**Vyhodnotenie medzirezortného pripomienkového konania**

Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

|  |  |
| --- | --- |
| Spôsob pripomienkového konania | Bežný, 15 pracovných dní (26.5.-15.6.2017) |
| Počet vznesených pripomienok, z toho zásadných | 706 /236 |
| Počet vyhodnotených pripomienok | 706 |
|  |  |
| Počet akceptovaných pripomienok, z toho zásadných | 429 /141 |
| Počet čiastočne akceptovaných pripomienok, z toho zásadných | 55 /20 |
| Počet neakceptovaných pripomienok, z toho zásadných | 221 /75 |
|  |  |
| Rozporové konanie (s kým, kedy, s akým výsledkom) | (19.9.-6.10.2017) všetky rozpory odstránené |
| Počet odstránených pripomienok | 95 |
| Počet neodstránených pripomienok | 0 |

Sumarizácia vznesených pripomienok podľa subjektov

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Č.** | **Subjekt** | **Pripomienky do termínu** | **Pripomienky po termíne** | **Nemali pripomienky** | **Vôbec nezaslali** |
| 1. | Agentúra pre riadenie dlhu a likvidity | 15 (8o,7z) | 0 (0o,0z) |  |  |
| 2. | Asociácia zamestnávatelských zväzov a združení Slovenskej republiky | 1 (1o,0z) | 0 (0o,0z) |  |  |
| 3. | DataCentrum elektronizácie územnej samosprávy Slovenska | 4 (3o,1z) | 0 (0o,0z) |  |  |
| 4. | DÔVERA zdravotná poisťovňa, a. s. | 1 (0o,1z) | 0 (0o,0z) |  |  |
| 5. | Generálna prokuratúra Slovenskej republiky | 32 (17o,15z) | 0 (0o,0z) |  |  |
| 6. | Ministerstvo dopravy a výstavby Slovenskej republiky | 13 (7o,6z) | 0 (0o,0z) |  |  |
| 7. | Ministerstvo financií Slovenskej republiky | 43 (23o,20z) | 0 (0o,0z) |  |  |
| 8. | Ministerstvo hospodárstva Slovenskej republiky | 19 (11o,8z) | 0 (0o,0z) |  |  |
| 9. | Ministerstvo kultúry Slovenskej republiky | 36 (36o,0z) | 0 (0o,0z) |  |  |
| 10. | Ministerstvo obrany Slovenskej republiky | 58 (22o,36z) | 0 (0o,0z) |  |  |
| 11. | Ministerstvo pôdohospodárstva a rozvoja vidieka Slovenskej republiky | 18 (18o,0z) | 0 (0o,0z) |  |  |
| 12. | Ministerstvo práce, sociálnych vecí a rodiny Slovenskej republiky | 2 (2o,0z) | 0 (0o,0z) |  |  |
| 13. | Ministerstvo spravodlivosti Slovenskej republiky | 14 (7o,7z) | 0 (0o,0z) |  |  |
| 14. | Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky | 28 (25o,3z) | 0 (0o,0z) |  |  |
| 15. | Ministerstvo vnútra Slovenskej republiky | 25 (18o,7z) | 0 (0o,0z) |  |  |
| 16. | Ministerstvo zdravotníctva Slovenskej republiky | 2 (0o,2z) | 0 (0o,0z) |  |  |
| 17. | Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky | 36 (28o,8z) | 0 (0o,0z) |  |  |
| 18. | Ministerstvo životného prostredia Slovenskej republiky | 41 (39o,2z) | 0 (0o,0z) |  |  |
| 19. | Národná banka Slovenska | 30 (22o,8z) | 0 (0o,0z) |  |  |
| 20. | Odbor aproximácie práva sekcie vládnej legislatívy Úradu vlády SR | 10 (10o,0z) | 0 (0o,0z) |  |  |
| 21. | Protimonopolný úrad Slovenskej republiky | 1 (1o,0z) | 0 (0o,0z) |  |  |
| 22. | Republiková únia zamestnávateľov | 21 (2o,19z) | 0 (0o,0z) |  |  |
| 23. | Slovenská banková asociácia | 23 (10o,13z) | 0 (0o,0z) |  |  |
| 24. | Slovenská informačná služba | 7 (0o,7z) | 0 (0o,0z) |  |  |
| 25. | Slovenská asociácia poisťovní | 1 (1o,0z) | 0 (0o,0z) |  |  |
| 26. | Slovensko.Digital | 7 (0o,7z) | 0 (0o,0z) |  |  |
| 27. | Sociálna poisťovňa, Ul. 29 augusta č. 8 a 10, 813 63 Bratislava 1 | 16 (16o,0z) | 0 (0o,0z) |  |  |
| 28. | Štatistický úrad Slovenskej republiky | 30 (30o,0z) | 0 (0o,0z) |  |  |
| 29. | Úrad jadrového dozoru Slovenskej republiky | 30 (21o,9z) | 0 (0o,0z) |  |  |
| 30. | Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky | 1 (1o,0z) | 0 (0o,0z) |  |  |
| 31. | Úrad na ochranu osobných údajov Slovenskej republiky | 8 (2o,6z) | 0 (0o,0z) |  |  |
| 32. | Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu | 57 (35o,22z) | 0 (0o,0z) |  |  |
| 33. | Úrad pre reguláciu elektronických komunikácií a poštových služieb | 10 (3o,7z) | 0 (0o,0z) |  |  |
| 34. | Úrad priemyselného vlastníctva Slovenskej republiky | 1 (1o,0z) | 0 (0o,0z) |  |  |
| 35. | Úrad pre verejné obstarávanie | 2 (2o,0z) | 0 (0o,0z) |  |  |
| 36. | Úrad vlády Slovenskej republiky | 41 (27o,14z) | 0 (0o,0z) |  |  |
| 37. | Verejnosť | 17 (17o,0z) | 0 (0o,0z) |  |  |
| 38. | Všeobecná zdravotná poisťovňa, a. s. | 4 (4o,0z) | 0 (0o,0z) |  |  |
| 39. | Združenie poskytovateľov webhostingu | 1 (0o,1z) | 0 (0o,0z) |  |  |
| 40. | Úrad pre reguláciu sieťových odvetví | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 41. | Úrad geodézie, kartografie a katastra Slovenskej republiky | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 42. | Správa štátnych hmotných rezerv Slovenskej republiky | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 43. | Národný bezpečnostný úrad | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 44. | Najvyšší kontrolný úrad Slovenskej republiky | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 45. | Najvyšší súd Slovenskej republiky | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 46. | Národná rada Slovenskej republiky | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 47. | Kancelária Ústavného súdu Slovenskej republiky | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 48. | Kancelária prezidenta Slovenskej republiky | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 49. | Slovenská poľnohospodárska a potravinárska komora | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 50. | Združenie miest a obcí Slovenska | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 51. | Splnomocnenec vlády Slovenskej republiky pre rómske komunity | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 52. | Konfederácia odborových zväzov Slovenskej republiky | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 53. | Úrad pre dohľad nad zdravotnou starostlivosťou | 0 (0o,0z) | 0 (0o,0z) |  | x |
| 54. | Konferencia biskupov Slovenska | 0 (0o,0z) | 0 (0o,0z) |  | x |
|  | Spolu | 706 (470o,236z) | 0 (0o,0z) |  |  |

Vyhodnotenie vecných pripomienok je uvedené v tabuľkovej časti.

|  |  |
| --- | --- |
| Vysvetlivky k použitým skratkám v tabuľke: | |
| O – obyčajná | A – akceptovaná |
| Z – zásadná | N – neakceptovaná |
|  | ČA – čiastočne akceptovaná |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Subjekt** | **Pripomienka** | **Typ** | **Vyh.** | **Spôsob vyhodnotenia** |
| **ARDAL** | **návrhu zákona ako celku** 1. Predkladaný návrh uvádza opakovane neurčité právne pojmy, ktoré sám nevymedzuje a ktoré nie sú v platných právnych predpisoch ustálené. Predkladateľ by mal preto v súlade s platnými Legislatívnymi pravidlami vlády SR znížiť mieru neurčitosti týchto pojmov v záujme predchádzania neskorším výkladovým problémom pri uplatňovaní zákona po jeho schválení. | Z | A |  |
| **ARDAL** | **ustanovenie § 27 ods. 5 návrhu zákona** 10. V nadväznosti na právomoci vecne príslušnej autority podľa § 11 návrhu zákona o kybernetickej bezpečnosti navrhujeme doplniť znenie ustanovenia § 27 ods. 5 nasledovne: „Vecne príslušná autorita v súčinnosti s prevádzkovateľom základnej služby alebo poskytovateľom digitálnej služby sú povinní bez zbytočného odkladu oznámiť úradu prostredníctvom jednotného informačného systému kybernetickej bezpečnosti vykonanie reaktívneho opatrenia...“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že vecne príslušná autorita nemá k dispozícii informačný systém. Je to prakticky nevykonateľné. |
| **ARDAL** | **ustanovenie § 29 návrhu zákona** 11. Navrhujeme zvážiť postúpenie právomoci vykonávať kontrolu podľa § 29 návrhu zákona o kybernetickej bezpečnosti z úradu na vecne príslušnú autoritu. Vecne príslušná autorita má tieto kompetencie podľa zákona č. 357/2015 Z. z. o finančnej kontrole a audite. Rovnako, pokiaľ ide o zverenie právomocí úradu, takéto zverenie nie je dostatočne odôvodnené a primerané účelu zákona. Osobitná časť dôvodovej správy by mala byť preto primerane doplnená. | O | A | Text nahradený novým znením a preformulovaný aj vzhľadom na pripomienky ostatných subjektov. |
| **ARDAL** | **ustanovenie § 29 ods. 9 návrhu zákona**  12. Navrhujeme uviesť znenie ustanovenia § 29 ods. 9 návrhu zákona do súladu s kompetenciami orgánov kontroly podľa zákona č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov nasledovne: „Príslušníci úradu sú oprávnení v súvislosti s výkonom kontroly ukladať kontrolovanému subjektu poriadkovú pokutu 100 eur za sťaženie výkonu kontroly alebo za marenie výkonu kontroly. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná z dôvodu nahradenia novým znením textu, ktorý bol preformulovaný aj vzhľadom na pripomienky ostatných subjektov. |
| **ARDAL** | **ustanovenie § 30 ods. 1, in fine návrhu zákona** 13. Navrhujeme vypustiť odkaz na zákon č. 357/2015 Z. z. o finančnej kontrole a audite uvádzaný v ustanovení § 30 ods. 1, in fine návrhu zákona v znení: „Opakované audity v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov sa vykonávajú spôsobom podľa osobitného predpisu – zákon č. 357/2015 Z. z. o finančnej kontrole a audite“. Uvádzaný zákon č. 357/2015 Z. z. o finančnej kontrole a audite nie je na vykonávanie auditu kybernetickej bezpečnosti uplatniteľný. | O | A | Text nahradený novým znením a preformulovaný aj vzhľadom na pripomienky ostatných subjektov. |
| **ARDAL** | **ustanovenie § 30 ods. 2 návrhu zákona**  14. Navrhujeme vypustiť povinnosť prevádzkovateľa základnej služby predložiť úplný obsah záverečnej správy o výsledkoch auditu úradu ... do 30 dní od ukončenia auditu podľa ustanovenia § 30 ods. 2 návrhu zákona z dôvodu, že takáto správa bude alebo môže obsahovať chránené informácie a jej predloženie pri súčasnom neurčení zodpovedajúcich záruk neprimerane navýši riziká informačnej bezpečnosti prevádzkovateľov základnej služby. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu reálnej neodôvodnenosti a zjavnej neprimeranosti obsahu a účelu zákona. |
| **ARDAL** | **ustanovenie § 31 ods. 1 písm. d) návrhu zákona** 15. Navrhujeme vypustiť priestupok podľa § 31 ods. 1 písm. d) návrhu zákona, ktorého sa môže dopustiť fyzická osoba, ktorá neposkytla úradu požadovanú súčinnosť pri výkone kontroly podľa navrhovaného zákona. Orgány kontroly podľa základných pravidiel kontrolnej činnosti ukladajú poriadkovú pokutu kontrolovanému subjektu, nie fyzickým osobám, ktoré by znemožnili priebeh kontroly, marili výsledok kontroly alebo nápravu zistených nedostatkov. Neposkytnutie požadovanej súčinnosti pri výkone kontroly úradom zo strany fyzickej osoby je nerešpektuje pravidlá zodpovednosti štátnych zamestnancov a výška pokuty za takýto priestupok až do výšky 5000 eur sa javí ako neprimeraná. | O | A |  |
| **ARDAL** | **ustanovenie § 6 ods. 2 návrhu zákona**  2. Navrhujeme úplne vylúčiť znenie ustanovenia § 6 ods. 2 z návrhu zákona „Na účely zabezpečenia plnenia úloh podľa tohto zákona môže úrad uzatvoriť dohodu o spolupráci s fyzickou osobou alebo právnickou osobou. Dohoda o spolupráci musí obsahovať konkrétnu formu a podmienky spolupráce. Dohoda o spolupráci nie je povinne zverejňovanou zmluvou“. Namietané znenie návrhu zákona úplne narúša akékoľvek bezpečnostné opatrenia prevádzkovateľa základnej služby v oblasti personálnej a fyzickej bezpečnosti. Podľa tohto návrhu akákoľvek osoba, ktorá bude mať uzatvorenú dohodu s úradom, bude mať kompetenciu oboznamovať sa s akýmikoľvek informáciami. Ak predkladateľ zotrvá na možnosti uzatvoriť dohodu o spolupráci, je potrebné stanoviť konkrétne podmienky, ktoré musí fyzická osoba alebo právnická osoba ako zmluvná strana splniť, vrátane ustanovenia povinnosti preukázania znalosti bezpečnostných a technických štandardov, kvalifikačných predpokladov a zručností v oblasti kybernetickej bezpečnosti. Tiež by mal byť formou písomnej dohody stanovený rozsah informácií, s ktorými bude takáto osoba oprávnená oboznamovať sa u prevádzkovateľa základnej služby a ustanovená povinnosť zachovávať mlčanlivosť o skutočnostiach, s ktorými sa táto osoba oboznámila pri vykonávaní takejto dohody. Taktiež, ak dohoda nie je vylúčená z povinného zverejňovania zmlúv podľa zákona č. 211/2000 Z. z. v znení neskorších predpisov, nezverejnenie tejto dohody je porušením tohto zákona. Aj v prípade nezverejňovaných zmlúv však platí povinnosť zverejniť informáciu o jej uzatvorení (tzv. notifikačná povinnosť). | Z | ČA | Uvedený odsek bol modifikovaný v rámci rozporových konaní tak, aby predstavoval kompromisné riešenie. Bol vypustený medzinárodný rozmer a rovnako tak nepriama novela zákona č. 211/2000 ZZ. Bolo doplnené, že dohoda sa môže uzatvoriť výlučne s FO a nie s podnikateľom a FO musí disponovať platným potvrdením NBÚ o bezpečnostnej previerke na požadovaný stupeň, ak bude teda potrebné. Na uvedenú dohodu sa vzťahuje zákon č. 211/2000 ZZ a je teda povinne zverejňovanou zmluvou. Vami navrhované ustanovenie by teda opätovne znamenalo nepriamu novelu tohto zákona, čo je podľa Legislatívnych pravidiel vlády neprípustné. So znením v navrhovanej podobe vyslovili súhlas všetky zainteresované subjekty. Záver: Z dôvodov vyššie uvedených považuje úrad rozpor za odstránený. |
