ako sú napríklad teroristické útoky. Posudzujú sa v ňom aj potenciálne vplyvy incidentov v jednom sektore na iné sektory alebo podsektory, pričom sa zohľadňujú aj možné cezhraničné vplyvy.

Opatrenia na zabezpečenie ochrany kritickej infraštruktúry zahŕňajú okrem iného povinnosť udržiavať technológiu, ktorá zabezpečuje ochranu a funkčnosť kritickej infraštruktúry, poskytovanie pokynov zamestnancom o bezpečnostnom pláne a pravidelné prehodnocovanie ochranných opatrení.

Kritické subjekty musia tiež úzko spolupracovať s príslušnými štátnymi orgánmi, a to aj poskytovaním potrebných informácií o svojej infraštruktúre a prijatých ochranných

opatreniach. Je tiež ich zodpovednosťou reagovať na incidenty a zabezpečiť, aby sa čo najrýchlejšie obnovila kontinuita poskytovaných základných služieb.

Ďalšou dôležitou povinnosťou je povinnosť informovať o zmenách, ktoré by mohli ovplyvniť identifikáciu a klasifikáciu subjektu ako kritického subjektu, vrátane možného prevodu kontroly nad kritickou infraštruktúrou na iný subjekt, ak by takýto prevod alebo prechod spôsobil dopad v poskytovaní základnej služby kritickým subjektom. Tu je dôležité poznamenať, že hlavným záujmom je chrániť poskytovanie základných služieb, preto je práve základná služba primárnym objektom pozornosti štátu. Vo vzťahu k prevodu a prechodu kritickej infraštruktúry je preto pre štát relevantná iba taká informácia o dispozícii s kritickou infraštruktúrou, pokiaľ by dispozičné zmeny mali vplyv na poskytovanie základnej služby a mohli by zasiahnuť do záujmov chránených zákonom.

Preverovanie zahraničných investícií má obrovský význam v súčasnom globalizovanom svete, kde medzinárodné kapitálové toky môžu mať významný vplyv na národnú bezpečnosť a stabilnú ekonomiku štátu. Tento proces je obzvlášť dôležitý v prípade investícií do sektorov, ktoré sú kritické pre fungovanie štátu a služieb jeho obyvateľov, ako napríklad energetika a priemysel.

Preverovanie zahraničných investícií umožňuje identifikovať a minimalizovať potenciálne bezpečnostné riziká. Zahraničný investor môže mať odlišné zámery, ktoré nemusia byť vždy transparentné alebo v súlade s národnými záujmami. Preto je nevyhnutné, aby sa každá investícia uskutočnená v kritických sektoroch podrobne preskúmala s ohľadom na možné bezpečnostné hrozby.

Zahraničné investície do týchto sektorov môžu priniesť potrebný kapitál a inovácie, ale tiež môžu predstavovať riziko pre národnú bezpečnosť, ak by sa tieto strategické aktíva dostali pod kontrolu subjektov s nepriaznivými zámermi. Investície môžu v niektorých prípadoch zapríčiniť monopolizáciu trhov, narušenie hospodárskej súťaže, alebo dokonca vyvolať ekonomickú závislosť na zahraničných subjektoch. Strategickejšie riadenie a regulácia týchto investícií pomáha chrániť vnútroštátny trh a zároveň podporuje udržateľný rozvoj a inovácie.

Preto je nesmierne dôležité, aby sa zahraničné investície, najmä tie, ktoré smerujú do kľúčových odvetví, dôkladne preverovali so zameraním na zabezpečenie, že takéto transakcie budú prospešné pre národné hospodárstvo, neohrozia národnú bezpečnosť a prispievajú k celkovej odolnosti štátu voči vonkajším a vnútorným hrozbám.

Celkovo ide vo vymedzených povinnostiach kritických subjektov o komplexný súbor opatrení, ktorého cieľom je zabezpečiť vysokú úroveň odolnosti a ochrany kritickej infraštruktúry, a tým prispieť k bezpečnosti a stabilnému fungovaniu spoločnosti a štátu v prípade ohrozenia alebo významných incidentov.

## K § 12

Kontaktná osoba zabezpečuje výmenu informácií týkajúcich sa odolnosti kritických subjektov v oblasti kritickej infraštruktúry medzi ústredným orgánom štátnej správy, v ktorom sa nachádza sektor kritickej infraštruktúry, a ministerstvom vnútra. Kritický subjekt poskytne kontaktnej osobe podmienky riadneho plnenia úloh. Existujú aj podmienky pre integritu kontaktnej osoby, ktorá bude zároveň oprávnenou osobou na oboznámenie sa s limitovanými informáciami.

Kontaktná osoba zabezpečuje komunikáciu medzi kritickým subjektom, príslušným ústredným orgánom, ministerstvom vnútra a medzi kritickými subjektmi pri zabezpečovaní odolnosti kritickej infraštruktúry a pri zabezpečovaní kontinuity poskytovania základnej služby, najmä výmeny relevantných informácií o identifikovaní a údaje o riziku jej narušenia alebo potencionálnych vplyvoch incidentov. Kontaktná osoba nemusí byť zamestnancom kritického subjektu, ale zároveň podlieha povinnostiam oprávnenej osoby. Oprávnenú osobu kritického subjektu určuje kritický subjekt. Rozsah oprávnenia kontaktnej osoby a oprávnených osôb určí kritický subjekt tak, aby zodpovedal ich činnostiam vykonávaným v kritickom subjekte. Kritický subjekt zároveň v povolení určí, či mu v potrebnom rozsahu umožní priamy alebo vzdialený prístup do priestorov kritickej infraštruktúry, limitovaných informácií alebo kontrolných systémov kritického subjektu.

V prípade kontaktnej a oprávnenej osoby sa bude môcť jednať aj o jednu osobu, ktorá zastreší pôsobnosť tak kontaktnej osoby a súčasne aj oprávnenej osoby.