| **ARDAL** | **ustanovenie § 29 ods. 6 návrhu zákona**  3. Navrhujeme vypustiť znenie § 29 ods. 6 návrhu zákona „Príslušníci úradu sú v súvislosti s výkonom kontroly a v rozsahu potrebnom na jej vykonanie oprávnení vstupovať do komunikačných a informačných systémov do úrovne správcu systému, vrátane oprávnenia dočasne zmeniť hardvérovú alebo softvérovú konfiguráciu. Navrhované znenie § 29 ods. 6 návrhu zákona poskytuje neprimerané kompetencie príslušníkom úradu vrátane neprimeraných zásahov do komunikačných a informačných systémov. V zmysle § 3 ods. 4 zákona 275/2006 Z. z. o informačných systémoch verejnej správy povinné osoby, ktoré sú správcami IS, sú povinné zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy, ktoré sú v ich správe, vrátane organizačného, odborného a technického zabezpečenia a zabezpečovať informačný systém verejnej správy proti zneužitiu. V prípade zmeny hardvérovej alebo softvérovej konfigurácie môže byť zabezpečovanie uvedených povinností ohrozené alebo priamo narušené. Súčasne môže nastať porušenie ustanovení zákona č. 122/2013 Z .z. o ochrane osobných údajov, nakoľko oprávnenie vstupovať do informačného systému na úrovni správcu systému môže mať za následok sprístupnenie osobných údajov dotknutých osôb za predpokladu, že sa v danom informačnom systéme spracúvali osobné údaje. Ak navrhované znenie § 29 ods. 6 zákona o kybernetickej bezpečnosti nebude zrušené, správca IS nemôže zabezpečiť splnenie povinností, ktoré mu ukladá zákon č. 275/2006 Z. z.. Návrh zákona by mal taktiež určiť, kto bude zodpovedný za nefunkčnosť alebo narušenie funkčnosti IS po zmene hardvérovej alebo softvérovej konfigurácie a kto bude znášať nepriaznivé následky s tým spojené, vrátane náhrady škody spôsobenej tretím osobám. | Z | A |  |
| **ARDAL** | **ustanovenie § 30 ods. 1 návrhu zákona**  4. Navrhujeme zmeniť znenie prvej vety ustanovenia § 30 ods. 1 návrhu zákona nasledovne: „Prevádzkovateľ základnej služby je povinný umožniť a podrobiť sa auditu kybernetickej bezpečnosti do 24 mesiacov odo dňa zápisu ... Prevádzkovateľ základnej služby je povinný vykonať audit kybernetickej bezpečnosti do 24 mesiacov odo dňa zápisu ...“. V zmysle tejto zmeny prevádzkovateľ bude povinný a oprávnený vykonať audit v súčinnosti s osobou podľa ustanovenia § 30 ods. 3 návrhu zákona o kybernetickej bezpečnosti, to znamená nezávislou a odborne spôsobilou osobou, ktorá má preukázateľnú prax s auditom informačnej bezpečnosti. Taktiež, ak náklady na audit podľa ustanovenia § 30 ods. 4 návrhu zákona znáša prevádzkovateľ základnej služby, zodpovednosť za výber odborne spôsobilého audítora by mal niesť výlučne prevádzkovateľ základnej služby a nie sa „podrobiť auditu“ vykonávanému osobou, ktorá mu bola určená úradom, ako je to navrhované v ustanovení § 30 ods. 1 návrhu zákona. | Z | A | Text primerane preformulovaný pri dodržaní zásad legislatívnej techniky. Subjekty s ustanovením vyjadrili súhlas. |
| **ARDAL** | **Príloha č. 1** 5. V prílohe č. 1 Sektor : Finančný sektor/Financie navrhujeme preformulovať označenie prevádzkovateľa základnej služby „Štátna pokladnica“ na „Štátna pokladnica, Agentúra pre riadenie dlhu a likvidity a Datacentrum“ . Uvedenú zmenu navrhujeme z dôvodu zaradenia Agentúry pre riadenie dlhu a likvidity a Štátnej pokladnice medzi prvky kritickej infraštruktúry v zmysle zákona č. 45/2011 Z. z. o kritickej infraštruktúre. Následkom narušenia bezpečnosti informačných systémov systému štátnej pokladnice by bolo znemožnené vykonávať činnosti Agentúry pre riadenie dlhu a likvidity v zmysle zákona č. 291/2002 Z. z. o Štátnej pokladnici a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Strata dôvernosti dát, zničenie dát alebo prelomenie integrity informačných systémov systému štátnej pokladnice by znemožnilo zabezpečovať špecifické finančné funkcie a úlohy Slovenskej republiky zastupovanej Agentúrou pre riadenie dlhu a likvidity. Činnosti uskutočňované ARDAL vyžadujú vysokú mieru dostupnosti a dôvery. V prípade ich nedostupnosti hrozí riziko finančného „defaultu“, zvýšenie reputačného rizika a následne vážne poškodenie ekonomických záujmov SR. | Z | A | Nahradené slovami: „správcovia a prevádzkovatelia systému štátnej pokladnice“. Záver: Rozpor odstránený. |
| **ARDAL** | **Príloha č. 3** 6. V prílohe č. 3 k zákonu č. 45/2011 Z. z. o kritickej infraštruktúre Sektory v pôsobnosti ústredných orgánov doplniť skupinu č. 9: Sektor: Štátna pokladnica, Agentúra pre riadenie dlhu a likvidity; Podsektor : systém štátnej pokladnice; Ústredný orgán : Ministerstvo financií SR. Pozri bod 5 vyššie. Agentúra pre riadenie dlhu a likvidity a Štátna pokladnica boli zaradené medzi prvky kritickej infraštruktúry v zmysle zákona č. 45/2011 Z. z. o kritickej infraštruktúre. Navrhnuté sektory sú klasifikované v inom rozsahu ako tie v kritickej infraštruktúre a aj smernici, ktorú tento návrh transponuje. | Z | N | Na základe rozporového konania s MV SR a MF SR bola upravená príloha č. 3 k zákonu o KI a primerane bola upravená príloha č. 1 k zákonu o KB v súlade so smernicou NIS, príloha kopíruje KI a rozširuje sa o národné špecifiká. Pripomienku teda z dôvodu vypustenia uvedeného sektoru nie je možné akceptovať. Záver: Rozpor odstránený. |
| **ARDAL** | **ustanovenie § 33 návrhu zákona** 7. Navrhujeme doplniť znenie návrhu zákona o znenie všeobecne záväzného právneho predpisu podľa ustanovenia § 33 návrhu zákona už v tejto etape legislatívneho procesu. Máme za to, že v súčasnosti nie je možné identifikovať rozsah a nastavenie postupov, činností a pravidiel, ktoré sa u prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb bude obligatórne pod ťarchou uplatnenia pokút vyžadovať. Pritom v etape medzirezortného pripomienkovania zákona nemajú žiadnu informáciu o ich rozsahu a predpoklade ich splnenia a nastavenia vo svojej organizácii, napr. prahové hodnoty pre identifikáciu základnej služby, obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie prevádzkovateľa základnej služby, kategórie a prahové hodnoty kybernetických bezpečnostných incidentov, podrobnosti o požiadavkách na audit, opakovaný audit a rozsah auditu, bezpečnostné štandardy a znalostné štandardy v oblasti kybernetickej bezpečnosti, klasifikáciu informácií a kategorizáciu sietí a informačných systémov, podrobnosti o vymieňaní informácií a osobných údajov s orgánmi členských štátov Európskej únie. | Z | A | Tézy vykonávacích predpisov budú súčasťou nasledujúceho legislatívneho procesu, budú premietnuté v dôvodovej správe a do účinnosti zákona sa predpokladá aj prijatie vykonávacieho predpisu. |
| **ARDAL** | **ustanovenie § 5 ods. c) návrhu zákona**  8. Navrhujeme doplniť znenie § 5 písm. c) návrhu zákona o kybernetickej bezpečnosti v nadväznosti na ustanovenia zákona č. 575/2001 Z. z. (Kompetenčný zákon), a ako vecne príslušnú autoritu uviesť aj Úrad podpredsedu vlády pre investície a informatizáciu. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že Úrad podpredsedu vlády pre investície a informatizáciu bol zaradený ako iný ústredný orgán štátnej správy v doplnenom písmene e). |
| **ARDAL** | **ustanovenie § 27 ods. 4 návrhu zákona**  9. V nadväznosti na právomoci vecne príslušnej autority podľa § 11 návrhu zákona o kybernetickej bezpečnosti navrhujeme doplniť znenie ustanovenia § 27 ods. 4 návrhu zákona aj o vecne príslušnú autoritu nasledovne: „Povinnosť vykonať reaktívne opatrenie ukladá úrad rozhodnutím vecne príslušnej autorite a prevádzkovateľovi základnej služby ...“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že vecne príslušná autorita nemá k dispozícii informačný systém. Je to prakticky nevykonateľné. |
| **AZZZ SR** | **predloženému návrhu** bez pripomienok | O | A |  |
| **DEUS** | **Čl. I § 2 ods. 2 písm. a)** Navrhujeme doplniť na koniec vety slovo "skutočností" Odôvodnenie: Úprava gramatiky | O | A |  |
| **DEUS** | **Čl. I § 30 ods. 3** Navrhujeme presnejšie vymedziť požiadavku na preukázateľnú odbornú spôsobilosť a prax v audite informačnej bezpečnosti tak, aby bola táto požiadavka jednoznačná a rozličným výkladom navrhovaného ustanovenia nemohlo dôjsť k obchádzaniu predkladateľom navrhovaného účelu. | O | A | Text preformulovaný a upravený v zmysle pripomienok. |
| **DEUS** | **Čl. I § 17 ods. 1** Navrhujeme za slovo ktorým doplniť slovo "je" Odôvodnenie: Úprava gramatiky | O | A |  |
| **DEUS** | **Čl. I § 17 ods. 1** Z predloženého návrhu ako aj jeho dôvodovej správy nám nie je zrejmé, akým spôsobom sa má uplatniť výnimka pre prevádzkovateľa základnej služby po prekročení prahových hodnôt kritérií, ktorý je správcom informačného systému verejnej správy. Žiadame preto jednoznačne vymedziť, či sú takýto prevádzkovateľ automaticky zapisovaný do registra prevádzkovateľov základných služieb, alebo tam nie je zaradený nikdy. | Z | A | Vaša pripomienka bola akceptovaná a spresnená v dôvodovej správe. V zásade ide o každého správcu informačného systému verejnej správy. Títo budú zaradení do registra prevádzkovateľa základnej služby automaticky, teda sa nemusia identifikovať. Úrad sám zaradí subjekt do registra prevádzkovateľa základnej služby a poskytne im o tom informáciu (údaje z meta IS). |
| **DÔVERA** | Národný bezpečnostný úrad (ďalej len „úrad“) predložil dňa 26.5.2017 do pripomienkového konania návrh zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „návrh zákona“). Lehota na predloženie pripomienok k návrhu zákona bola stanovená do 15.6.2017. Obchodná spoločnosť DÔVERA zdravotná poisťovňa, a. s., so sídlom Einsteinova 25, 851 01 Bratislava, IČO: 35 942 436, zapísaná v Obchodnom registri Okresného súdu Bratislava I, oddiel Sa, vložka č. 3627/B (ďalej len „zdravotná poisťovňa“) týmto predkladá svoju zásadnú pripomienku k návrhu zákona. Za článok X návrhu zákona navrhujeme vložiť nový článok XI, ktorý znie: „Zákon č. 581/2004 Z. z. o zdravotných poisťovniach, dohľade nad zdravotnou starostlivosťou a o zmene a doplnení niektorých zákonov v znení zákona č. 719/2004 Z. z., zákona č. 353/2005 Z. z., zákona č. 538/2005 Z. z., zákona č. 660/2005 Z. z., zákona č. 25/2006 Z. z., zákona č. 282/2006 Z. z., zákona č. 522/2006 Z. z., zákona č. 12/2007 Z. z., zákona č. 215/2007 Z. z., zákona č. 309/2007 Z. z., zákona č. 330/2007 Z. z., zákona č. 358/2007 Z. z., zákona č. 530/2007 Z. z., zákona č. 594/2007 Z. z., zákona č. 232/2008 Z. z., zákona č. 297/2008 Z. z., zákona č. 461/2008 Z. z., zákona č. 581/2008 Z. z., zákona č. 192/2009 Z. z., zákona č. 533/2009 Z. z., zákona č. 121/2010 Z. z., zákona č. 34/2011 Z. z., nálezu Ústavného súdu Slovenskej republiky č. 79/2011 Z. z., zákona č. 97/2011 Z. z., zákona č. 133/2011 Z. z., zákona č. 250/2011 Z. z., zákona č. 362/2011 Z. z., zákona č. 547/2011 Z. z., zákona č. 185/2012 Z. z., zákona č. 313/2012 Z. z., zákona č. 421/2012 Z. z., zákona č. 41/2013 Z. z., zákona č. 153/2013 Z. z., zákona č. 220/2013 Z. z., zákona č. 338/2013 Z. z., zákona č. 352/2013 Z. z., zákona č. 185/2014 Z. z., zákona č. 77/2015 Z. z., zákona č.140/2015 Z. z., zákona č. 265/2015 Z. z., zákona č. 429/2015 Z. z., zákona č. 91/2016 Z. z., zákona č.125/2016 Z. z., zákona č. 286/2016 Z. z., zákona č. 315/2016 Z. z., zákona č. 317/2016 Z. z., zákona č. 356/2016 Z. z. a zákona č. 41/2017 Z. z. sa mení a dopĺňa takto: V § 76 odsek 3 sa dopĺňa nové písm. k), ktoré znie: „k) Národného bezpečnostného úradu na účely plnenia povinností pri zabezpečovaní kybernetickej bezpečnosti podľa osobitného predpisu x).“ Poznámka pod čiarou k odkazu x znie: „x) zákon č …/2017 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“ Doterajší článok XI návrhu zákona navrhujeme prečíslovať na článok XII. Odôvodnenie: Zdravotná poisťovňa je s poukázaním na ustanovenie § 3 písm. h) návrhu zákona zaradená medzi prevádzkovateľov základnej služby. Zdravotná poisťovňa, t.j. všetci jej zamestnanci, sú v zmysle ustanovenia § 76 zákona č. 581/2004 Z.z. o zdravotných poisťovniach, dohľade nad zdravotnou starostlivosťou a o zmene a doplnení niektorých zákonov v znení neskorších predpisov povinní zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvedeli pri výkone alebo v súvislosti s výkonom svojej funkcie alebo zamestnania, a to aj po skončení výkonu funkcie alebo zamestnania. Ak má mať zdravotná poisťovňa reálne možnosť plniť si povinnosti podľa návrhu zákona, je potrebné upraviť rozsah výnimiek z povinnosti mlčanlivosti, aby bola zdravotná poisťovňa oprávnená poskytovať úradu súčinnosť a plniť si oznamovacie povinnosti v zmysle návrhu zákona. pravne@dovera.sk | Z | N | Povinnosť mlčanlivosti vo veciach kybernetickej bezpečnosti je obsiahnutá v § 12 ods. 1, ktorá platí pre každého, kto vykonáva úlohy súvisiace s kybernetickou bezpečnosťou. (rovnako ako v zákone č. 581/2004 Z. z. ide o všeobecnú povinnosť zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvedel v súvislosti s úlohami vyplývajúcimi zo zákona, v ktorom je táto povinnosť deklarovaná). Teda povinnosť je upravená v zákone o KB tam kde patrí a nie je potrebné ju uvádzať v inom predpise. Tejto povinnosti môže osobu zbaviť len v konaní pred orgánom verejnej moci konkrétny štatutár. Rovnako na presne uvedené účely sa povinnosť zachovávať nevzťahuje pre PZS a jeho zamestnancov. Vyššie uvedené sa vzťahuje ale len na informácie, ktoré majú súvis s vykonávaním úloh podľa zákon o kybernetickej bezpečnosti a nejde o úlohy, ktoré sú vykonávané podľa zákona č. 581/2004 Z. z. Uvedenie výnimky z mlčanlivosti vo veciach kybernetickej bezpečnosti teda musí byť upravené v zákone, ktorého sa týka a nie je potrebné upravovať uvedené v iných právnych predpisoch. Text vyššie uvedený bude obsahom dôvodovej správy. |
| **GPSR** | **2. K čl. I, § 1** § 1 navrhujeme doplniť písmenom e) v tomto znení: „e) podmienky dobrovoľného a povinného hlásenia bezpečnostných incidentov.“. Táto významná oblasť procesov spojených s kybernetickou bezpečnosťou je súčasťou zákona (napr. § 18, ale aj na iných miestach), pritom však nie je vymedzená v určení predmetu zákona. Z hľadiska systematiky zákona alternatívne túto skutočnosť navrhujeme zaradiť pod ustanovenia § 2 návrhu zákona (pôsobnosť zákona). | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že oblasť, ktorú navrhujete, je už súčasťou systému zabezpečenia kybernetickej bezpečnosti. |
| **GPSR** | **4. K čl. I, § 3 písm. f)** Definícia kybernetického bezpečnostného incidentu v § 3 písm. f) návrhu zákona sa vo veľkej miere prekrýva so skutkovými podstatami trestných činov uvedenými v § 247 - § 247d Trestného zákona. Návrh zákona však v tomto ustanovení, ani na inom mieste nerieši interakciu s trestným konaním, neodkazuje na povinnosti v rámci trestného konania a neprihliada na viacerých miestach, napríklad na nevyhnutnosť zabezpečenia dôkazov (reakcia na bezpečnostný incident by mala byť vedená spôsobom, aby nedošlo k znehodnoteniu dôkazov pre následné trestné konanie). Ide o komplexnosť posúdenia navrhovanej zákonnej úpravy. Táto pripomienka je zásadná. | Z | N | Po vysvetlení rozpor odstránený. |
| **GPSR** | **24. K čl. I, § 23** Kybernetické bezpečnostné incidenty a ich kategórie navrhujeme definovať v tomto zákone. Ide potrebu z hľadiska dosiahnutia čo najvyššej miery komplexnosti právnej úpravy. V tejto súvislosti upozorňujeme, že predmetom posudzovania návrhu zákona by mali byť aj návrhy vykonávacích predpisov. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná, ustanovenie bolo preformulované a boli určené základné parametre na definovanie závažného kybernetického bezpečnostného incidentu v súlade so smernicou NIS. |
| **GPSR** | **18. K čl. I, § 11 ods. 2** Navrhujeme definovať náležitosti zmluvy podľa poslednej vety tak, aby obsahovala povinnosť, že využívanie jednotky CSIRT, ktorú prevádzkuje iná vecne príslušná autorita, sa zabezpečovalo len po predchádzajúcom súhlase prevádzkovateľa základnej služby. Táto pripomienka je zásadná. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že prevádzkovateľ základnej služby nezabezpečuje jednotku CSIRT, ale je v pôsobnosti a úlohou výlučne verejne príslušného subjektu. V kontexte návrhu zákona s prihliadnutím na § 11 ide o zákonné zabezpečenie ISVS prostredníctvom CSIRT v pôsobnosti orgánu určenom výlučne zákonom. Záver: Po vysvetlení rozpor odstránený. |
| **GPSR** | **10. K čl. I, § 6 ods. 1 písm. s)** Navrhujeme pred slovo „bezpečnostných“ vložiť slovo „vnútroštátnych“ alebo písmeno s) vypustiť a problematiku hlásení o vnútroštátnych bezpečnostných incidentoch spojiť so zahraničnými v písmene u). | O | A |  |
| **GPSR** | **11. K čl. I, § 6 ods. 2** Navrhujeme ustanoviť obligatórnu písomnú formu dohody a vypustiť poslednú vetu. Nepredpokladáme, že by obsah takýchto dohôd nebolo možné zverejniť. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a zapracovaná. |
| **GPSR** | **22. K čl. I, § 17 ods. 3** Nesúhlasíme s tým, aby bola služba zaradená do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb až na základe oznámenia potom, čo prevádzkovateľ služby zistí prekročenie prahových hodnôt kritérií. Odôvodnenie: Sme toho názoru, že zoznam základných služieb by mal byť definovaný a prístupný už v čase vydávania tohto zákona. Táto pripomienka je zásadná. | Z | N | Ide o transpozíciu smernice NIS, ktorá definuje tento prístup. Pre lepšiu identifikáciu bola upravená príloha č. 1. Princíp existuje v zákone o KI, teda identifikovanie subjektov na základe určených kritérií. Do nadobudnutia účinnosti tohto zákona sa predpokladá aj prijatie vykonávacích predpisov, ktorých tézy budú súčasťou schvaľovacieho procesu. Záver: Po vysvetlení rozpor odstránený. |
| **GPSR** | **6. K čl. I, § 5 písm. c) prvý bod** Odporúčame vypustiť prvý bod ako duplicitný k § 5 písm. b). | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že nie je pripomienkou v zmysle Legislatívnych pravidiel vlády. Úrad vystupuje ako vecne príslušný subjekt aj ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť a na základe toho má teda dve oddelené úlohy. |
| **GPSR** | **20. K čl. I, § 14 ods. 1 písm. b)** Odporúčame zvážiť, či je nevyhnutné, aby podmienkou akreditácie každej jednotky CSIRT bola povinnosť mať vytvorené podmienky umožňujúce chránený prenos a spracovanie údajov spôsobom podľa zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že pracoviská a informačné systémy musia byť v zmysle smernice umiestnené na zabezpečených miestach a rovnako musí byť zabezpečená kontinuita infraštruktúry. |
| **GPSR** | **19. K čl. I, § 12 ods. 9** Odsek 9 navrhujeme upraviť tak, aby nevytváral prekážku možnosti použitia údajov aj na účely trestného konania. Táto pripomienka je zásadná. | Z | A | Vaša pripomienka bola akceptovaná. Povinnosť bola premietnutá do odseku 3. Prevádzkovateľ základnej služby a poskytovateľ digitálnej služby podľa upraveného odseku 3 ako prvé subjekty nahlasujúce kybernetický bezpečnostný incident majú povinnosť hlásiť informácie vyžadované podľa osobitných predpisov, teda aj kriminalitu, protispoločenskú činnosť. V rámci úloh prevádzkovateľa základnej služby bolo doplnené ustanovenie, podľa ktorého má prevádzkovateľ základnej služby povinnosť pri riešení kybernetického bezpečnostného incidentu zabezpečovať dôkazy na účely trestného konania. Úrad má na účely zabezpečenia kybernetickej bezpečnosti povinnosť vybudovať dôveryhodnú infraštruktúru, ktorá bude pre všetky subjekty zárukou integrity, pravdivosti, bezpečnosti a nepopierateľnosti, z tohto dôvodu úrad sám seba limituje pri manipulácii s informáciami. Doplnené aj medzi povinnosti prevádzkovateľa základnej služby do § 19 ods. 4 písmeno d) a e). |
| **GPSR** | **31. K čl. IV bodu 6 [§ 7 ods. 2 písm. f) a g)]** Písmená f) a g) navrhujeme vypustiť, pretože v navrhovanom znení by mohli byť v rozpore s § 2 ods. 1 a 2 zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z. o Vojenskom spravodajstve. Táto pripomienka je zásadná. | Z | N | Záver: Po vysvetlení rozpor odstránený. MOSR sa zaviazalo novelizovať právne predpisy (zákon o ozbrojených silách a zákon o obrane) vo svojej vecnej pôsobnosti tak, aby zohľadňovali potreby zabezpečenia obrany vo vzťahu ku kybernetickému priestoru a súhlasilo s vypustením kompetencií MOSR (teda problematiky obrany, nie ochrany, ako je predmet úpravy v zákone o kybernetickej bezpečnosti návrhu zákona o kybernetickej bezpečnosti), keďže takáto úprava pri dodržaní legislatívno-technických zásad v záujme zabezpečenia riadneho výkonu verejnej moci má byť upravená v predpise vo vecnej pôsobnosti povinného štátneho orgánu. |
| **GPSR** | **29. K čl. IV bodu 6 [§ 7 ods. 2 písm. d)]** Písmeno d) navrhujeme vypustiť z dôvodu duplicity s platným znením § 7 písm. f). | O | N | Text bol preformulovaný. |
| **GPSR** | **30. K čl. IV bodu 6 [§ 7 ods. 2 písm. e), § 7 ods. 4 písm. b)]** Písmeno e) navrhujeme vypustiť, pretože v navrhovanom znení by mohlo byť v rozpore s platným znením § 7 písm. i). Táto pripomienka je zásadná. | Z | N | Záver: Po vysvetlení rozpor odstránený. MOSR sa zaviazalo novelizovať právne predpisy (zákon o ozbrojených silách a zákon o obrane) vo svojej vecnej pôsobnosti tak, aby zohľadňovali potreby zabezpečenia obrany vo vzťahu ku kybernetickému priestoru a súhlasilo s vypustením kompetencií MOSR (teda problematiky obrany, nie ochrany, ako je predmet úpravy v zákone o kybernetickej bezpečnosti návrhu zákona o kybernetickej bezpečnosti), keďže takáto úprava pri dodržaní legislatívno-technických zásad v záujme zabezpečenia riadneho výkonu verejnej moci má byť upravená v predpise vo vecnej pôsobnosti povinného štátneho orgánu. |
| **GPSR** | **3. K čl. I, § 2 ods. 1** Slová „môžu sa použiť“ navrhujeme nahradiť slovami „použijú sa“. V ustanovení § 2 ods. 1 sa uvádza: „Ak osobitný predpis ustanovuje rovnocenné alebo vyššie požiadavky na zabezpečenie sietí a informačných systémov ako tento zákon, môžu sa použiť ustanovenia osobitného predpisu.“. Z hľadiska jednoznačného vymedzenia práv a povinností považujeme za vhodné, aby zákon odkazoval na požiadavky osobitnej právnej úpravy s tým, že sa použije prísnejšia úprava. V poznámke pod čiarou k odkazu 1 navrhujeme v súvislosti s našou všeobecnou pripomienkou doplniť aj Trestný poriadok. Je zrejmé, že bezpečnostné incidenty môžu zároveň napĺňať skutkovú podstatu niektorého z trestných činov. Preto je dôležité zabezpečiť, aby oprávnenia orgánov činných v trestnom konaní nebolo možné v tomto kontexte spochybniť. Táto pripomienka je zásadná. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že veta bola vypustená bez náhrady. Záver: Po vysvetlení rozpor odstránený. |
| **GPSR** | **13. K čl. I, § 9 ods. 3** Slová „na tento účel sú povinné poskytnúť mu informácie v požadovanom rozsahu“ odporúčame nahradiť slovami „poskytujú mu informácie v rozsahu nevyhnutnom na tento účel“. | O | A | Text preformulovaný a upravený v zmysle pripomienok. |
| **GPSR** | **12. K čl. I, § 8** Slová „Organizácie severoatlantickej zmluvy“ odporúčame nahradiť slovami „Organizácie Severoatlantickej zmluvy“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený a zaradený medzi úlohy úradu z dôvodu duplicitnej úlohy v zákone na účely konkrétnej definície stanovených opatrení v oblasti medzinárodných vzťahov a spolupráce. |
| **GPSR** | **5. K čl. I, § 4** Toto ustanovenie navrhujeme dopracovať. Zásady uvedené v § 4 sú vágne, v niektorých prípadoch opakujú princípy už zakotvené napríklad v Ústave Slovenskej republiky (napríklad § 4 ods. 2). Väčšina zásad nekorešponduje s nadpisom „Zásady kybernetickej bezpečnosti“, t. j. /podľa definície v § 3 písm. b)/ zásady „stavu, v ktorom sú siete a informačné systémy schopné odolávať kybernetickým bezpečnostným incidentom“. Obsah § 4 v predloženej forme tvoria skôr všeobecné pravidlá spolupráce, uplatňovania oprávnení orgánov verejnej moci, prevencie a vzdelávania. Ustanovenie § 4 ods. 6 nemá opodstatnenie, keďže podrobnejšie je rozpracované v § 26. V prípade, ak nedôjde k vypusteniu, prípadne zásadnému prepracovaniu celého § 4, navrhujeme v § 4 ods. 2 v poslednej vete vypustiť slovo „vtedy“ a vypustiť odsek 6. Táto pripomienka je zásadná. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. Záver: Po vysvetlení rozpor odstránený. |
| **GPSR** | **28. K čl. IV bodu 6 [§ 7 ods. 2 písm. a) až c)]** Upozorňujeme na možnú duplicitu s § 12 ods. 1 písm. a), c) a d) zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy. | O | N | Text preformulovaný v spolupráci s MOSR. |
| **GPSR** | **32. K čl. IV bodu 6 [§ 7 ods. 4 písm. b) druhý bod]** Upozorňujeme na možnú duplicitu s § 24 až 27 návrhu zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. | O | N | Text bol preformulovaný. |
| **GPSR** | **16. K čl. I, § 10 ods. 5** V § 10 ods. 5 písm. h) navrhujeme vypustiť spojenie „partneri Národnej jednotky CSIRT“, prípadne špecifikovať v texte zákona takýchto partnerov. Podobne je potrebné vymedziť kritériá subjektov, ktoré sem možno zaradiť na základe rozhodnutia úradu /písmeno j)/. Vzhľadom na to, že ide o neverejnú časť systému, okruh subjektov, ktoré majú priamy prístup, by mal byť jednoznačne vymedzený. Text písmen h) a j) predstavuje neohraničený a neidentifikovateľný počet subjektov s priamym prístupom do neverejnej časti systému, ktorý nie je obmedzený účelom, postavením týchto subjektov a nie je ani časovo ohraničený. V zmysle našej základnej všeobecnej pripomienky a v kontexte širokej blanketnej úpravy vyznieva paradoxne skutočnosť, že zoznam subjektov neobsahuje policajné orgány (alebo ich špecializované zložky), ani orgány činné v trestnom konaní, pre ktoré môžu byť údaje v systéme (ak sa napríklad už nenachádzajú v dispozícii subjektu, ktorý ich poskytol) dôležité pre trestné konanie, prípadne môžu byť dôležitým nástrojom pre realizáciu prevencie v súlade so zákonom Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov. Obdobným spôsobom je potrebné vnímať aj problematiku bezpečnosti súdneho informačného systému. Táto pripomienka je zásadná. | Z | A | Vaša pripomienka bola akceptovaná a zapracovaná. |