Kontaktná osoba a oprávnená osoba, vrátane záujemcu o získanie takejto pozície u kritického subjektu, musia kritickému subjektu preukázať svoju totožnosť a bezúhonnosť. Preukázanie totožnosti a bezúhonnosť sa vyžadujú len za účelom hodnotenia potencionálneho rizika pre dotknutý kritický subjekt. Na účely tohto zákona sa za bezúhonnú osobu považuje fyzická osoba, ktorá nebola odsúdená za úmyselný trestný čin, ktorého spáchanie by mohlo viesť k porušeniu odolnosti kritického subjektu pri vykonávaní činností v kritickom subjekte. Fyzická osoba, ktorá je štátnym občanom Slovenskej republiky, poskytne kritickému subjektu výpis z registra trestov na účely preukázania bezúhonnosti. Výpis z registra trestov nesmie byť v čase jeho podania starší ako tri mesiace. Fyzická osoba, ktorá nie je štátnym občanom Slovenskej republiky, je povinná na preukázanie bezúhonnosti poskytnúť kritickému subjektu výpis z registra trestov vydaný príslušným orgánom štátu, ktorého je štátnym príslušníkom. Ak sa takýto dokument v tejto krajine nevydá, výpis z registra trestov sa nahradí rovnocenným dokumentom vydaným príslušným súdnym alebo správnym orgánom alebo čestným vyhlásením potvrdeným príslušným orgánom krajiny. Výpis z registra trestov alebo dokument, ktorý ho nahrádza, nesmie byť v čase podania starší ako tri mesiace, musí k nemu byť priložené osvedčenie a musí sa predložiť spolu s overeným prekladom do štátneho jazyka. Úradný preklad výpisu z registra trestov alebo listiny, ktorá ho nahrádza do štátneho jazyka, sa nevyžaduje od občana Českej republiky. Počas doby platnosti oprávnenia sú kontaktná osoba a oprávnená osoba povinné bez zbytočného odkladu oznámiť kritickému subjektu každú zmenu skutočností rozhodujúcich pre posúdenie integrity, a to najneskôr do 14 dní od právoplatného odsúdenia kritického subjektu za úmyselný trestný čin.

## K § 13

Vzhľadom na dôležitosť limitovaných informácií z hľadiska posudzovania bezpečnosti kritickej infraštruktúry sú stanovené potrebné pravidlá na zabezpečenie jej ochrany pred odhalením. Zákon zavádza pojem "limitovaná informácia", ktorý nahrádza rozsah citlivých informácií podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre. Limitované informácie o kritickej infraštruktúre ako osobitnom type neverejných informácií nebudú verejnosti sprístupnené z dôvodu ich významu.

## K § 14

Kritické subjekty sú povinné okamžite informovať sektorovo príslušné ústredné orgány o incidentoch, ktoré narúšajú alebo môžu významne narušiť ich prevádzku v situáciách vymedzených zákonom. Tieto informácie umožňujú ústrednému orgánu získať komplexný prehľad o celkových rizikách, ktorým čelia kritické subjekty, a následne na ne primerane reagovať. Na tento účel sa stanovuje postup oznamovania incidentov a stanovenie prahových hodnôt v posúdení rizika ústredným orgánom podľa § 8 ods. 3 písm. e) na určenie toho, kedy je skutočné alebo potenciálne narušenie významné, a preto by sa incidenty mali oznamovať. Určenie významnosti incidentu je založené na kritériách, najmä počet a podiel používateľov dotknutých narušením, trvanie narušenia a geografické územie dotknuté narušením s prihliadnutím na to, či je toto územie geograficky izolované. Určenie prahových hodnôt pre oznámenie incidentov priebežne posudzujú a aktualizujú ústredné orgány na úseku kritickej infraštruktúry. Vzhľadom na možné cezhraničné a reťazové účinky takýchto narušení sa zavádza postup, v rámci ktorého sú bezpečnostné zložky, ako aj ostatné dotknuté členské štáty informované prostredníctvom miest jednotného kontaktu.

V § 14 ods. 3 sa uvádzajú kritériá významnosti vplyvu, ktoré navrhujú jednotlivé ústredné orgány a ktoré po ich schválení vládou v stratégii budú predstavovať kritériá pre identifikáciu subjektov ako kritických subjektov podľa § 9 ods. 1 písm. c). Kritériá významnosti vplyvu na poskytovanie základnej služby vychádzajú obsahovo zo smernice (EÚ) 2022/2557. Spôsob a metodika výpočtu jednotlivých prahových hodnôt bude obsahovať práve stratégia.

Vzhľadom na to, že podľa čl. 6 ods. 2 smernice (EÚ) 2022/2557 členský štát pri identifikácii kritických subjektov musí zohľadniť „posúdenie rizika členským štátom a svoju stratégiu.“, čo bolo premietnuté aj do § 7 ods. 1 písm. d), § 8 ods. 2 a § 9 ods. 2, ako aj vzhľadom na rozdielnosť jednotlivých sektorov a základných služieb, nie je možné priamo zákonom ustanoviť konkrétne číselné/percentuálne vyjadrenie jednotlivých kritérií a ich prahových hodnôt. Práve proces konzultácií s podnikateľským sektorom pri tvorbe stratégie bude významným faktorom pre kvalitné a relevantné nastavenie jednotlivých kritérií.

Do úvahy sa budú brať tiež existujúce relevantné dáta a exaktné inštitúty týkajúce sa poskytovania základných služieb. Z toho dôvodu sa napríklad pri výpočte trhového podielu bude zohľadňovať existujúca európska a vnútroštátna legislatíva na úseku hospodárskej súťaže, a to s cieľom nastavenia takých prahových hodnôt, ktoré vychádzajú z ustálených a jednotných postupov v oblasti definície relevantného trhu a podielu subjektu na ňom.

Schválené kritériá v stratégii nebude možné zverejniť a bude sa na nich vzťahovať režim podľa zákona č. 215/2004 Z. z. Identifikovanému kritickému subjektu bude ale oznámené naplnenie konkrétneho kritéria podľa § 14 ods. 3, podľa schválenej stratégie, alebo jej aktualizácie a to v samotnom písomnom oznámení podľa § 9 ods. 2., na ktoré sa bude vzťahovať režim limitovanej informácie.

Incidenty, ktoré významne narúšajú alebo môžu výrazne narušiť poskytovanie základných služieb, sa musia oznamovať elektronicky a to spôsobom, ktorý určí príslušný ústredný orgán na svojom webovom sídle.

Kritické subjekty sú povinné predložiť prvé oznámenie o incidente do 24 hodín od zistenia incidentu vrátane informácií o predbežnej alebo skutočnej príčine, dotknutých osobách, trvaní incidentu a možnom cezhraničnom vplyve incidentu. V prvotnom oznámení kritický subjekt poskytne také údaje, ktorými v danom čase disponuje, čo v prípade § 14 ods. 5 písm. b) bude predstavovať len odhad počtu a podielu používateľov základných služieb dotknutých

incidentom a to u konkrétneho kritického subjektu, nie vo vzťahu ku všetkým používateľom základnej služby (teda tým, ktorým sa základná služba poskytuje inými kritickými subjektmi). V prípade, že incident trvá dlhšie ako mesiac, musí byť predložená podrobná správa o incidente.

Po prijatí oznámenia o incidente ústredný orgán poskytne kritickému subjektu ďalšie relevantné informácie ohľadom incidentu na základe jeho posúdenia a vo verejnom záujme môže informovať verejnosť o významnom narušení poskytovania základnej služby. Ústredný orgán vedie zoznam všetkých incidentov, ktoré ovplyvnili poskytovanie základných služieb, a informuje o nich ministerstvo vnútra. Následne ministerstvo vnútra informuje ďalšie relevantné bezpečnostné zložky a medzinárodných partnerov.