| **GPSR** | **7. K čl. I, § 5, § 6 ods. 1 písm. f) a g) a § 11** V § 5, § 6 ods. 1 písm. f) a písm. g) a § 11 a v celom texte návrhu zákona navrhujeme pojem „autorita“ nahradiť pojmom „orgán“ alebo „subjekt“. Podľa § 5 písm. c), prípadne charakteristík v § 11 je zrejmé, že v rámci právneho poriadku Slovenskej republiky sa na označenie daného subjektu používa pojem „orgán“. V zmysle vyššie uvedenej všeobecnej pripomienky poukazujeme v kontexte tohto ustanovenia na skutočnosť, že návrh zákona nerieši začlenenie Generálnej prokuratúry Slovenskej republiky a jej systémov do systému kybernetickej bezpečnosti, pričom z nášho pohľadu do rozsahu úpravy zákona spadá aspoň register trestov (okrem iného sa z neho poskytujú údaje na účely ochrany a bezpečnosti štátu, taktiež poskytuje informácie vo vzťahu k iným členským štátom Európskej únie v rámci Európskeho informačného systému registrov trestov; výpis z registra trestov možno získať aj na integrovaných obslužných miestach alebo na veľvyslanectvách v cudzine). V prípade začlenenia registra trestov do rozsahu pôsobnosti zákona navrhujeme doplniť do § 5 písm. c) aj Generálnu prokuratúru Slovenskej republiky. Z hľadiska filozofie zákona navrhujeme zvážiť aj zaradenie Ministerstva spravodlivosti Slovenskej republiky. Táto pripomienka je zásadná. | Z | A | Vaša pripomienka bola akceptovaná. Pojem vecne príslušná autorita bol v celom texte nahradený pojmom ústredný orgán. Ministerstvo vnútra SR vznieslo pripomienku, aby sa pojem vecne príslušná autorita prispôsobil pojmu ako ho pozná zákon o kritickej infraštruktúre, keďže tieto predpisy musia fungovať popri sebe a ich cieľom je zabezpečenie kritickej infraštruktúry (budova a systém), čo by vecne zjednodušilo orientáciu subjektov v rámci oboch predpisov. |
| **GPSR** | **14. K čl. I, § 10** V odseku 1 druhej vete navrhujeme slovo „slúži“ nahradiť slovami „je určený“. V odseku 2 tretiu vetu navrhujeme upraviť takto: „Verejná časť jednotného informačného systému kybernetickej bezpečnosti obsahuje.“. Odseky 1, 3 a 4 navrhujeme presunúť do § 3, keďže ide o vymedzenie základných pojmov. V odseku 5 navrhujeme slovo „podobe“ nahradiť slovom „forme“. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná. Ide o úradom zvolenú legislatívnu techniku. |
| **GPSR** | **8. K čl. I, § 6 ods. 1 písm. b)** V písmene b) navrhujeme slová „záväznú politiku“ nahradiť slovami „záväzné zásady“. Navrhovateľ ani v dôvodovej správe neuvádza, čo sa myslí záväznými zásadami správania v kybernetickom priestore. Je potrebné pripomenúť, že normatívne zásahy do práv a povinností subjektov vyžadujú zákonnú úpravu. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že politikou sa myslia zásady. Úrad vydáva aj politiky podpisovaní v oblasti elektronického podpisu. Nie je to novum ale zaužívané slovné spojenie. |
| **GPSR** | **21. K čl. I, § 16 a 27** V prípade reaktívnej služby by jednotka CSIRT mala mať povinnosť kontaktovať orgány činné v trestnom konaní, ak by v dôsledku realizácie tohto postupu mohlo dôjsť k zničeniu dôkazov (za predpokladu, že by incident napĺňal znaky niektorej zo skutkových podstát trestných činov). Takúto povinnosť by mal mať aj úrad pri postupe podľa § 27. Táto pripomienka je zásadná. | Z | A | Vaša pripomienka bola akceptovaná. Prevádzkovateľ základnej služby a poskytovateľ digitálnej služby hlásia kybernetické bezpečnostné incidenty a majú všetky povinnosti, ktoré im platná právna úprava ukladá. Jednotka CSIRT je klientské centrum bez právnej subjektivity, zriaďuje ju príslušný orgán verejnej moci a má presne vymedzené úlohy. Povinnosti, ktoré žiadate vo Vašej pripomienke sú teda predmetom povinností prevádzkovateľa základnej služby a poskytovateľa digitálnej služby a nie jednotky CSIRT. Prevádzkovateľ základnej služby a poskytovateľ digitálnej služby má ustanovené výnimky na Vami požadované účely z povinnosti mlčanlivosti, teda čo sa týka účelu Vašej pripomienky, ten je obsiahnutý v § 12 a následne aj medzi povinnosťami prevádzkovateľa základnej služby. Text upravený v zmysle vyhodnotenia vyššie uvedenej pripomienky. |
| **GPSR** | **26. K čl. I, § 33** Z dôvodu vykonateľnosti a efektívnosti navrhovaného systému navrhujeme, aby zo splnomocňovacieho ustanovenia boli vypustené písmená b) a d) a aby tieto boli upravené zákonom. V tejto súvislosti upozorňujeme, že predmetom posudzovania návrhu zákona by mali byť aj návrhy vykonávacích predpisov. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a zapracovaná, pretože do zákona boli premietnuté základné parametre, na základe ktorých budú presnejšie špecifiká uvedené vo vyhláške. V rámci zabezpečovania kybernetickej bezpečnosti sa pri jednotlivých opatreniach vychádza z ISO 27002, na ktorú zákon odkazuje a ktorá bude obsiahnutá svojim spôsobom vo vykonávacom predpise. |
| **GPSR** | **25. K čl. I, § 28 ods. 4** Z hľadiska vykonateľnosti a efektívnosti systému by vyhlásenie stavu kybernetického ohrozenia ústnym vyhlásením malo byť precíznejšie špecifikované. Ústne prehlásenie (napríklad v kancelárii úradu) by bolo nepochybne neúčinné. Nie je zrejmé, či účelom ustanovenia bolo upraviť odklad zverejnenia kybernetického ohrozenia, alebo bol touto úpravou sledovaný iný cieľ. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **GPSR** | **27. K čl. IV a V** Z hľadiska vymedzenia úloh Ministerstva obrany Slovenskej republiky v oblasti kybernetickej obrany je otázne, o aké postupy v čase mieru ide. Napríklad podľa navrhovaného znenia § 7 ods. 2 písm. f) zákona č. 319/2002 Z. z. o obrane Slovenskej republiky získava, sústreďuje a analyzuje informácie dôležité pre zabezpečenie kybernetickej obrany, ako aj ďalších novelizovaných ustanovení. V každom prípade je potrebné text precizovať tak, aby vylučoval automatické nasadenie technických prostriedkov monitorujúcich prevádzku na internete a pod. Je potrebné skúmať, či nasadenie takýchto prostriedkov by malo podliehať súhlasu súdu. Táto pripomienka je zásadná. | Z | N | Záver: Po vysvetlení rozpor odstránený. MOSR sa zaviazalo novelizovať právne predpisy (zákon o ozbrojených silách a zákon o obrane) vo svojej vecnej pôsobnosti tak, aby zohľadňovali potreby zabezpečenia obrany vo vzťahu ku kybernetickému priestoru a súhlasilo s vypustením kompetencií MOSR (teda problematiky obrany, nie ochrany, ako je predmet úpravy v zákone o kybernetickej bezpečnosti návrhu zákona o kybernetickej bezpečnosti), keďže takáto úprava pri dodržaní legislatívno-technických zásad v záujme zabezpečenia riadneho výkonu verejnej moci má byť upravená v predpise vo vecnej pôsobnosti povinného štátneho orgánu. |
| **GPSR** | **15. K čl. I, § 10 ods. 1 druhá veta** Z návrhu zákona nie je jednoznačne zrejmé, aké údaje a informácie má Jednotný informačný systém kybernetickej bezpečnosti spracovávať a vyhodnocovať. Navrhované znenie je vágne, a preto navrhujeme konkrétnejšie vymedziť tieto údaje a informácie. | O | A |  |
| **GPSR** | **9. K čl. I, § 6 ods. 1 písm. q) a r)** Z návrhu zákona nie je zrejmý rozdiel medzi „vyhlasovaním varovania pred bezpečnostným incidentom“ a „včasným varovaním“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že varovanie prebieha v komunikačnom kanáli medzi ústrednými orgánmi definovanými v zákone. Vyhlásenie varovania úradom pred kybernetickým bezpečnostným incidentom predstavuje konanie úradu smerom k verejnosti. |
| **GPSR** | **1. Všeobecne** Zákon nijakým spôsobom nereaguje na skutočnosť, že aj orgány činné v trestnom konaní (a súdy) používajú informačné systémy. Navrhujeme túto skutočnosť posúdiť komplexne, nakoľko podľa nášho názoru „súbor minimálnych požiadaviek na zabezpečenie kybernetickej bezpečnosti“ (§ 2 návrhu zákona) sa musí dotýkať aj informačných systémov, ktorých prevádzkovateľmi sú Ministerstvo vnútra Slovenskej republiky, Generálna prokuratúra Slovenskej republiky a Ministerstvo spravodlivosti Slovenskej republiky. V kladnom prípade je túto skutočnosť potrebné aj jednoznačne v zákone vyjadriť (rozsah pôsobnosti, prípadné obmedzenia jeho pôsobnosti na predmetné systémy). Táto pripomienka je zásadná. | Z | A | Vysvetlené na rozporovom konaní, text primerane upravený a dovysvetlenie bude uvedené v dôvodovej správe. |
| **GPSR** | **17. K čl. I, § 10 ods. 7** Znenie odseku 7 je potrebné vyjadriť precíznejšie. V navrhovanom texte je ustanovená podmienka sprístupnenia údajov tretím osobám so súhlasom úradu. Nie je však zrejmé, či sa tento súhlas vyžaduje ako dodatočná podmienka v prípade, ak je síce samostatný údaj súčasťou systému, ale súčasne sa má poskytnúť napríklad na základe príkazu súdu alebo prokurátora podľa osobitného zákona. Z uvedeného dôvodu je potrebné text precizovať napríklad doplnením vety: „Súhlas úradu nie je potrebný, ak sú údaje poskytované podľa osobitného predpisu.“. Táto pripomienka je zásadná. | Z | N | Vaša pripomienka nebola akceptovaná a text bol vypustený bez náhrady. Záver: Po vysvetlení rozpor odstránený. |
| **GPSR** | **23. K čl. I, § 17 ods. 4** Žiadame doplniť povinnosť úradu informovať prevádzkovateľa, že služba bola zaradená do zoznamu základných služieb a prevádzkovateľ do registra prevádzkovateľov základných služieb na základe podnetu vecne príslušnej autority alebo z iniciatívy úradu. Táto pripomienka je zásadná. | Z | A | Vaša pripomienka bola akceptovaná a textácia bola preformulovaná. |
| **MDaVSR** | **CI. II** II odporúčam v úvodnej vete slovo „mení“ nahradiť slovom „dopĺňa“. | O | A |  |
| **MDaVSR** | **Čl. I v § 11 ods. 2 písm. g)**  odporúčam slovo „klasifikácie“ nahradiť slovom „klasifikáciu“. | O | A |  |
| **MDaVSR** | **Čl. I § 4 ods. 6** odporúčam slovo „neboli“ nahradiť slovami „nie sú“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **MDaVSR** | **Čl. I v poznámke pod čiarou k odkazu 31**  odporúčam za slovo „zákona“ doplniť slová „Národnej rady Slovenskej republiky“. | O | A |  |
| **MDaVSR** | **návrhu zákona**  Návrh zákona predpokladá vydanie vykonávacieho právneho predpisu podľa § 33 návrhu zákona, avšak tento vykonávací predpis nie je súčasťou sprievodných dokumentov zverejnených s návrhom zákona. Vykonávacím predpisom pritom majú byť upravené aj kľúčové skutočnosti, napríklad z hľadiska určenia, ktoré subjekty vymenované v jednotlivých sektoroch uvedených v prílohe č. 1 budú patriť do kategórie prevádzkovateľov základných služieb (prahové hodnoty pre identifikáciu základnej služby). Odporúčam, aby bol vykonávací predpis zverejnený a nadobudol účinnosť spolu s návrhom zákona, keďže tak prevádzkovateľom služieb, ako aj vecne príslušným autoritám, plynie podľa § 35 návrhu zákona odo dňa účinnosti zákona lehota, v ktorej majú úradu oznámiť informácie podľa § 17 ods. 1 návrhu zákona na základe kritérií uvedených vo vykonávacom predpise. Bez poznania prahových hodnôt a kritérií z vykonávacieho predpisu je problematické sa vyjadriť k otázke povinností, kladených na prevádzkovateľov služby v jednotlivých sektoroch. | O | A | Tézy vyhlášok budú súčasťou schvaľovacieho procesu, identifikácia PZS bližšie určená kritériami doplnenými do zákona, náčrt prahových hodnôt doplnený do dôvodovej správy, účinnosť sa navrhuje k máju 2018, po schválení zákona bude dostatočný čas na vydanie vyhlášok. |
| **MDaVSR** | **Čl. IX** odporúčam v bode 1. vypustiť jedenkrát slová „o zmene“. | O | A | Vysvetlené na rozporovom konaní. |
| **MDaVSR** | **Čl. I** odporúčam v poznámke pod čiarou k odkazu 3 za slová „§ 2 ods.1 písm. g) a ods. 3 zákona“ doplniť slová „Národnej rady Slovenskej republiky“ a za slová „§ 2 ods. 1 písm. c) zákona“ doplniť slová „Národnej rady Slovenskej republiky“. | O | A |  |
| **MDaVSR** | **Prílohe č. 1**  žiadam upraviť podľa smernice EP a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica“). Odôvodnenie: Prílohou č. 1 návrhu zákona je tabuľka bez názvu, hoci podľa čl. 4 ods. 4. smernice by mala tvoriť zoznam „typov subjektov“ – prevádzkovateľov základných služieb. V tabuľke má byť podľa prílohy II smernice uvedené len odvetvie „Digitálna infraštruktúra“, pododvetvie a typ subjektu „internetové prepojovacie uzly, poskytovanie služieb DNS a registre domén“; nad rámec je v prílohe uvedený sektor elektronických komunikácií. Navrhované znenie je v rozpore s cieľmi smernice a vytvára duplicitu. Informácie o bezpečnostných incidentoch poskytujú podniky Úradu pre reguláciu, ktorý ich každoročne predkladá Európskej komisii a agentúre ENISA. | Z | A | Vysvetlené na rozporovom konaní. Príloha č. 1 prepracovaná v zmysle doručených pripomienok a dohôd. |