Ohlasovacia povinnosť a kritériá na určenie závažnosti incidentov sú základnými prvkami účinnej reakcie na incidenty, ktoré ohrozujú odolnosť kritickej infraštruktúry a kontinuitu poskytovania základných služieb. Tieto postupy umožňujú rýchlu a koordinovanú reakciu a zabezpečujú, aby kritické subjekty a štátne orgány mali aktuálne informácie na riadenie krízových situácií.

## K § 15

Vzhľadom na čoraz prepojenejšiu povahu poskytovania základných služieb a rastúcu vzájomnú závislosť v sektoroch, predstavuje chýbajúca úroveň odolnosti jediného kritického subjektu vážne riziko pre kritické subjekty pôsobiace v iných sektoroch nie len v rámci vnútorného trhu, ale aj v rámci trhu na úrovni EÚ. V reakcii na to štátna správa na úseku kritickej infraštruktúry poskytuje podporu kritickým subjektom na zvýšenie ich odolnosti. Táto podpora zahŕňa vývoj poradenských materiálov a metodík, podporu v súvislosti s organizáciou testovania odolnosti, poskytovanie poradenských služieb, výmenu informácií a najlepších postupov s kritickými subjektmi pôsobiacimi v sektoroch a podsektoroch kritickej infraštruktúry.

Ministerstvo vnútra a ústredné orgány spolupracujú s kritickými subjektmi pôsobiacimi v sektoroch a podsektoroch uvedených v prílohe č. 1 a vymieňajú si s nimi informácie a najlepšie postupy. Kritické subjekty si môžu navzájom vymieňať informácie o záležitostiach upravených týmto zákonom. Tým nie sú dotknuté povinnosti stanovené v osobitných ustanoveniach týkajúcich sa najmä utajovaných skutočností, limitovaných informácií, hospodárskej súťaže a ochrany osobných údajov.

## K § 16

Zavádzajú sa právomoci ústredných orgánov, ktoré zahŕňajú najmä právomoc vykonávať kontroly, kde sa postupuje ako pri výkone kontroly v štátnej správe. Kontrolu kritických subjektov potom bude vykonávať ministerstvo a ostatné ústredné orgány štátnej správy u tých kritických subjektov, ktoré zaradili do zoznamu kritických subjektov a ktoré tak patria do ich vecnej pôsobnosti. Bude sa vyžadovať od kritických subjektov, aby poskytovali informácie a dôkazy týkajúce sa opatrení, ktoré prijali na splnenie svojich povinností, a v prípade potreby vydávať príkazy na nápravu zistených porušení. Pri vydávaní takýchto príkazov sa nebudú vyžadovať opatrenia, ktoré presahujú rámec toho, čo je nevyhnutné a primerané tomu, aby dotknutý kritický subjekt dodržiaval povinnosti podľa smernice (EÚ) 2022/2557, a to najmä so zreteľom na závažnosť ich porušenia a hospodársku kapacitu

kritického subjektu. Ministerstvo a ústredné orgány spolupracujú a vymieňajú si informácie s orgánmi štátnej správy na úseku kritickej infraštruktúry.

Ústredné orgány budú tiež oprávnené kontrolovať plnenie povinností kritických subjektov podľa tohto zákona, vrátane oprávnenia (možnosti) nariadiť alebo vykonať audit, ktorý umožňuje článok 21 smernice (EÚ) 2022/2557. V kontexte zákona ide v prípade auditu o nástroj, ktorý môže nadväzovať na kontrolu kritických subjektov a je tak jedným z možných opatrení, ktoré je možné u kritického subjektu realizovať v prípade dôvodného podozrenia zistených nedostatkov alebo pochybení. V tomto nastavení je splnená aj zásada transparentnosti a nezávislého posúdenia prijatých opatrení kritického subjektu. Náklady vykonávaného auditu znáša ústredný orgán, ktorý ho nariadil. Ústredné orgány si budú môcť upraviť interným predpisom postup pri vykonávaní auditu, prípadne ďalšie podrobnosti o audite, keď ho bude vykonávať priamo ústredný orgán. V prípade, ak bude audit nariadený a bude ho vykonávať iná osoba než ústredný orgán, napríklad znalec, tam bude nutné rešpektovať limity stanovené príslušnými právnymi predpismi.

## K § 17 - 18

Na úseku kritickej infraštruktúry majú finančné sankcie zásadný význam pre zabezpečenie dodržiavania stanovených povinností kritickými subjektmi. Tieto sankcie predstavujú často jediný efektívny prostriedok na zabezpečenie dodržiavania legislatívy v tejto oblasti, keďže riziko finančnej straty môže motivovať subjekty k zachovaniu prísnych bezpečnostných opatrení a k prevencii potenciálnych porušení povinností. V kontexte zabezpečovania odolnosti kritickej infraštruktúry proti rôznym hrozbám je dodržiavanie legislatívy a predpisov kľúčové pre udržanie funkčnosti životne dôležitých služieb pre spoločnosť a ekonomiku.

Zabezpečenie odolnosti kritickej infraštruktúry si vyžaduje od subjektov podniknutie vhodných technických, organizačných a personálnych opatrení. Tieto opatrenia môžu byť spojené s nákladmi, no potenciálna finančná strata z nevyhovujúcich sankcií za nesplnenie legislatívnych požiadaviek môže byť motiváciou pre subjekty k investovaniu do týchto nevyhnutných opatrení. Zákon o kritickej infraštruktúre podrobne vymedzuje povinnosti kritických subjektov a stanovuje mechanizmus dohľadu a kontroly nad ich dodržiavaním, vrátane možnosti uloženia sankcií za neplnenie týchto povinností. Finančné sankcie, stanovené za porušenie legislatívy, slúžia taktiež ako varovný signál pre subjekty, ktoré zanedbávajú svoje súvisiace povinnosti. Pôsobia ako dôležitý regulačný nástroj, ktorý má za cieľ zvýšiť odolnosť kritickej infraštruktúry a minimalizovať riziko výpadkov životne dôležitých základných služieb.

## K § 19 - 23

V spoločných ustanoveniach sa odkazuje na príslušnú prílohu zákona, upravuje sa vzťah k niektorým osobitným zákonom (správneho poriadku, zákonu o ochrane utajovaných skutočností a zákonu o kontrole v štátnej správe) a vymedzujú sa prechodné ustanovenia týkajúce sa povinnosti prevádzkovateľov prvkov kritickej infraštruktúry, ktoré sa zároveň vzťahujú aj na prevádzkovateľov prvkov európskej kritickej infraštruktúry podľa zákona 45/2011 Z. z. o kritickej infraštruktúre.

Dôležitým ustanovením v tejto časti je § 19, ktorý je kľúčovým pre kritické subjekty pôsobiace v sektore digitálnej infraštruktúry, financií a v podsektore jadrová energetika, pre ktoré sa na účely povinností a činností vzťahujú osobitné právne predpisy.

V prechodných ustanoveniach sa stanovujú úlohy a lehoty ústredným orgánom štátnej správy vrátane lehôt ich splnenia, ktoré sa týkajú najmä Stratégie a postupu pri identifikácii kritických subjektov na úseku kritickej infraštruktúry. Týmto spôsobom sa zabezpečí vytvorenie novej sústavy kritických subjektov na úseku kritickej infraštruktúry.

V záverečných ustanoveniach sa preberajú právne záväzné akty Európskej únie a informácie o zrušení zákona č. 45/2011 Z. z. o kritickej infraštruktúre spolu s odkazmi na ďalšie osobitné zákony.

## Čl. II

Navrhuje sa potreba zamedzenia prístupu k údajom a informáciám, ktorých zverejnenie môže narušiť bezpečnosť, odhaliť aktíva a aj slabé stránky podniku alebo orgánu verejnej moci a tým narušiť nielen bezpečnostné prostredie, ale aj dobré meno a hospodársku súťaž.

## Čl. III.

Legislatívno-technická úprava v súvislosti s precizovaním terminológie a pojmológie. V poznámkach a referenciách, kde sa upravuje vzťah k niektorým osobitným zákonom sa vypúšťa slovo „prvkov“.

## Čl. IV.

K bodu 1:

Základným cieľom zavedenia inštitútu limitovanej informácie je posilnenie bezpečnosti štátu spôsobom, ktorým bude právo na informácie dotknuté len v nevyhnutne potrebnej miere. Aktuálne celospoločenské dianie, stav spoločnosti a bezpečnostného prostredia vyplývajúceho z mimoriadnych udalostí, incidentov a iných negatívnych skutočností je podrobne popísané vo všeobecnej časti dôvodovej správy, a keďže tieto udalosti rovnako vplyvajú aj na potrebu zavedenia inštitútu limitovaných informácií v slovenskom systéme práva, je opodstatnené pripomenúť tie najdôležitejšie:

- V súčasnom geopolitickom kontexte, ktorý sa vyznačuje rastúcou nestabilitou, najmä v dôsledku vojny na Ukrajine a rastúcej zložitosti bezpečnostných hrozieb, ako aj následkami zmeny klímy, ako je nárast nezvyčajných klimatických udalostí alebo nedostatok vody, musí Slovenská republika zostať ostražitá a neustále sa prispôbovať.
- Nachádzame sa v dobe, kedy sa frekvencia výskytu mimoriadnych udalostí a incidentov výrazne zvýšila a tým sa priamoúmerne zintenzívnilo možné ohrozenie nielen života, zdravia, bezpečnosti a majetku obyvateľov, životného prostredia, ale aj fungovania štátu.
- Vychádzajúc z doterajších skúseností, dostupných informácií a zaznamenaných trendov je možné predpokladať, že v nasledujúcom období bude celkové dianie ovplyvnené doznením pandémie COVID-19, ako aj neistotou vyplývajúcou z vojny na Ukrajine a na to nadväzujúcej vysokej miery inflácie a dôsledkami ekonomickej stagnácie, ktorá bude mať negatívny dopad na celkovú finančnú situáciu.
- V čoraz viac prepojenom svete sa stala odolnosť voči hrozbám pre bezpečnostné prostredie prvoradou. Bezpečnostné prostredie zahŕňa rôzne kritické aspekty vrátane fyzickej



- infraštruktúry, informačných systémov, personálu a citlivých údajov. Ochrana tohto prostredia si vyžaduje komplexný prístup, ktorý rieši potenciálne hrozby a zraniteľnosti.
- V dnešnej digitálnej dobe je kybernetická bezpečnosť kritickým aspektom ochrany bezpečnostného prostredia. Na ochranu informačných systémov a citlivých údajov sú nevyhnutné spoľahlivé opatrenia kybernetickej bezpečnosti.
  - Základné služby, ktoré poskytujú subjekty prevádzkujúce kritickú infraštruktúru, sú kľúčové pre zachovanie životne dôležitých spoločenských funkcií, hospodárskych činností, verejného zdravia, bezpečnosti alebo životného prostredia a na vnútornom trhu majú byť poskytované nerušeným spôsobom. Preto vzhľadom na význam týchto základných služieb pre vnútorný trh a z toho vyplývajúcu potrebu zvýšiť odolnosť kritickej infraštruktúry, v širšom zmysle zabezpečiť odolnosť kritických subjektov poskytujúcich tieto služby, musí Slovenská republika prijať opatrenia na posilnenie takejto odolnosti a zmiernenie akýchkoľvek narušení pri poskytovaní takýchto základných služieb. Takéto narušenia môžu mať inak vážne dôsledky nielen pre občanov Slovenskej republiky, ale aj Európskej únie, hospodárstva Slovenskej republiky a dôveru v demokratický systém, kde hrozby môžu ovplyvniť fungovanie vnútorného trhu, najmä v kontexte rastúcej vzájomnej závislosti medzi sektormi vnútri štátu aj cezhranične.
  - Zraniteľnosť, ktorá na úseku kritickej infraštruktúry nebola niekoľko rokov riešená je ochrana citlivých informácií zavedená v § 12 zákona č. 45/2011 Z. z. o kritickej infraštruktúre. Platné právne predpisy chránia oprávnené záujmy prostredníctvom ochrany určitých kategórií informácií. Pokrytá je oblasť utajovaných skutočností, oblasť ochrany osobných údajov, obchodného tajomstva, no ochrana citlivých informácií nie je dostatočne rozpracovaná. Tento nedokonalý stav problematiky citlivých informácií, zapríčinil zvýšený stupeň latentného pohľadu na význam a obsah informácií, čo má v danom prípade priamy vplyv na bezpečnosť. Keďže platné právne predpisy neobsahujú zoznamy explicitne vyjadrených skutočností, ktoré sú citlivou informáciou (s výnimkou zoznamov utajovaných skutočností predpísaných zákonom č. 215/2004 Z. z. v znení neskorších predpisov), zavádza sa pojem limitovanej informácie, ktorý nahrádza práve opomínaný druh citlivých informácií. Inštitút citlivej informácie nie je nahradený v celom právnom poriadku, ostáva zachovaný napríklad v zákone č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov.