| **MDaVSR** | **Čl. I § 2 ods. 1**  žiadam vypustiť z poznámky pod čiarou k odkazu 1 slová „§ 64 až 68 zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov,“. Odôvodnenie: Žiadam, aby osobitným predpisom vo vzťahu k zákonu č. 351/2011 Z. z. o elektronických komunikáciách (ďalej len „zákon o elektronických komunikáciách“), pokiaľ ide o bezpečnosť a integritu verejných sietí a služieb, bol zákon o kybernetickej bezpečnosti. Bezpečnosť a integrita verejných sietí a služieb, upravená v § 64 zákona o elektronických komunikáciách, je širší pojem ako kybernetická bezpečnosť; kybernetická bezpečnosť je len jednou z oblastí bezpečnosti a integrity verejných sietí a služieb. Takejto úprave zodpovedá aj Čl. IX bod 2. návrhu zákona o kybernetickej bezpečnosti. V tejto súvislosti je z pohľadu zákona o elektronických komunikáciách nevyhnutné, aby zostala zachovaná správna a úplná implementácia čl. 13a ods. 3 Smernice Európskeho parlamentu a Rady 2002/21/ES o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica) v platnom znení. | Z | A | Záver: Vypustené ustanovenia týkajúce sa zákona č. 351/2011 ZZ z čl. I. Po dohode s ÚpREKaPŠ upravené znenie novelizačného bodu k zákonu č. 351/2011 ZZ a upravená príloha č. 1, vypustený telekomunikačný sektor (akceptovanie aj pripomienky RÚZ). Problematika potreby hlásenia incidentov a spolupráce s NBÚ, ako aj prístupu k telekomunikačnému tajomstvu vysvetlená v rámci rozporových konaní a mejlovou komunikáciou a vzhľadom na túto potrebu došlo ku konsenzu a úprave textu návrhu zákona. MDaVSR precizovalo text a ÚpREKaPŠ navrhlo znenie novely zákona č. 351/2011 ZZ v zmysle uzavretej dohody na rozporovom konaní. |
| **MDaVSR** | **Čl. IX bod 3** žiadam vypustiť znenie alebo dôvodovú správu osobitnej časti doplniť o zdôvodnenie navrhovanej zmeny. Odôvodnenie: Znenie § 64 ods. 3 zákona o elektronických komunikáciách je transpozíciou článku 13a ods. 3 citovanej rámcovej smernice, podľa ktorého „členské štáty zabezpečia, aby podniky, ktoré poskytujú verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby, informovali príslušný národný regulačný orgán o narušení bezpečnosti alebo strate integrity, ktoré malo významný vplyv na prevádzku sietí alebo služieb“. Podniky majú povinnosť informovať Úrad pre reguláciu elektronických komunikácií a poštových služieb (ďalej len „Úrad pre reguláciu“). Navrhuje sa, aby podniky informovali Úrad pre reguláciu „prostredníctvom jednotného informačného systému kybernetickej bezpečnosti“, ktorý sa zavádza v § 10 návrhu zákona o kybernetickej bezpečnosti. Z návrhu zákona nie je zrejmé, akým spôsobom budú podniky informovať priamo Úrad pre reguláciu prostredníctvom uvedeného jednotného informačného systému kybernetickej bezpečnosti, keďže Úrad pre reguláciu tento systém neprevádzkuje. Žiadam preto navrhované ustanovenie vysvetliť, konkrétne ako má informačný mechanizmus od podnikov k Úradu pre reguláciu prebiehať, resp. ako sa Úrad pre reguláciu o incidente cez systém dozvie. Súčasne zdôrazňujem potrebu zabezpečiť, aby bol Úrad pre reguláciu informovaný o incidentoch súvisiacich s kybernetickou bezpečnosťou, ktoré by narušili bezpečnosť a integritu sietí alebo služieb, aby bola zachovaná správna a úplná transpozícia článku 13a citovanej rámcovej smernice. | Z | A | Vysvetlené na rozporovom konaní, odsek bol vypustený. |
| **MDaVSR** | **Čl. IX v bode 1.**  žiadam vypustiť znenie alebo dôvodovú správu osobitnej časti doplniť o zdôvodnenie navrhovanej zmeny. Odôvodnenie: Žiadam jednoznačne zdôvodniť potrebu zaradenia konkrétnych orgánov verejnej moci, ktoré vykonávajú pôsobnosť v oblasti kybernetickej bezpečnosti podľa § 5 návrhu zákona medzi „iné orgány štátu“. Podľa § 55 ods. 6 zákona o elektronických komunikáciách sa za orgány štátu považujú najmä bezpečnostné zbory, ktorých úlohou je odhaľovanie a stíhanie trestnej činnosti a ochrana ústavného zriadenia a bezpečnosti štátu, čo umožňuje týmto orgánom po splnení zákonných podmienok uplatniť zákonom uznanú výnimku z ochrany špecifického typu tajomstva, v tomto prípade telekomunikačného (vrátane odpočúvania a záznamu telekomunikačnej prevádzky podľa príslušných ustanovení Trestného poriadku). Navrhovanú zmenu je preto nevyhnutné upraviť a odôvodniť. | Z | A | Vysvetlené na rozporovom konaní. |
| **MDaVSR** | **Čl. I v § 3 písm. a)**  žiadam za slovom „sieťou“ vypustiť slová „a informačným systémom“. Odôvodnenie: Elektronická komunikačná sieť nie je podľa zákona o elektronických komunikáciách informačným systémom. Pojem „informačný systém“ sa nachádza za týmto pojmom, pričom sa odkazuje na zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. | Z | A |  |
| **MDaVSR** | **Čl. VIII v prílohe č. 3**  žiadam zadefinovať sektor „Kybernetický priestor“ spolu s podsektormi „Siete a informačné systémy a Informačnokomunikačné technológie“. Odôvodnenie: Pojem „Kybernetický priestor“ bol vytvorený bez zadefinovania sektorových kritérií, rozšírenia alebo zúženia jestvujúcich sektorov a prvkov kritickej infraštruktúry. Pokiaľ nebude „kybernetický priestor“ exaktne zadefinovaný, vytvára sa duplicita s oblasťou elektronických komunikácií. | Z | N | Po vysvetlení bol rozpor odstránený, príloha č. 3 bola upravená. |
| **MFSR** | **K čl. I k § 19** § 19 žiadam doplniť odsekom 7, ktorý znie: „(7) Úrad je povinný každý rok a po každej zmene majúcej významný vplyv na bezpečnostné opatrenia preveriť účinnosť prijatých bezpečnostných opatrení prostredníctvom komplexného interného a externého penetračného testu vykonaného prostredníctvom zahraničnej, alebo domácej jednotky CSIRT mimo organizačnej pôsobnosti úradu.“. Ide o zabezpečenie systematického dohľadu nad kybernetickou bezpečnosťou v celej organizačnej štruktúre kybernetickej bezpečnosti v SR. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že bezpečnostné opatrenia vyplývajú priamo z bezpečnostnej normy 27002. Úrad na účely auditu vydá schému, v ktorej budú opatrenia uvedené konkrétne. Takéto opatrenie priamo reflektuje na zmeny v bezpečnostnom okolí. Záver: Po vysvetlení rozpor odstránený. |
| **MFSR** | **K čl. I k § 3** 1. Do navrhovaného ustanovenia odporúčam doplniť definície používaných pojmov, ako sú „aktívum“, „aktivovaný prvok kybernetického priestoru“, „last resort CSIRT“ (resp. jeho slovenského ekvivalentu a tiež identifikovať skratky CSIRT, CERT a ich ekvivalenty (identické útvary). 2. Žiadam preformulovať znenie písmena j) a prispôsobiť kritériá slovenským podmienkam, pretože navrhované kritériá nemusia reflektovať hodnotu aktív prevádzkovateľa. Žiadam určiť kritériá napríklad „vplyv na trh“, „poskytovanie podpory pre kritické služby“, „škoda pre Slovenskú republiku pri nedostupnosti služby“, „strategickosť obsluhovaného sektora podľa zákona o kritickej infraštruktúre“. | O | N | Vaša pripomienka nebola akceptovaná, z dôvodu že bol upravený celý § 3 a boli zavedené nové pojmy. |
| **MFSR** | **K čl. I k § 19** 1. Odsek 1 odporúčam preformulovať z dôvodu nejednoznačnosti. 2. Znenie odseku 3 písm. h) odporúčam preformulovať, pretože technické opatrenie nie je oblasť. 3. V odseku 6 odporúčam na konci doplniť tieto slová: „prostredníctvom bezpečnostného auditu a v prípade verejnej správy prostredníctvom penetračného testu a ohodnotenia zraniteľností“. | O | A | Vaša pripomienka bola akceptovaná a upravená v zmysle ISO/IEC 27002. |
| **MFSR** | **K čl. I k § 29** 1. Odsek 6 žiadam vypustiť, pretože priznáva úradu neprimerané kompetencie, znižuje bezpečnosť kontrolovaných informačných systémov vzhľadom na kompromitáciu administratívnych účtov. Zmenou konfigurácie môže dôjsť k zníženiu bezpečnosti alebo ohrozeniu funkčnosti informačných systémov. Rovnako nie je zrejmé, kto preberá zodpovednosť za vzniknuté škody. 2. V odseku 7 žiadam za slová „sú povinné spolupracovať“ vložiť slová „v primeranej miere“. 3. Odseky 9 až 12 žiadam vypustiť, pretože priznávajú úradu neprimerané kompetencie (napríklad zastrašovať kontrolované subjekty alebo pokutovať pracovníkov z objektívnych dôvodov neprítomných na pracovisku). Tieto, v demokracii neakceptovateľné, ustanovenia je možné využívať na vyvíjanie nátlaku voči zamestnanom a narušovať interné riadiace procesy v organizácii. Alternatívne žiadam znenie upraviť tak, že sa pokuta ukladá kontrolovanému subjektu a nie jeho zamestnancom. | Z | A |  |
| **MFSR** | **K čl. I k § 13** 1. Rozhodnutie o akreditácii podľa odseku 5 by malo byť vydané na dobu neurčitú, najmä pre orgány verejnej moci z dôvodu zníženia administratívnej záťaže na opätovnú akreditáciu. Nie je dôvod v prípade fungujúcich jednotiek ich opätovne akreditovať. Nefunkčnosť jednotiek, resp. neplnenie požiadaviek na ich fungovanie je už riešená v § 15 ods. 4. 2. V odseku 8 prvej vete žiadam slová „môže na základe žiadosti uznať“ nahradiť slovami „uzná“. Súčasne žiadam vypustiť druhú vetu. 3. Znenie odseku 10 žiadam vypustiť, pretože platenie správnych poplatkov upravuje osobitný zákon. | Z | N | Záver: Po vysvetlení rozpor odstránený. |
| **MFSR** | **K čl. I k § 30** 1. V § 30 odporúčam a) definovať pojmy „interný audit“ a „externý audit“ a uložiť povinnosť vecne príslušnej autority vykonávať interný audit informačnej bezpečnosti aspoň raz ročne a výkon externého auditu nezávislým a úradom povereným audítorom vykonávať aspoň raz za dva roky, b) definovať tiež pojem „audit kybernetickej bezpečnosti“ a doplniť ho o požiadavky na audítora a rozsah auditu, c) v odseku 1 slová „sa vykonajú spôsobom podľa osobitného predpisu“ nahradiť slovami „sa vykonajú postupom podľa osobitného predpisu32)“ a s tým súvisiacu poznámku pod čiarou k odkazu 32, ktorá odkazuje všeobecne na zákon č. 357/2015 o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov odporúčam precizovať takto: „32) § 22 až 27 zákona č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov.“; ide o spresnenie ustanovenia z dôvodu odkazu na procesné ustanovenia zákona č. 357/2015 o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov. Upozorňujem, že zákon č. 357/2015 Z. z. je aplikovateľný len na orgány verejnej správy a na finančnú kontrolu a kontroly týkajúce sa informačných systémov verejnej správy. 2. V § 30 ods. 3 odporúčam precizovanie pojmu „nezávislá, odborne spôsobilá osoba s preukázateľnou praxou v audite informačnej bezpečnosti“ (napríklad taká osoba, ktorá svoju nezávislosť, prax a odbornosť preukazuje príslušným presne špecifikovaným certifikátom). | O | N | Vaša pripomienka nebola akceptovaná, pretože text bol preformulovaný v zmysle pripomienok. |
| **MFSR** | **K čl. I k § 10** 1. V odseku 1 žiadam nahradiť slová „efektívne riadenie, evidenciu“ slovami „efektívne riadenie, koordináciu, evidenciu“, pretože je potrebné na národnej úrovni zabezpečiť najmä koordináciu. 2. V odseku 5 žiadam vypustiť písmeno h), pretože partneri nie sú definovaní alebo presne definovať partnerov. 3. § 10 žiadam doplniť odsekom 8 znenia: „(8) Úrad poskytne subjektom povinne zapojených do jednotného systému správy kybernetického priestoru bezodplatne všetky súčasti systému potrebné na ich zapojenie do tohto systému.“. | Z | A |  |
| **MFSR** | **K čl. I k § 28** 1. V odseku 4 odporúčam, z dôvodu zrozumiteľnosti, upraviť prvú vetu napríklad takto: „Stav podľa odseku 3 je vyhlásený zverejnením, pričom v čase naliehavej situácie podľa odseku 8 je postačujúce vyhlásiť stav kybernetického ohrozenia len ústnou formou.“. 2. V odseku 5 odporúčam slová „poskytovateľ digitálnej služby“ nahradiť slovami „poskytovateľovi digitálnej služby“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **MFSR** | **K čl. I k § 27** 1. V odseku 5 žiadam na konci bodku nahradiť čiarkou a pripojiť tieto slová: „ak je to technicky možné, prijaté opatrenie nezníži bezpečnosť systému, nie je neprimerane technicky náročné alebo implementáciou opatrenia nedôjde k ohrozeniu kontinuity činností organizácií“. 2. V odseku 6 a v celom texte návrhu vo všetkých tvaroch žiadam slovo „úrad“ nahradiť slovami „vecne príslušná autorita“. | Z | N | Text preformulovaný v zmysle doručených pripomienok, uvedený paragraf rieši situácie v prípade, ak príslušný subjekt nevie zabezpečiť riešenie kybernetických bezpečnostných incidentov. Záver: Po vysvetlení rozpor odstránený. |
| **MFSR** | **K čl. I k § 12** 1. V odseku 5 žiadam za slová „podľa tohto zákona“ vložiť slová „a úkony súvisiace s riešením bezpečnostného incidentu alebo vydania varovania“, pretože priama komunikácia nemôže byť zakázaná pri riešení incidentu. 2. Žiadam vypustiť odsek 7, pretože nie je vhodné, potrebné ani účelné, aby pri spracúvaní osobných údajov bol úrad vyňatý z pôsobnosti zákona o ochrane osobných údajov. | Z | A | Záver: Po vysvetlení rozpor odstránený, upravené ustanovenia o mlčanlivosti aj vzhľadom na pripomienky ostatných dotknutých subjektov. Spracovanie osobných údajov v zmysle nariadenia GDPR. Do § 12 ods. 5 vložené navrhované slová. |
| **MFSR** | **K čl. I k § 35** 1. V prechodných a záverečných ustanoveniach odporúčam dočasne poveriť CSIRT.SK plnením úloh vládneho aj národného CSIRTu odo dňa nadobudnutia účinnosti tohto zákona. 2. Z predmetného návrhu zákona vyplývajú povinnosti pre prevádzkovateľov základných služieb, ktoré musia byť splnené pod hrozbami sankcií. Plnenie mnohých povinností však bude závisieť až od príslušných usmernení. Z tohto dôvodu navrhujem v odseku 5 prehodnotiť slová „do 18 mesiacov odo dňa účinnosti tohto zákona“. | O | ČA | Text bol preformulovaný v zmysle pripomienky. |
| **MFSR** | **K čl. VIII (novela zákona č. 45.2011 Z. z.) k bodu 4 (príloha č. 3)** 1. V stĺpci „Sektor“ bod 4 Kybernetický priestor podsektor odporúčam uviesť v znení: „4. Bezpečnosť kybernetického priestoru“. 2. Medzi predmetné sektory je potrebné zapracovať aj podsektor „Informačný systém Štátnej pokladnice“. | O | N | Bod 4 bol vypustený z prílohy č. 3 |
| **MFSR** | **K čl. I k § 32** 1. Znenie odseku 2 odporúčam preformulovať s dôvodu neprimerane vysokých pokút v porovnaní s vágne definovanými povinnosťami. 2. V odsekoch 2 a 4 žiadam nahradiť slová „predchádzajúci účtovný rok“ slovami „predchádzajúce účtovné obdobie“, za účelom zosúladenia s terminológiou zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov. 3. V odseku 9 žiadam poslednú vetu uviesť takto: „Ak nie je posledná účtovná závierka za predchádzajúce účtovné obdobie k dispozícii alebo ak nie je vykázaný žiadny obrat, úrad uloží pokutu podľa odsekov 2 a 4 až do 100 000 eur.“; ide o spresnenie textu, ak nie je k dispozícii posledná účtovná závierka. | O | A |  |
| **MFSR** | **K prílohe č. 1** 1. Znenie prílohy žiadam zosúladiť so zákonom o kritickej infraštruktúre s cieľom jednoznačného zadefinovania sektorov a podsektorov a ich gestorov (vecne príslušná autorita). 2. Mám za to, že Bankovníctvo a Finančné trhy patria do zákona o kritickej infraštruktúre. 3. Upozorňujem, že chemický priemysel je podsektor sektoru Priemysel. 4. Sektor Verejná správa nemôže obsahovať obranu, bezpečnosť a utajované skutočnosti, ktoré sú vylúčené z informačných systémov verejnej správy. Vláda schvaľuje sektory kritickej infraštruktúry, navrhovaný zákon túto kompetenciu vláde odoberá. | O | A |  |
| **MFSR** | **K čl. I k § 11** Je potrebné rozlíšiť vecne príslušné autority pre jednotlivé rezorty a ich príslušné informačné systémy a infraštruktúry a vecne príslušné autority pre jednotlivé sektory a podsektory. Znenie žiadam doplniť v zmysle, že každý ústredný orgán štátnej správy je vecne príslušnou autoritou pre svoj rezort a jeho podriadené organizácie. | Z | A | Upravená pôsobnosť ústredných orgánov a iných orgánov štátnej správy v nadväznosti na pripomienku č. 1 a jej úpravu v texte zákona. |
| **MFSR** | **Všeobecne** Návrh odporúčam zosúladiť so zákonom č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, so zákonom č. 211/2000 Z. z. o slobodnom prístupe k informáciám v znení neskorších predpisov, so zákonom č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a so zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy v znení neskorších predpisov. | O | A |  |
| **MFSR** | **K čl. I k § 18 a 21** Navrhované znenia odporúčam preformulovať, pretože povinnosti prevádzkovateľov základnej služby a poskytovateľov digitálnej služby sú nejednoznačne definované, pričom ich nedodržanie je sankcionované a takéto formulácie môžu znížiť právnu istotu prevádzkovateľov základnej služby a poskytovateľov digitálnej služby. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a znenie bolo preformulované. |
| **MFSR** | **K čl. I k § 29** Niektorí prevádzkovatelia základných služieb sú zároveň aj prvkami kritickej infraštruktúry. Akékoľvek narušenie alebo prípadný výpadok ich služieb môže mať pre Slovenskú republiku kritický dopad. Navrhujem uplatnenie výnimiek pre prvky kritickej infraštruktúry v celom § 29, ktoré by zohľadňovali nebezpečenstvo narušenia, stratu integrity a dôvernosti ich informačných systémov a informácií, ktoré spracúvajú. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu nahradenia novým znením textu, ktorý bol preformulovaný aj vzhľadom na pripomienky ostatných subjektov. |
| **MFSR** | **K prílohe č. 2 (Digitálne služby)** Odporúčam doplniť zoznam o nasledovné digitálne služby: „4. služba elektronickej pošty, 5. internetové úložiská, 6. služby webového sídla, - 7. hostingové služby.“. | O | N | Zoznam digitálnych služieb výchádza zo smernice a je jednotný pre celú EÚ. |
| **MFSR** | **K čl. I k § 24** Odsek 5 odporúčam preformulovať z dôvodu nejednoznačnosti a nesúladu s § 10 ods. 6 v kontradikcii s dohodou podľa § 24 ods. 5. | O | A |  |
| **MFSR** | **K čl. I k § 21** Odsek 5 žiadam vypustiť z dôvodu nejednoznačnosti (terminologická nepresnosť pojmu „osobitný záujem“). | Z | N | Záver: Po vysvetlení rozpor odstránený. |
| **MFSR** | **K čl. I k § 5** Písmeno c) žiadam doplniť desiatym bodom tohto znenia: „10. „ústredný orgán štátnej správy neuvedený v prvom bode až deviatom bode v rozsahu svojej pôsobnosti.“. Každý ústredný orgán má mať znalosti o bezpečnosti vo svojom rezorte, súčasne je zodpovedný za výkon svojich kompetencií vrátane prevádzky informačných systémov verejnej správy, a preto musí byť zodpovedný za definovanie požadovanej úrovne bezpečnosti a jej zabezpečenie. | Z | A | Upravené v § 4 písmeno c) v zmysle zachovania významu pripomienky, vysvetlené na rozporovom konaní. |
| **MFSR** | **K čl. I k § 13** Podľa dôvodovej správy je národná jednotka CSIRT organizačnou zložkou NBÚ. Z návrhu však nie je zrejmé, či aj ostatné jednotky CSIRT budú organizačnou súčasťou vecne príslušných autorít alebo budú vystupovať ako samostatné právnické osoby. Odporúčam preto postavenie jednotiek CSIRT upraviť. | O | A | Vaša pripomienka bola akceptovaná a odôvodnená v dôvodovej správe. Vecne príslušný subjekt zabezpečuje jednotku CSIRT a teda tento subjekt rozhoduje akú podobu pracovisko bude mať. |
| **MFSR** | **K čl. I k § 27** Upozorňujem, že reaktívne opatrenie podľa odseku 3 nie je možné vykonať pred vznikom kybernetického bezpečnostného incidentu. Odporúčam zadefinovať, čo sa má diať počas riešenia, po riešení kybernetického bezpečnostného incidentu a následne, z hľadiska systematiky členenia návrhu, presunúť do § 3. | O | A |  |
| **MFSR** | **K čl. I k § 30** V § 30 ods. 2 žiadam na konci pripojiť túto vetu: „Správa môže byť upravená do tvaru, ktorý neobsahuje citlivé informácie, ktoré by mohli ohroziť bezpečnosť organizácie, alebo informačného systému.“. | Z | N | Záver: Po vysvetlení rozpor odstránený. Auditná správa neobsahuje citlivé informácie. |
| **MFSR** | **K čl. I k § 17** V odseku 1 odporúčam za slovo „ktorým“ vložiť slovo „je“. | O | A |  |
| **MFSR** | **K čl. I k § 6** V odseku 1 žiadam preformulovať písmeno p), pretože informačný systém nie je možné viesť, ale spravovať alebo prevádzkovať. | Z | A |  |
| **MFSR** | **K čl. I k § 31** V odseku 1 žiadam vypustiť písmeno d) z dôvodu absentujúcej kontroly, vágnosti, neprimeraných kompetencií úradu použiteľných na vyvíjanie nátlaku mimo rozsahu zákona, ústavy SR. | Z | A |  |
| **MFSR** | **K čl. I k § 11** V odseku 2 vecne príslušná autorita môže na základe zmluvy využívať jednotku CSIRT, ktorú prevádzkuje iná vecne príslušná autorita. Táto zmluva má okrem iného obsahovať aj vyčíslenie prevádzkových nákladov, ktoré je povinná vecne príslušná autorita uhradiť vecne príslušnej autorite prevádzkujúcej jednotku CSIRT. Podľa návrhu sú vecne príslušnými autoritami rozpočtové organizácie. Upozorňujem, že rozpočtová organizácia zostavuje svoj rozpočet príjmov a výdavkov, pričom plnenie úloh v rámci svojej pôsobnosti má byť podľa princípov rozpočtového hospodárenia zabezpečené v rámci rozpočtu rozpočtovej organizácie; ak plnenie úloh rozpočtovej organizácie prechádza na inú rozpočtovú organizáciu postupuje sa podľa § 17 a 18 zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. | O | A |  |
| **MFSR** | **K čl. I k § 2** V odseku 2 písm. a) odporúčam vypustiť slová „o ochrane utajovaných,“ ako nadbytočné. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že je legislatívno-technicky nesprávna. |
| **MFSR** | **K čl. I k § 16** V odseku 3 písm. b) odporúčam za slovo „analýza“ vložiť slová „a riešenie“. | O | N | Vaša pripomienka nebola akceptovaná a bola upravená v zmysle pripomienky č. 300 od MO SR. |
| **MFSR** | **K čl. I k § 9** V odseku 3 žiadam slová „informácie v požadovanom rozsahu“ nahradiť slovami „informácie v primeranom rozsahu“. Navrhovaná forma znamená riziko svojvoľného určenia rozsahu informácie nad rámec nevyhnutnosti a z dôvodu vysokého stupňa centralizácie citlivých informácií, čo predstavuje zbytočné bezpečnostné riziko. | Z | A |  |
| **MFSR** | **K čl. I k § 18** V odseku 4 odporúčam na konci doplniť slová „po odstránení citlivých údajov“; je potrebné pri oznamovaní informácií zohľadniť ochranu osobných údajov, obchodného tajomstva, bankového tajomstva, poštového tajomstva, daňového tajomstva a utajovaných skutočností. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že po abstrahovaní údajov je informácia nekompletná a reálne nepoužiteľná. Incidenty sú povinné prevádzkovateľovi hlásiť "vcelku", nahlásené údaje chráni úrad. |
| **MFSR** | **K čl. I k § 28** V odseku 6 žiadam na konci pripojiť slová „a vecne príslušnú autoritu“. | Z | N | Záver: text preformulovaný po dohode s MOSR. Po vysvetlení rozpor odstránený. |
| **MFSR** | **K čl. I k § 33** V písmene b) odporúčam prahové hodnoty pre jednoznačnú identifikáciu poskytovateľa základnej služby upraviť tak, ako je to upravené u poskytovateľa digitálnej služby. | O | A |  |
| **MFSR** | **K prílohe č. 1** V sektore 7. Finančný sektor/Financie v stĺpci PZS žiadam nahradiť slová „Štátna pokladnica“ slovami „osoby zapojené do systému Štátnej pokladnice“. | Z | A |  |
| **MFSR** | **Všeobecne** Vnútorná štruktúra návrhu by mala rozlišovať vecne príslušnú sektorovú autoritu od rezortnej vecne príslušnej autority a popísať úlohy, povinnosti a zodpovednosť osobitne pre každý tento typ. Každý ÚOŠS by mal byť vecne príslušnou autoritou (VPA) pre organizácie vo svojej pôsobnosti v sektore „verejná správa“. | Z | A |  |
| **MFSR** | **Všeobecne** Z doložky vybraných vplyvov (ďalej len „doložka vplyvov“) vyplýva, že návrh bude mať pozitívny vplyv aj negatívny vplyv na rozpočet verejnej správy, pričom výdavky súvisiace s realizáciou návrhu budú v rozpočte zabezpečené iba čiastočne. Súčasne sa v časti 2.1.1 Financovanie návrhu uvádza, že finančné prostriedky vyplývajúce z návrhu budú zabezpečené v rámci schválených limitov rozpočtu v jednotlivých rozpočtových rokoch bez dodatočných požiadaviek na rozpočet. Uvedené žiadam zosúladiť a zároveň žiadam upraviť aj text v predkladacej správe, podľa ktorého návrh bude mať iba negatívny vplyv na rozpočet verejnej správy. V Analýze vplyvov na rozpočet verejnej správy, na zamestnanosť vo verejnej správe a financovanie návrhu (ďalej len „analýza vplyvov“) tabuľke č. 1 sú na roky 2018 až 2021 kvantifikované celkové výdavky verejnej správy v objemoch od 51 406 tis. eur do 57 406 tis. eur, ale výdavky v riadku „financovanie zabezpečené v rozpočte“ za tieto roky sú uvedené vo vyššej sume (od 54 000 tis. eur do 60 000 tis. eur) ako celkové výdavky. Uvedené žiadam zosúladiť. V analýze vplyvov tabuľke č. 1 sú kvantifikované výdavky za EÚ zdroje a spolufinancovanie zo štátneho rozpočtu z viacerých operačných programov (OP Integrovaná infraštruktúra, OP Výskum a inovácie a OP Ľudské zdroje), ale tieto výdavky nie sú členené podľa jednotlivých kapitol. Upozorňujem, že v schválenom rozpočte kapitoly NBÚ na rok 2017, ani v návrhu rozpočtu na roky 2018 až 2020 nie sú rozpočtované výdavky na EÚ a spolufinancovanie zo štátneho rozpočtu. V nadväznosti na uvedené žiadam do tabuľky č. 1 doplniť názvy jednotlivých kapitol, v ktorých sú prostriedky na uvedené operačné programy rozpočtované a uviesť aktuálne sumy na roky 2018 až 2020. Žiadam tiež uviesť kvantifikáciu výdavkov na roky 2017 až 2020 (uvedené sú roky 2018 až 2021) a vyplniť všetky relevantné tabuľky analýzy vplyvov, vrátane tabuliek č. 4 a 5, pretože v rámci predbežného pripomienkového konania boli vyplnené tabuľky č. 4, 4a, 5 a 5a, ktoré však neboli v súlade s údajmi v tabuľke č. 1 a súčasne bol v tabuľkách č. 5 a 5a nesprávne uvedený priemerný mzdový výdavok. V súčasnosti majú tabuľky č. 4 a 5 nulové hodnoty aj napriek návrhom zákonov, ktoré sa novelizujú v ďalších článkoch. Z doložky vplyvov ani z analýzy vplyvov nie je zrejmý vplyv na zamestnanosť, resp. riadky „Vplyv na počet zamestnancov“ a „Vplyv na mzdové výdavky“ obsahujú nulové hodnoty, pričom podľa podkladov jednotlivých kapitol štátneho rozpočtu k návrhu rozpočtu verejnej správy na roky 2018 až 2020 si tieto nárokujú krytie predmetných výdavkov a zvýšenie počtu zamestnancov. Podľa jednotnej metodiky na posudzovanie vybraných vplyvov je potrebné do doložky vplyvov doplniť všetky predpokladané výdavky spojené s realizáciou návrhu, vrátane nového medzirezortného programu na ochranu kybernetického priestoru. Výdavky je potrebné kvantifikovať podľa zdrojového krytia, programovej klasifikácie a jednotlivých subjektov verejnej správy. S predloženým materiálom možno súhlasiť len za podmienky, že všetky výdavky budú rozpočtovo zabezpečené v rámci schválených limitov počtu zamestnancov a limitov výdavkov dotknutých kapitol štátneho rozpočtu, bez dodatočných požiadaviek na zvýšenie limitu počtu zamestnancov a štátny rozpočet. Pre posúdenie finančných vplyvov žiadam o vypracovanie kvantifikácie vplyvov noviel zákonov v čl. III, VI a X (zákon č. 73/1998 Z. z., zákon č. 553/2003 Z. z. a zákon č. 55/2017 Z. z.), pričom upozorňujem, že s navrhovanými zmenami výšky príplatku, resp. osobného platu nesúhlasím. | Z | N | Rozpor trvá. V súvislosti s touto pripomienkou prebiehajú rokovania medzi NBÚ a MFSR. |