V právnom poriadku Slovenskej republiky je už zavedený systém ochrany informácií inštitútom utajovanej skutočnosti, ktorá je zadefinovaná zákonom č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Zákon č. 215/2004 Z. z. ustanovuje ochranu takých informácií, ktoré majú potenciál ohroziť záujmy Slovenskej republiky (ako je napr. zachovanie ústavnosti, zvrchovanosti, obrana, atď.). V prípade stupňa utajenia Vyhradené sa uvádza, že neoprávnená manipulácia s takouto utajovanou skutočnosťou by mohla zapríčiniť poškodenie právom chránených záujmov právnickej osoby alebo fyzickej osoby, čo by mohlo byť nevýhodné pre záujmy Slovenskej republiky. V právnom systéme Slovenskej republiky však absentuje právna úprava takých informácií, ktorých vyzradenie alebo zverejnenie síce nepredstavuje pre Slovenskú republiku určitú mieru ujmy na jej záujmoch (utajované informácie), no napriek tomu sú pre štát dôležité, keďže ich voľným (nekontrolovateľným) šírením verejnosti môžu ohroziť, obmedziť alebo znemožniť plnenie úloh subjektu v oblasti zabezpečenia vnútorného poriadku alebo ich zverejnenie by ohrozilo poskytovanie základnej služby kritickým subjektom. Rovnako platné právne predpisy Slovenskej republiky neobsahujú zoznamy explicitne vyjadrených skutočností, ktoré sú citlivou/limitovanou informáciou (s výnimkou zoznamov utajovaných skutočností podľa zákona o ochrane utajovaných skutočností). Zákomom č. 45/2011 Z. z. o kritickej infraštruktúre bola síce zavedená do právneho poriadku ochrana

citlivých informácií, avšak táto právna úprava, ako aj definícia tohto druhu informácií a ich aplikácia v praxi bola a je nedostatočná a už prekonaná. Tento nežiaduci stav problematiky citlivých informácií zapríčinil aj zmenu pohľadu na význam a obsah informácií.

Ešte vypuklejším problémom sa uvedené javí vo vzťahu k potrebe zabezpečenia neverejných informácií poskytnutých Slovenskej republike inými štátmi alebo medzinárodnými inštitúciami, ktorých je Slovenská republika členom. Tento inštitút „limitovaných informácií“ majú štáty alebo medzinárodné inštitúcie zavedený rôzne a líšia sa aj ich označením, napríklad v Európskej únii majú „EU LIMITE“, vo Francúzsku „Diffusion Restreinte“ a v Organizácii Severoatlantickej zmluvy „NATO UNCLASSIFIED“. Spoločným znakom uvedených neverejných informácií je, že nie sú utajovanými skutočnosťami, avšak nie sú určené ani pre verejnosť (nezverejňujú sa v médiách, na internete a neuvoľňujú sa pre občanov). Pri zachovaní pravidiel ukladania a zachovaní integrity je možné ich postupovať iným inštitúciám pre výkon ich povinností a právomocí. Zverejniť a sprístupniť tieto informácie inému subjektu (tzv. tretej strane) než určenému okruhu osôb, nie je možné bez súhlasu ich pôvodcu (t. j. poskytujúceho štátu alebo medzinárodnej inštitúcie).

V zmysle Ústavy Slovenskej republiky (čl. 26 ods. 4) je právo na informácie zaručené, pričom právo vyhľadávať a šíriť informácie možno obmedziť zákonom, ak ide o opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti. Navrhovaným znením sa ustanovujú oblasti, v ktorých môže limitovaná informácia vzniknúť, pričom primárnym cieľom navrhovanej úpravy je upraviť taký druh informácií, ktorých šírením by mohlo dôjsť k ohrozeniu alebo narušeniu činnosti orgánov štátnej správy v oblasti bezpečnosti, obrany alebo verejného poriadku alebo ich zverejnenie by ohrozilo poskytovanie základnej služby kritickým subjektom. Na strane druhej navrhovaná úprava však jasne vymedzuje oblasti, v ktorých limitovaná informácia vzniknúť nemôže (riešené odkazom na § 4 zákona o ochrane utajovaných skutočností), konkrétne, ak ide o nezákonný alebo nesprávny postup alebo nezákonné rozhodnutie verejných činiteľov a orgánov verejnej moci, trestnú činnosť verejných činiteľov, nehospodárne, neefektívne a neúčelne nakladanie s verejnými prostriedkami, závažné ohrozenie alebo poškodenie životného prostredia, života a zdravia, platové náležitosti, hmotné zabezpečenie a hmotné výhody verejných činiteľov. Takouto legálnou definíciou limitovaných informácií navrhovaná úprava dostatočne jasne, presne a jednoznačne vymedzuje hranice možností určenia limitovaných informácií a primerane zužuje rozsah určenia limitovaných informácií v súlade s Ústavou Slovenskej republiky, čím zabráňuje extenzívnej interpretácii výnimky pri obmedzení základného práva na informácie, resp. svojvoľe v rozhodovaní orgánu verejnej moci o určení limitovanej informácie.

Navyše zo súdnej judikatúry vyplýva, že verejnosti by mali byť prístupné všetky dokumenty orgánov verejnej moci, treba však chrániť niektoré verejné záujmy prostredníctvom výnimiek. Sloboda prejavu a právo vyhľadávať a šíriť informácie sa v zmysle čl. 26 ods. 4 Ústavy Slovenskej republiky zaručuje, avšak aj táto má svoje limity, keďže všetky základné práva a slobody sa chránia len v takej miere a v takom rozsahu, dokiaľ uplatnením jedného práva alebo slobody nedôjde k neprimeranému obmedzeniu, či dokonca popretiu iného práva alebo slobody. Slobodu prejavu a právo vyhľadávať a šíriť informácie možno obmedziť zákonom, ak ide o opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti. Materiálna podmienka na ústavne konformné obmedzenie práva na šírenie informácií z dôvodu sledovania legitímneho cieľa spočívajúceho v zachovávaní bezpečnosti štátu je v prípade navrhovanej úpravy limitovanej informácie splnená.

S ohľadom na všetky tieto skutočnosti sa do zákona o ochrane utajovaných skutočností zavádza limitovaná informácia a ustanovuje sa jednotná úprava tejto kategórie informácií. Cieľom je poskytnúť jasné pravidlá a podmienky na ochranu limitovaných informácií.

K bodu 2 a 4:

Medzi základné pojmy sa dopĺňa vedúci, ktorý bol pôvodne v zákone zavedený len ako legislatívna skratka v § 8 ods. 1. Dôvodom je potreba rozšírenia použitia pojmu „vedúci“ aj na limitované informácie.