| **MFSR** | **K čl. I k § 1** Znenie § 1 odporúčam doplniť písmenom h), ktoré znie: „h) úroveň bezpečnosti informačných systémov v organizácii.“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že oblasť, ktorú navrhujete, je už súčasťou systému zabezpečenia kybernetickej bezpečnosti. |
| **MFSR** | **K čl. II (novela zákona č. 145.1995 Z. z.)** Znenie novelizačného článku žiadam upraviť takto: „1.V prílohe Prehľad sadzobníka správnych poplatkov sa na konci pripájajú tieto slová: „XXV. Kybernetická bezpečnosť ........................................................................ 276“. 2. Sadzobník správnych poplatkov sa dopĺňa časťou XXV, ktorá vrátane nadpisu znie: „XXV. ČASŤ Kybernetická bezpečnosť Položka 276 Akreditácia jednotky CSIRT ...................................................................... 1 500 eur“.“. | Z | A |  |
| **MFSR** | **K čl. I k § 23** Znenie odporúčam preformulovať z dôvodu nejednoznačnosti a z hľadiska systematiky členenia návrhu vložiť do § 3. | O | N | Vaša pripomienka nebola akceptovaná a znenie bolo vypustené. Právna úprava bola premietnutá v preformulovanej podobe s obsahom aj jednotlivých kriteriálnych parametrov v rámci § o hlásení kybernetických bezpečnostných incidentov. Parametre sú v súlade so smernicou NIS na určenie závažného kybernetického bezpečnostného incidentu. Jednotlivé kategórie sú odstupňované od závažnosti od 1 po 3, v záujme flexibilného reagovania na bezpečnostné prostredie je nevyhnutné špecifikáciu prenechať do vykonávacieho predpisu. |
| **MFSR** | **K čl. I k § 14** Znenie odseku 1 písm. b) až d) príliš striktnými podmienkami nastavenými na ochranu utajovaných informácií neprimerane obmedzuje vznik jednotiek CSIRT (nad rámec potrieb vyplývajúcich z návrhu) u subjektov a zároveň neupravuje kompetencie CSIRTov na úrovni sektora alebo podsektora. Navrhované znenie preto žiadam zjednodušiť, pretože sa nepredpokladá nakladanie s utajovanými skutočnosťami. | Z | ČA | Záver: Kompromisné riešenie úradu, kedy príslušné poznámky sú uvedené len príkladom, podmienka schopnosti IS prijímať utajované skutočnosti zostala zachovaná. Rozpor odstránený. |
| **MFSR** | **K čl. I k § 18** Znenie odseku 7 žiadam vypustiť z dôvodu nejednoznačnosti (napríklad nejasnosť pojmu „osobitné záujmy“). | Z | ČA | Záver: Po vysvetlení rozpor odstránený. |
| **MHSR** | **Prílohe č. 1** Navrhujeme nepoužívať v prílohe č. 1 skratku „PZS“ pre slová „prevádzkovateľa základných služieb“, nakoľko sa použila len v prílohe č. 1 návrhu materiálu a viackrát sa neopakuje, ale je vhodné ju rozpísať. Odôvodnenie: Legislatívno-technická pripomienka. | O | A | Upravená príloha v zmysle požiadavky upravenej MHSR (VPA pre IS hospodárskej mobilizácie je UPVII). |
| **MHSR** | **Prílohe č. 1** Navrhujeme nepoužívať v prílohe č. 1 skratku „VPA“ pre slová „vecne príslušné autority“, nakoľko sa použila len v prílohe č. 1 návrhu materiálu a viackrát sa neopakuje, ale je vhodné ju rozpísať. Odôvodnenie: Legislatívno-technická pripomienka. | O | A |  |
| **MHSR** | **§ 17** Odporúčame prehodnotiť znenie § 17 ods. 3 a 4 vo vzťahu k odseku 1. Odôvodnenie: Podľa nás nenadväzuje správne znenie odseku 3 a 4 na odsek 1, nakoľko tento hovorí o oznámení, keď došlo u prevádzkovateľa základnej služby k prekročeniu prahových hodnôt kritérií a odseky 3 a 4 o zaradení do zoznamu základných služieb a prevádzkovateľa základných služieb do registra prevádzkovateľov základných služieb. | O | A | Vaša pripomienka bola akceptovaná a textácia bola preformulovaná. |
| **MHSR** | **§ 11 ods. 1** V § 11 ods. 1 navrhujeme prvú a druhú úvodnú vetu nahradiť jednou vetou v znení: „Vecne príslušná autorita podľa § 5 písm. c) v rámci svojej pôsobnosti zodpovedá za zabezpečenie kybernetickej bezpečnosti a zabezpečuje“. Odôvodnenie: Štylistická pripomienka. | O | A |  |
| **MHSR** | **§ 25 ods. 2 a § 26 ods. 2** V § 25 ods. 2 a § 26 ods. 2 navrhujeme na konci vety doplniť slová „, ak je tento dostupný, inak sa hlásenie môže vykonať aj iným dostupným spôsobom“. Odôvodnenie: Môže sa stať, že informačný systém kybernetickej bezpečnosti bude z nejakého dôvodu práve v čase potreby nahlásenia incidentu nedostupný, a tak by mala byť v návrhu zákona uvedená aj alternatívna možnosť. | O | N | Vaša pripomienka nebola akceptovaná. Vysvetlenie je v dôvodovej správe. |
| **MHSR** | **§ 27 ods. 4** V § 27 ods. 4 navrhujeme slová „počas núdzového stavu“ nahradiť slovami „v rámci vyhláseného núdzového stavu“. Odôvodnenie: Núdzový stav sa vyhlasuje. Len v rámci trvania jeho vyhlásenia je možné obmedzovať práva. | O | N | Pripomienka nebola akceptovaná z dôvodu, že text bol preformulovaný. |
| **MHSR** | **§ 27 ods. 8** V § 27 ods. 5 navrhujeme zvážiť doplnenie vety, ktorá znie: „V prípade nedostupnosti jednotného informačného systému kybernetickej bezpečnosti alebo ak nemôže prevádzkovateľ základnej služby alebo poskytovateľ digitálnej služby oznámiť vykonanie reaktívneho opatrenia cez tento informačný systém, oznámi to úradu iným dostupným spôsobom.“. Odôvodnenie: Môže sa stať, že kybernetický bezpečnostný incident spôsobí nedostupnosť informačného systému kybernetickej bezpečnosti alebo nie je prevádzkovateľ základnej služby alebo poskytovateľ digitálnej služby schopný z dôvodu kybernetického bezpečnostného incidentu poslať oznámenie cez informačný systém kybernetickej bezpečnosti, a tak by mala byť v návrhu zákona uvedená aj alternatívna možnosť. | O | A | Upravené v § 34. |
| **MHSR** | **§ 28 ods. 1** V § 28 ods. 1 navrhujeme odsek formulovať nasledovne: „Kybernetické ohrozenie nastáva v prípade závažného zníženia úrovne kybernetickej bezpečnosti alebo bezprostrednej hrozby alebo rizika ohrozenia kybernetickej bezpečnosti, ak by v jeho dôsledku mohlo dôjsť k narušeniu bezpečnosti.26) Na jeho riešenie je možné vyhlásiť stav kybernetického ohrozenia.“. Odôvodnenie: Je dôležité najskôr definovať, čo je chápané pod slovami „kybernetické ohrozenie“ (v § 3 návrhu zákona to nie je definované) a až následne, keď príde k ohrozeniu, sa môže podľa zváženia situácie vyhlásiť stav kybernetického ohrozenia. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná. Ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **MHSR** | **§ 28 ods. 2 a 3** V § 28 ods. 2 a 3 žiadame odseky formulovať nasledovne: „(2) Úrad vyhlasuje stav kybernetického ohrozenia na nevyhnutný čas, najdlhšie na 10 za sebou nasledujúcich dní s možnosťou jeho opakovaného predĺženia najviac na dobu 30 za sebou nasledujúcich dní, ako aj jeho ukončenie. (3) Vyhlásenie stavu kybernetického ohrozenia a jeho ukončenie nadobúda účinnosť vyhlásením.“. Odôvodnenie: Je potrebné presne definovať, kto vyhlasuje a ukončuje stav kybernetického ohrozenia a kým spôsobom. Nechávame na zváženie, či neuviesť v návrhu zákona akou formou sa stav kybernetického ohrozenia vyhlasuje a ukončuje. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. MOSR sa zaviazalo novelizovať právne predpisy (zákon o ozbrojených silách a zákon o obrane) vo svojej vecnej pôsobnosti tak, aby zohľadňovali potreby zabezpečenia obrany vo vzťahu ku kybernetickému priestoru a súhlasilo s vypustením kompetencií MOSR (teda problematiky obrany, nie ochrany, ako je predmet úpravy v zákone o kybernetickej bezpečnosti návrhu zákona o kybernetickej bezpečnosti), keďže takáto úprava pri dodržaní legislatívno-technických zásad v záujme zabezpečenia riadneho výkonu verejnej moci má byť upravená v predpise vo vecnej pôsobnosti povinného štátneho orgánu. |
| **MHSR** | **§ 28 ods. 4** V § 28 ods. 4 odporúčame slová „v čase naliehavej situácie“ nahradiť slovami „v prípade naliehavej situácie“ alebo „v období naliehavej situácie“. Odôvodnenie: Situácia sa realizuje v nejakom období, ktoré nemá presné časové ohraničenie. | O | N | Vaša pripomienka bola čiastočne akceptovaná. Ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **MHSR** | **§ 28 ods. 7** V § 28 ods. 7 žiadame slová „o vyhlásení krízovej situácie“ nahradiť slovami „o vyhlásenie núdzového stavu, alebo o podanie návrhu na vyhlásenie výnimočného stavu alebo vojnového stavu“. Odôvodnenie: Krízová situácia sa podľa ústavného zákona č. 227/2002 Z. z. ani iného zákona nevyhlasuje, ale ide o obdobie v ktorom pôsobia negatívne faktory (javy/udalosti) v štáte a tieto majú na štát negatívny dopad a na riešenie krízovej situácie je možné v súlade s ústavným zákonom č. 227/2002 Z. z. vyhlásiť núdzový stav, výnimočný stav, vojnový stav alebo vypovedať vojnu. | Z | A | MOSR sa zaviazalo novelizovať právne predpisy (zákon o ozbrojených silách a zákon o obrane) vo svojej vecnej pôsobnosti tak, aby zohľadňovali potreby zabezpečenia obrany vo vzťahu ku kybernetickému priestoru a súhlasilo s vypustením kompetencií MOSR (teda problematiky obrany, nie ochrany, ako je predmet úpravy v zákone o kybernetickej bezpečnosti návrhu zákona o kybernetickej bezpečnosti), keďže takáto úprava pri dodržaní legislatívno-technických zásad v záujme zabezpečenia riadneho výkonu verejnej moci má byť upravená v predpise vo vecnej pôsobnosti povinného štátneho orgánu. Pojem v texte nahradený podľa pripomienky. |
| **MHSR** | **§ 29** V § 29 žiadame vypustiť odsek 6. Odôvodnenie: Z bezpečnostného hľadiska nie je prípustné, aby sa aj keď kontrolnému orgánu umožnil vstup do zabezpečených komunikačných a informačných systémov do úrovne správcu systému prevádzkovateľa informačného systému. Taktiež je vonkoncom neprípustné, aby sa kontrolnému orgánu čo i len dočasne dali oprávnenia na zmenu hardvérovej alebo softvérovej konfigurácie. Znamenalo by to ohrozenie funkčnosti a narušenie integrity systému. Kontrolný orgán ma kontrolovať, či má prevádzkovateľ informačného systému spracovanú potrebnú dokumentáciu, v ktorej je aj popísaná hardvérová a softvérová konfigurácia a spôsob zabezpečenia ochrany prevádzkovaného informačného systému. Na základe poskytnutých dokumentov by mal vedieť posúdiť, či je ochrana informačného systému dostatočná alebo nie. | Z | A | Text preformulovaný, nové znenie ustanovenia o kontrole bez sporného ustanovenia. |
| **MHSR** | **§ 30 ods. 1** V § 30 ods. 1 žiadame zmeniť limit na realizáciu auditu z 24 mesiacov na 48 mesiacov. Odôvodnenie: Nakoľko nie sú na oblasť zabezpečenia kybernetickej bezpečnosti zatiaľ naplánované žiadne finančné prostriedky a ani po nadobudnutí účinnosti zákona nebude podľa nás hneď možné tieto finančné náklady na zabezpečenie plnenia úloh vyplývajúcich z tohto návrhu zákona hneď vyčísliť a realizovať, a preto je termín do 24 mesiacov nepostačujúci. Po schválení štátneho rozpočtu na budúci rok je len veľmi ťažko možné dosiahnuť navýšenie finančných prostriedkov na novú oblasť riešenia v roku 2018, a preto je lepšie termín predĺžiť aspoň na 48 mesiacov. Okrem toho, pri audite sa chce, aby náklady na audit znášal prevádzkovateľ základnej služby a veľakrát bude musieť tento audit vykonať za neho súkromná spoločnosť, nakoľko určite aspoň v rámci štátnej správy sa nenachádzajú odborníci, ktorí by vedeli taký audit vykonať a to znamená, že si to bude vyžadovať aj hľadanie finančných prostriedkov na zaplatenie auditu, ktoré v súčasnosti nevie nikto presne vyčísliť. | Z | A | Vaša pripomienka bola čiastočne akceptovaná. Text bol nahradený novým znením, ktoré bolo preformulované aj vzhľadom na pripomienky ostatných subjektov. Po vysvetlení bol rozpor odstránený. |
| **MHSR** | **§ 35 ods. 5** V § 35 ods. 5 žiadame zmeniť limit na prijatie bezpečnostných opatrení z 18 mesiacov na 24 mesiacov. Odôvodnenie: Nakoľko nie sú na oblasť zabezpečenia kybernetickej bezpečnosti zatiaľ naplánované žiadne finančné prostriedky a ani po nadobudnutí účinnosti zákona nebude podľa nás hneď možné tieto finančné náklady na zabezpečenie plnenia úloh vyplývajúcich z tohto návrhu zákona hneď vyčísliť a realizovať, a preto je termín do 18 mesiacov nepostačujúci. Po schválení štátneho rozpočtu na budúci rok je len veľmi ťažko možné dosiahnuť navýšenie finančných prostriedkov na novú oblasť riešenia v roku 2018, a preto je lepšie termín predĺžiť aspoň na 24 mesiacov. | Z | A | Preformulované na 24 mesiacov. |
| **MHSR** | **§ 9 ods. 6** V § 9 ods. 6 navrhujeme na konci druhej vety doplniť slová „kybernetickej bezpečnosti“. Odôvodnenie: Keďže v rámci návrhu zákona nebola zavedená legislatívna skratka pre jednotný informačný systém kybernetickej bezpečnosti, tak by sa v rámci celého návrhu zákona mal používať celý názov informačného systému. | O | A |  |