K bodu 3:

V súlade s praktickými požiadavkami orgánov štátnej správy sa navrhuje jednotná úprava limitovanej informácii. Cieľom je poskytnúť jasné pravidlá a podmienky na ich ochranu. Základným princípom, na ktorom je limitovaná informácia založená, je zásada „potreba poznať“ („need-to-know“), povinnosť zachovať mlčanlivosť, znalosť pravidiel manipulácie a ich dodržiavanie. Z tohto dôvodu limitovanú informáciu nemožno sprístupniť neurčitému okruhu osôb a táto informácia nepodlieha zverejneniu podľa zákona o slobode informácií. Zavádza sa fakultatívna možnosť pre vedúceho rozhodnúť vo vymedzených oblastiach o limitovanej informácii; zároveň sa ustanovuje možnosť, aby takúto informáciu určil aj kritický subjekt, a to na účel zabezpečenia ochrany kritickej infraštruktúry. Zavádza sa spôsob označovania takejto informácie, subjekt zodpovedný za jej sprístupnenie a ochranu, ako aj povinnosti subjektu vo vzťahu k vedeniu zoznamov limitovaných informácií a zverejňovania zásad ich manipulácie.

Rozhodnúť o určení limitovanej informácie môže vedúci, ktorým na účely zákona je štatutárny orgán orgánu verejnej moci, alebo kritický subjekt, ak ide o potrebu zabezpečenia ochrany kritickej infraštruktúry. Kritický subjekt je následne povinný upovedomiť o tom ústredný orgán na úseku kritickej infraštruktúry (príslušný ústredný orgán štátnej správy).

Predmetné ustanovenia ďalej upravujú oblasti, v ktorých limitovaná informácia môže vzniknúť, a to jednak vecné ako aj ich materiálne vymedzenie. V odseku 1 písm. a) je vecným vymedzením limitovaných informácií to, že sa týkajú utajovaných skutočností a materiálnou podmienkou možné ohrozenie činnosti záujmov Slovenskej republiky. Samotný moment vzniku utajovanej skutočnosti totiž jej pôvodca nie vždy vie jednoznačne a presne stanoviť, a práve v takýchto prípadoch, tzn. do momentu rozhodnutia o utajení informácie, je opodstatnené zabezpečiť aspoň minimálnu ochranu takejto informácie jej určením za limitovanú informáciu. Môže ísť napríklad o špecifickú činnosť, úkon alebo rokovanie, ktorého výsledkom bude vznik utajovanej skutočnosti. Rovnako však takými informáciami, ktoré nedosahujú úroveň utajovaných skutočností môžu byť aj rôzne čiastkové informácie alebo podkladové materiály, na základe ktorých utajovaná skutočnosť vzniká, prípadne technické parametre alebo bezpečnostné nastavenia napríklad zariadení, na ktorých sa spracúvajú a ukladajú utajované skutočnosti. V odseku 1 písm. b) sa vecne vymedzujú informácie týkajúce sa činnosti a organizácie orgánu verejnej moci alebo subjektu plniaceho úlohy v oblasti verejného poriadku, bezpečnosti a obrany Slovenskej republiky a materiálnou podmienkou je ohrozenie, obmedzenie alebo znemožnenie plnenia týchto úloh. Určiť informáciu ako limitovanú podľa odseku 1 písm. b) je možné len v oblastiach určených nariadením vlády Slovenskej republiky. V odseku 1 písm. c) je tiež jasne stanovené vecné vymedzenie, že sú to informácie o kritickej infraštruktúre, ako aj materiálna podmienka možnosti ohrozenia poskytovania základnej služby kritickým subjektom.

Zákon o ochrane utajovaných skutočností zakazuje utajovať skutočnosti, ktoré sú predmetom legitímneho záujmu verejnosti a v kontexte uvedeného sa ustanovuje (odsek 5), že zákaz utajovania niektorých informácií sa rovnako vzťahuje aj na limitovanú informáciu.

Ten subjekt, ktorý určil informáciu za limitovanú, je v súlade so zásadami manipulácie s limitovanými informáciami zverejnenými na vlastnom webovom sídle zodpovedný za stanovenie podmienok manipulácie, ako aj o jej distribúcii a adresátoch, ktorými môžu byť tak právnické osoby, ale i konkrétne fyzické osoby. O tom, kto v rámci orgánu verejnej moci, resp. v kritickom subjekte môže rozhodnúť o poskytnutí limitovanej informácie, je na samotnom rozhodnutí vedúceho. Zo skúseností z aplikačnej praxe sa odporúča vykonať takéto rozhodnutie prostredníctvom interného aktu riadenia.

Právna úprava limitovanej informácie bola inšpirovaná aj pravidlami Európskej únie, jej členských štátov a Organizácie Severoatlantickej zmluvy vo vzťahu k používaniu neverejných informácií. Z uvedeného dôvodu uvádzame niektoré z týchto pravidiel.

EURÓPSKA ÚNIA (EÚ). Dokumenty EÚ s označením „LIMITE“ sa považujú za dokumenty, na ktoré sa vzťahuje povinnosť zachovávať služobné tajomstvo v súlade s článkom 339 Zmluvy o fungovaní Európskej únie (ZFEÚ) a článkom 6 ods. 1 rokovacieho poriadku Rady. Okrem toho sa pri ich manipulácii musia dodržiavať príslušné právne predpisy EÚ, najmä nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie. V roku 2018 schválila Rada (EÚ) usmernenie pre manipuláciu s internými dokumentmi Rady (č. 7695/18) podľa ktorého platí, že tieto dokumenty nie sú určené pre verejnosť (nezverejňujú sa v médiách, na internete a neuvoľňujú sa pre oboznamovanie sa občanov). Pri zachovaní pravidiel ukladania a zachovania ich integrity je možné ich postupovať iným inštitúciám pre výkon ich povinností a právomocí. Dokument je možné zaslať osobe len po ubezpečení sa o jej identite (t. j. že pochádza zo subjektu, ktorý je oprávnený mať k takémuto dokumentu prístup). Podmienkou oboznámenia sa osoby je zásada „need-to-know“. EÚ dlhodobo pripravuje dokument, ktorého súčasťou je aj časť o neutajovaných informáciách (NON-CLASSIFIED INFORMATION). Momentálne sa uvažuje o dvoch stupňoch týchto informácií, konkrétne „EU INTERNAL NON-CLASSIFIED“ (EÚ interné neutajované informácie) a „EU PUBLIC“ (verejné informácie). Zámerom je stanoviť jednotné pravidlá ochrany týchto informácií pre všetky EÚ inštitúcie (prijatím predmetného nariadenia sa prejde z „EU LIMITÉ“ na „EU INTERNAL NON-CLASSIFIED“). Bezpečnostné pravidlá a ochrana týchto informácií zostane na rovnakej úrovni, t. j. tieto informácie sú určené na použitie subjektom EÚ pri výkone ich funkcií, nie sú verejné, ale ani utajované. Na takéto informácie sa vzťahuje povinnosť zachovávať služobné tajomstvo. Interné neutajované informácie sa môžu vymieňať mimo subjektov EÚ len s fyzickými alebo právnickými osobami, ktoré ich potrebujú poznať, čiže základnou podmienkou ich sprístupnenia je zásada „need-to-know“.

FRANCÚZSKA REPUBLIKA. Ochrana poskytnutá dokumentom a nosičom s označením „Restricted Diffusion“ nie je tajomstvom národnej obrany. Toto ochranné označenie upozorňuje, že dokument alebo nosič obsahuje citlivé informácie, pričom tento nie je utajovanou skutočnosťou, používatelia musia dodržať určitú diskretnosť a pravidlá na špecifickú ochranu. Manipulácia s „Diffusion Resteinte“ nevyžaduje bezpečnostnú previerku osoby, ale prístup k týmto informáciám majú len ľudia na základe zásady „Potreba poznať“ (need-to-known). Toto označenie možno použiť napríklad pri informáciách, ktoré by mohli podkopávať vedenie zahraničnej politiky Francúzska, štátnej bezpečnosti, verejnej bezpečnosti, osobnej bezpečnosti alebo bezpečnosti informačných systémov verejnej správy. Na vytváranie

týchto informácií je možné použiť schválený informačný systém pre úroveň „Diffusion Restreinte“ alebo pre utajované skutočnosti.

ORGANIZÁCIA SEVEROATLANTICKEJ ZMLUVY (NATO). Vedenie a dohľad nad neutajovanými informáciami NATO a informáciami, ktoré sú citlivé, nie však utajované upravuje Bezpečnostná politika NATO C-M(2002)60 z 23. júla 2002 o riadení neutajovaných informácií NATO. Informácie označené ako „NATO UNCLASSIFIED“ (NU) sa môžu používať len na oficiálne účely a prístup k nim môžu mať len osoby, orgány alebo organizácie, ktoré ich potrebujú na základe zásady „need-to-know“. Informácie NATO, ktoré sa však môžu zverejniť (RELEASABLE TO PUBLIC) nemajú žiadne označenie a keďže boli preskúmané v súlade s postupmi a pravidlami NATO alebo vnútroštátnymi postupmi, je možné ich zverejniť. Všetky informácie NATO vyžadujú takú ochranu, ktorá zabezpečí ich integritu a dostupnosť. Rovnako sa to týka aj informácií NATO, ktoré sú uvoľňované verejnosti (napr. uvoľnenie médiám). Zmena ich obsahu (strata integrity) alebo odmietnutie legitímneho prístupu k nim (strata dostupnosti) by mohli zapríčiniť škodu záujmom NATO.

Spoločným menovateľom pre prístup osôb k limitovaným informáciám a ich oboznámeniu sa je teda jej „potreba poznať“ („need-to-know“), povinnosť zachovať mlčanlivosť, znalosť pravidiel manipulácie a ich dodržiavanie; za daným účelom právny predpis nevyžaduje splnenie iných špeciálnych podmienok, napr. bezúhonnosť osoby, bezpečnostná previerka alebo vykonanie záznamu o určení osoby.

V prípade distribúcie elektronickej limitovanej informácie je nutné sa vopred uistiť, že jej príjemcom je konkrétna odosielateľovi známa osoba.

Ustanovuje sa povinnosť pre subjekt, ktorý určil limitovanú informáciu, aby viedol zoznam limitovaných informácií. V danom prípade nejde o zoznam, ktorý by bol ekvivalentný zoznamu utajovaných skutočností v zmysle § 2 nariadenia vlády č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností. Naopak takýmto súhrnným zoznamom limitovaných informácií sa myslia konkrétne registrátorne záznamy, ktoré orgán verejnej moci alebo kritický subjekt určil ako limitované informácie spolu s odôvodnením takéhoto určenia.

Rovnako sa ustanovuje povinnosť pre úrad zverejniť na svojom webovom sídle základné princípy manipulácie s limitovanou informáciou, ktoré upravujú minimálne bezpečnostné opatrenia na zabezpečenie ochrany limitovaných informácií. Predbežný návrh týchto zásad prikladáme.

## I. ČASŤ – ZÁKLADNÉ PRAVIDLÁ

1. Ochranu limitovanej informácie počas manipulácie zabezpečuje osoba, ktorá má udelený prístup k limitovanej informácii najmä tým, že neumožní jej sprístupnenie neoprávnenej osobe.

## II. ČASŤ - OZNAČOVANIE

2. Každá limitovaná informácia sa označuje slovom „Limit“ už pri jej vytváraní a to na každej strane v hornej a dolnej časti; prázdne strany sa tak neoznačujú. Ak limitovaná informácia obsahuje prílohu, ktorá obsahuje limitovanú informáciu, príloha sa označuje podľa prvej vety. Ak sa limitovaná informácia skladá z rôznych častí, časť obsahujúca limitovanú informáciu sa môže označiť na začiatku a na konci takejto časti slovom „Limit“ v hranatých zátvorkách. Označenie limitovanej informácie v elektronickej podobe sa

vykoná tak, že je možné identifikovať limitovanú informáciu bez nutnosti oboznámenia sa s jej obsahom (pozn. napríklad priamo v názve súboru).

3. Ten, kto limitovanú informáciu určil, môže rozhodnúť o osobitných požiadavkách alebo obmedzeniach manipulácie, a to najmä o rozsahu a spôsobe distribúcie, ktoré sa uvedú na prvej strane limitovanej informácie spravidla pod označenie „Limit“; len ten, kto limitovanú informáciu určil, môže rozhodnúť o zmene alebo zrušení osobitných požiadaviek alebo obmedzení manipulácie. Každá zmena alebo zrušenie osobitných požiadaviek alebo obmedzení manipulácie sa neodkladne a preukázateľne oznamuje všetkým adresátom; adresát preukázateľne oboznámi všetky osoby, ktoré majú prístup k limitovanej informácii.
4. Ak ten, kto určil limitovanú informáciu rozhodne o zrušení takéhoto určenia, vyznačí sa to zreteľne na limitovanej informácii tak, aby bolo zrejmé pôvodné označenie a oznámi zrušenie takéhoto určenia všetkým adresátom, ktorým bola limitovaná informácia doručená.

### III. ČASŤ – UKLADANIE

5. Limitovaná informácia sa ukladá v priestoroch právnickej osoby v zamknutom úschovnom objekte (nábytku). Ak je to nevyhnutné, limitovanú informáciu je možné vyniesť mimo priestory právnickej osoby s tým, že osoba s prístupom k limitovanej informácii má túto informáciu pod neustálym dozorom alebo je zabezpečená v zamknutom úschovnom objekte (nábytku).

### IV. ČASŤ - DISTRIBÚCIA

6. Limitovanú informáciu je možné spracovať a distribuovať prostredníctvom technických zariadení, ktoré musia zabezpečovať najmenej jednoznačnú identifikáciu používateľa. Ak je nevyhnutné zaslať limitovanú informáciu elektronicky masovokomunikačnými prostriedkami (mail, fax) alebo iným obdobným spôsobom (poštovým podnikom), musí byť odosielateľovi známa menovite osoba príjemcu alebo jeho funkcia. Pri zasielaní limitovanej informácie poštovým podnikom sa na obale vyznačí menovite osoba príjemcu alebo jeho funkcia, adresa odosielateľa, pričom sa na obale neuvádza označenie „Limit“.
7. Ak komunikačné a informačné systémy, pomocou ktorých sa manipuluje s limitovanou informáciou, splňajú požiadavku na zabezpečenie integrity, dôvernosti a dostupnosti limitovanej informácie, tak sa nevyžadujú prísnejšie technické opatrenia na zabezpečenie ochrany ako štandardné opatrenia na ochranu siete.

### V. ČASŤ – ĎALŠIE OPATRENIA

8. Limitovanú informáciu je možné rozmnožiť, vyhotoviť preklad alebo transformovať do inej podoby, ak ten, kto ju za limitovanú informáciu určil, to v pokynoch na manipuláciu s limitovanou informáciou alebo v osobitných požiadavkách alebo obmedzeniach manipulácie podľa odseku 3 neuviedol inak; v takom prípade iba na základe preukázateľného súhlasu toho, kto určil limitovanú informáciu.
9. Na manipuláciu s limitovanou informáciou, ktorá je registratúrnym záznamom sa vzťahuje osobitný predpis. Ochrana takejto limitovanej informácie, ktorá je označená trvalou dokumentárnou hodnotou („A“), zabezpečí právnická osoba, v pôsobnosti ktorej sa limitovaná informácia nachádza (pozn. neodovzdáva sa príslušnému archívu); to neplatí, ak určenie za limitovanú informáciu je zrušené.

K bodu 5:

Formálna úprava textu.

K bodu 6:

Medzi povinnosti nepovolanej osoby pri získaní informácie alebo nájdení veci, ktorá je utajovaná, sa dopĺňa, že sa uvedené vzťahuje aj na limitované informácie.

K bodu 7:

Upravuje sa postavenie Slovenskej informačnej služby, Vojenského spravodajstva a Policajného zboru vo vzťahu k limitovanej informácii.

## Čl. V-IX

Legislatívno-technická úprava v súvislosti s precizovaním terminológie a pojmológie. V poznámkach a referenciách, kde sa upravuje vzťah k niektorým osobitným zákonom sa slová „prvkom kritickej infraštruktúry“ nahrádzajú slovami „kritickou infraštruktúrou“, ďalej slová „citlivou informáciou o kritickej infraštruktúre“ nahrádzajú slovami „limitovanou informáciou o kritickej infraštruktúre“.

Navrhované zmeny zákona č. 497/2022 Z. z. o preverovaní zahraničných investícií a o zmene a doplnení niektorých zákonov v znení zákona č. 95/2023 Z. z. nadväzujú na novú právnu úpravu v oblasti kritickej infraštruktúry.

V bode 1. a 2. je zohľadnené zavedenie inštitútu limitovanej informácie v zákone č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov. Okruh údajov z informačných systémov verejnej správy, ktoré sú vyňaté z oprávnenia Ministerstva hospodárstva SR na prístup pri vykonávaní agendy preverovania zahraničných investícií, sa tak mení z utajovaných skutočností a citlivých informácií na utajované skutočnosti, citlivé informácie a limitované informácie.

Bod 3. reflektuje na vypustenie úpravy týkajúcej sa oprávnenia Ministerstva hospodárstva SR preveriť určitý okruh prevodov a prechodov kritickej infraštruktúry v sektoroch energetika a priemysel (z dôvodu ochrany bezpečnosti a verejného poriadku Slovenskej republiky a bezpečnosti a verejného poriadku Európskej únie) z legislatívy upravujúcej kritickú infraštruktúru a jej ponechanie výlučne v zákone č. 497/2022 Z. z. o preverovaní zahraničných investícií a o zmene a doplnení niektorých zákonov v znení zákona č. 95/2023 Z. z.

Úprava pôvodne obsiahnutá v § 9a zákona č. 45/2011 Z. z. o kritickej infraštruktúre mala skôr informatívny charakter a pre oprávnenie Ministerstva hospodárstva SR preveriť určitý okruh prevodov a prechodov kritickej infraštruktúry bol rozhodujúci zákon č. 497/2022 Z. z. o preverovaní zahraničných investícií a o zmene a doplnení niektorých zákonov v znení zákona č. 95/2023 Z. z. Uvedené bolo zohľadnené pri príprave nového zákona o kritickej infraštruktúre.

Týmto spôsobom bol zachovaný status quo pokiaľ ide o rozsah oprávnenia Ministerstva hospodárstva SR preveriť určité prevody a prechody kritickej infraštruktúry z dôvodu ochrany bezpečnosti a verejného poriadku Slovenskej republiky a bezpečnosti a verejného poriadku Európskej únie, skutočnosť, že dané preverenie sa vzťahuje aj na prevody a prechody, kde na strane nadobúdateľa (na strane „nového“ kritického subjektu) vystupuje fyzická osoba, ktorá je občanom Európskej únie, fyzická osoba-podnikateľ s miestom podnikania v Európskej únii alebo právnická osoba so sídlom v Európskej únii, ako aj pokiaľ ide o spôsob, akým sa preverenie realizuje. Zachovanie statusu quo v tejto oblasti je nevyhnutnou reflexiou na pretrvávajúce trendy v realizácii strategických a predátorských investícií, hybridné pôsobenie aktérov z tretích krajín v kritických sektoroch, ako aj ďalšie okolnosti geopolitického diania prispievajúce k eskalácii napätia, ktoré odôvodňujú požiadavku na zvýšenie obozretnosti, a to aj prostredníctvom zachovania a využívania tohto typu spôsobilosti štátu.

Čl. X  
(účinnosť)

Navrhuje sa účinnosť 1. januára 2025 tak, aby zákon o kritickej infraštruktúre a novela zákona o kybernetickej bezpečnosti nadobudli účinnosť naraz.

K prílohe č. 1

V súlade s § 9 návrhu zákona sa ustanovujú sektory vrátane podsektorov kritickej infraštruktúry s uvedením príslušného ústredného orgánu štátnej správy, do ktorých sa budú zaraďovať kritické subjekty podľa stanoveného postupu a kritérií podľa § 14 ods. 3.

K prílohe č. 2

Ide o transpozičnú prílohu s presným označením zoznamu preberaných právnych aktov a údajmi o ich nahradení, spolu s informáciami o ich publikácií.