| **MHSR** | **§ 5** V návrhu materiálu žiadame doplniť samostatné ustanovenie pre pôsobnosť vlády SR v rámci oblasti kybernetickej bezpečnosti vo väzbe na § 5 písm. a) návrhu zákona. Odôvodnenie: V návrhu materiálu chýba samostatné ustanovenie pre pôsobnosť vlády SR v rámci oblasti kybernetickej bezpečnosti vo väzbe na § 5 písm. a) návrhu zákona. V § 6 je riešená pôsobnosť NBÚ vo väzbe na § 5 písm. b) návrhu zákona a v § 11 pôsobnosť vecne príslušnej autority vo väzbe na § 5 písm. c) návrhu zákona. | Z | N | Ustanovenie bolo z textu zákona vypustené. |
| **MHSR** | **Prílohe č. 1** V prílohe č. 1 návrhu materiálu žiadame doplniť do tabuľky, v rámci sektora 8. Verejná správa, aj Ministerstvo hospodárstva SR, ako správcu a prevádzkovateľa jednotného informačného systému hospodárskej mobilizácie. Odôvodnenie: Ministerstvo hospodárstva SR je správcom špecifického aplikačného programu jednotného informačného systému hospodárskej mobilizácie v súlade s § 39 ods. 7 zákona č. 179/2011 Z. z. a prevádzkovateľom je podľa § 39 ods. 9 zákona č. 179/2011 Z. z. je ministerstvom hospodárstva SR určená právnická osoba, ktorá plní funkciu systémového integrátora špecifického aplikačného programu jednotného informačného systému hospodárskej mobilizácie. Tento informačný systém je určený pre všetkých používateľov zo subjektov hospodárskej mobilizácie, ktorí vykonávajú opatrenia hospodárskej mobilizácie v súlade s vydaným písomným rozhodnutím, zákonom o hospodárskej mobilizácie alebo uznesením vlády SR č. 637/2011. Keďže ide o informačný systém verejnej správy, v rámci ktorého sa spracúvajú údaje potrebné na zabezpečenie vykonávania opatrení hospodárskej mobilizácie za celú SR, tak je žiaduce, aby aj tento informačný systém bol zaradený do zoznamu základných služieb v rámci sektora Verejná správa, nakoľko sa v ňom spracúvajú údaje, ktoré je potrebné chrániť. | Z | ČA | Príloha č. 1 je nahradená novým znením v zmysle smernice NIS. po vysvetlení bol rozpor odstránený. |
| **MHSR** | **Doložke vybraných vplyvov** V rámci doložky vybraných vplyvov je vhodné aspoň čiastočne naplánovať finančné prostriedky pre vecne príslušné autority na zabezpečenie prvotných nákladov na rozbehnutie celého procesu riešenia kybernetickej bezpečnosti. Odôvodnenie: Bez naplánovaných finančných prostriedkov a ich schválenia v zákone o štátnom rozpočte na rok 2018 nie sú vecne príslušné autority, ale ani vláda SR a NBÚ, schopné zabezpečiť rozbeh celého procesu riešenia kybernetickej bezpečnosti. V návrhu zákona by sa mali aspoň nejaké finančné prostriedky vyčísliť, aby vláda SR pri schvaľovaní tohto návrhu zákona už počítala s potrebou navýšenia štátneho rozpočtu aspoň na rok 2018 u dotknutých vecne príslušných autorít. Keďže ide o nový zákon a problematiku, ktorá sa doteraz v rámci SR neriešila, tak nikto s finančnými nákladmi na túto oblasť nepočítal a len za podpory vlády SR a zabezpečenia krytia finančných prostriedkov zo strany štátu je možné celý systém kybernetickej bezpečnosti rozbehnúť na úrovni vecne príslušných autorít. Keďže sa plánuje vytvoriť aj medzirezortný rozpočtový program pre túto oblasť, tak už by v návrhu zákona mali byť aj navrhnuté finančné prostriedky na zabezpečenie realizácie prvotných úloh vecne príslušných autorít. | Z | A | Úrad predloží MFSR novú doložku s požiadavkami všetkých subjektov na rozpočet a trvá na jej uplatnení. |
| **MHSR** | **§ 17 ods. 1** V§ 17 ods. 1 navrhujeme slová „Ak prevádzkovateľ služby ...“ nahradiť slovami „Ak prevádzkovateľ základnej služby ...“ a slová „...služby, ktorým správca informačného systému ...“ nahradiť slovami „... služby, ktorým je správca informačného systému ...“. Odôvodnenie: Ustanovenie § 17 má popisovať základnú službu a máme za to, že sa to týka prevádzkovateľa základnej služby. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná z dôvodu že prevádzkovateľ služby sa stáva prevádzkovateľom základnej služby až kumulatívnym splnením podmienok uvedených v § 3 písm. l). |
| **MKSR** | **Čl. IX** 1. Navrhujeme doplniť novelizačný bod 1 v tomto znení: "1. V § 8 sa odsek 1 dopĺňa písmenom j), ktoré znie: "j) Národným bezpečnostným úradom v oblasti kybernetickej bezpečnosti.".". Odôvodnenie: Určenie oblasti spolupráce Úradu pre reguláciu elektronických komunikácií a poštových služieb a Národného bezpečnostného úradu. 2. Pôvodne novelizačný bod 1 odporúčame upraviť takto: "2. V poznámke pod čiarou k odkazu 42 sa na konci pripájajú slová:..." a ostatné body prečíslovať. 3. V bode 4 (pred zmenou 3) navrhujeme v odseku 3 slová "informovať úrad prostredníctvom" nahradiť slovami "informovať úrad a Národný bezpečnostný úrad prostredníctvom". Odôvodnenie: Zosúladenie povinností Podniku vo vzťahu k požiadavkám efektívneho výkonu opatrení súvisiacich so zaisťovaním kybernetickej bezpečnosti. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a zapracovaná. Slovo "úrad" je podľa zákona č. 351/2011 Z. z. leg skratka úradu pre reguláciu sieťových odvetví a nie NBÚ. |
| **MKSR** | **Čl. V**  1. Novelizačné body 3 a 4 odporúčame označiť ako body 1 a 2. 2.V bode 1 v poznámke pod čiarou k odkazu 8a odporúčame nahradiť slová "§ 1 ods. 2 Zákon" slovami "§ 2 ods. 2 písm. b) zákona". 3. V bode 2 v § 4e ods. 3 odporúčame nahradiť slovo "Opatrenie" slovom "Opatrenia" a slová "ods. 2" slovami "odseku 2", v odseku 4 slovo "Dopravy" uviesť malým začiatočným písmenom a za slová "minister obrany" vložiť čiarku a slová "minister vnútra Slovenskej republiky alebo minister dopravy a výstavby Slovenskej republiky". | O | A |  |
| **MKSR** | **Čl. I § 5** 1. Upozorňujeme, že NBÚ je uvedený v písmene b) aj písmene c) bod 1. Odporúčame úrad vypustiť z písmena c) z dôvodu duplicity a doterajšie body 2 až 9 označiť ako body 1 až 8. 2. V § 5 písm. c) odporúčame doplniť nový bod "9. Vojenské spravodajstvo". Odôvodnenie: Zosúladenie zoznamu vecne príslušných autorít s prílohou č. 1 (Sektor 8. Verejná správa, časť Spravodajské služby). | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že úrad vystupuje aj ako vecne príslušný subjekt aj ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť a na základe toho má teda dve oddelené úlohy. |
| **MKSR** | **Čl. I § 32** 1. Upozorňujeme, že porušenie povinnosti podľa § 21 ods. 1 a 3 je sankcionované podľa odseku 3 aj 4. V súlade so zásadou Ne bis in idem uplatňovanou v našom právnom poriadku, žiadame ponechať len jednu sankciu za jedno porušenie povinnosti. 2. V odseku 8 odporúčame upraviť znenie prvej vety (slová finančná pomoc poskytnutá). 3. V odseku 13 odporúčame vložiť za slová "Na konanie" slová "o uložení pokuty za správny delikt". | O | A |  |
| **MKSR** | **Čl. I § 4** 1. V odseku 1 odporúčame slová "je záležitosťou" nahradiť napríklad slovami "sa zabezpečuje" alebo "sa uskutočňuje" a ostatné slová uviesť do správneho gramatického tvaru. 2. Odsek 5 odporúčame upraviť. Ak základnou zásadou kybernetickej bezpečnosti má byť aj riadenie rizík, potom považujeme za vhodné doplniť v základných pojmoch aj pojem "riadenie rizík" a zásadu odporúčame formulovať jednoznačne a zrozumiteľne, napríklad "Riadenie rizík sa uskutočňuje (zabezpečuje)...". | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **MKSR** | **Čl. I § 33**  1. V úvodnej vete odporúčame nahradiť slovo "upraví" slovom "ustanoví" a v písmene e) vložiť za slová "na audit" slovo "a" a pred slovo "rozsahu" slovo "podrobnosti". 2. V písmene h) upozorňujeme na nesprávny vnútorný odkaz na § 6 ods. 1 písm. d). | O | A |  |
| **MKSR** | **Čl. VIII** 1. V úvodnej vete odporúčame vypustiť slová "a dopĺňa", v bode 1 nahradiť slovo "písmeno" slovom "písm." a body 2 a 3 zlúčiť do jedného bodu. 2. V novom bode 2 (predtým body 2 a 3) odporúčame odkazy 2a a 2b označiť ako odkazy 4a a 4b. 3. V úvodnej vete bodu 4 odporúčame vložiť za slová "Príloha č. 3" slová "vrátane nadpisu". 4. V Prílohe č. 3. pri sektore 2. Elektronické komunikácie v stĺpci "Ústredný orgán" navrhujeme slová "Ministerstvo dopravy a výstavby Slovenskej republiky" nahradiť slovami "Národný bezpečnostný úrad". Odôvodnenie: Efektívny výkon činností spojených so zaisťovaním kybernetickej bezpečnosti vyžaduje úzku koordináciu sektora "Elektronické komunikácie" a sektora "Kybernetický priestor". Považujeme preto za prínosné, aby bol Národný bezpečnostný úrad ústredným orgánom na úseku kritickej infraštruktúry v sektoroch "Elektronické komunikácie" a "Kybernetický priestor". | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a zapracovaná z dôvodu, že ustanovenie bolo preformulované v zmysle pripomienok iných subjektov najmä MVSR. |
| **MKSR** | **Príloha č. 1**  1. Za slová "Príloha č. 1" odporúčame vložiť slová "k zákonu č. .../2017 Z. z." a vo vysvetlivkách odporúčame uviesť vysvetlenie k použitým skratkám "PZS" a "VPA". 2. V časti tabuľky prislúchajúcej sektoru "9. Sektor elektronických komunikácii" v stĺpci "VPA" navrhujeme slová "Ministerstvo dopravy a výstavby SR, Úrad pre reguláciu elektronických komunikácií a poštových služieb" nahradiť slovami "Národný bezpečnostný úrad". Odôvodnenie: Efektívny výkon činností spojených so zaisťovaním kybernetickej bezpečnosti vyžaduje úzku koordináciu sektora "4. Digitálna infraštruktúra", sektora "8. Verejná správa" v časti ISVS a sektora "9. Sektor elektronických komunikácií". Považujeme preto za prínosné, aby bol Národný bezpečnostný úrad VPA s pôsobnosťou pre vyššie vymenované sektory. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná z dôvodu že text bol preformulovaný. |
| **MKSR** | **Čl. II až X** Na konci tých novelizačných bodov, kde je to potrebné, odporúčame doplniť bodku alebo úvodzovky a bodku. | O | A |  |
| **MKSR** | **Všeobecne**  Návrh zákona je v rozpore s článkom 17 ods. 1 písm. i) Legislatívnych pravidiel Vlády Slovenskej republiky – neobsahuje návrh vykonávacieho predpisu (všeobecne záväzného právneho predpisu) určeného splnomocňovacím ustanovením v §33. Máme za to, že vykonávací predpis má nadobudnúť účinnosť súčasne so zákonom (1. január 2018), najmä vzhľadom na povinnosti ukladané Prevádzkovateľovi a Vecne príslušnej autorite v § 35 (Prechodné a záverečné ustanovenia). Žiadame doplniť návrh vykonávacieho predpisu určeného splnomocňovacím ustanovením v § 33. | O | A |  |
| **MKSR** | **Poznámky pod čiarou- všeobecne** Odporúčame prekontrolovať poznámky pod čiarou a zosúladiť ich s Legislatívnymi pravidlami vlády SR, napríklad poznámka č. 1 a 4 (bod 23.8. a 23.7. prílohy č. 1 k Legislatívnym pravidlám vlády SR). Taktiež upozorňujeme na uvádzanie neúplných názvov zákonov, napríklad poznámka č. 3, potrebu uvádzania skrátených citácii tam, kde je to potrebné, napríklad poznámka č. 3- zákon č. 198/1994 Z. z. a na potrebu uvádzania správnych znení príslušných ustanovení zákonov, napríklad poznámka č. 3- § 2 ods. 1 písm. c) zákona č. 198/1994 Z. z. v znení zákona č. 444/2015 Z. z. | O | A |  |
| **MKSR** | **Čl. I § 8**  Slová "medzinárodným organizáciám" odporúčame nahradiť slovami "medzinárodnými organizáciami". | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený a zaradený medzi úlohy úradu z dôvodu duplicitnej úlohy v zákone na účely konkrétnej definície stanovených opatrení v oblasti medzinárodných vzťahov a spolupráce. |
| **MKSR** | **Čl. VI** V § 13c ods. 1 odporúčame nahradiť slovo "vykonávania" slovom "vykonávanie" a v odseku 2 slovo "odsekov" slovom "odseku". | O | N | Pripomienka nebola akceptovaná z dôvodu, že bola akceptovaná pripomienka ÚVSR a ustanovenie bolo vypustené bez náhrady. |
| **MKSR** | **Čl. X bod 2**  V § 141a ods. 1 odporúčame nahradiť slovo "vykonávania" slovom "vykonávanie" a za slová "kybernetickej bezpečnosti" vložiť čiarku. | O | A |  |
| **MKSR** | **Čl. I § 20**  V § 20 odporúčame jednoznačnejšie formulovať znenie odseku 1 vo väzbe na prílohu č. 2. Ak v prílohe č. 2 má byť zoznam digitálnych služieb, na ktoré sa vzťahuje tento zákon a podľa odseku 1 § 20 sa ich poskytovatelia majú prihlásiť do registra poskytovateľov digitálnych služieb, odporúčame prehodnotiť navrhované "zaradenie do zoznamu digitálnych služieb". Ak predkladateľ chce týmto zákonom postihovať aj iné digitálne služby ako tie, ktoré sú uvedené v prílohe č. 2, zo znenia odseku 1 to jednoznačne nevyplýva. | O | A | Vaša pripomienka bola akceptovaná a textácia bola upravená v zmysle pripomienky. |
| **MKSR** | **Čl. IV**  V bode 1 odporúčame nahradiť odkaz 1a odkazom 5a, novelizačné body 3 až 6 označiť ako body 2 až 5, v bode 3 (predtým 4) nahradiť slovo "plánovania" slovom "plánovanie", v bode 5 (predtým 6) v odseku 4 písm. c) nahradiť odkaz 9h odkazom 9f a upraviť označenie poznámok pod čiarou. Upozorňujeme, že v navrhnutom znení je poznámka pod čiarou k odkazu 9f uvedená, ale odkaz 9f nie je v normatívnom texte použitý. | O | A |  |
| **MKSR** | **Príloha č. 3**  V nadpise odporúčame vypustiť dvojbodku a za názvom smernice odporúčame uviesť publikačný zdroj. Odôvodnenie: Bod 62.9. prílohy č. 1 k Legislatívnym pravidlám vlády SR. | O | A |  |
| **MKSR** | **Čl. IV bod 6**  V navrhovanom odseku 4 písm. a) a b) navrhujeme slová "prijíma hlásenia" nahradiť slovami "analyzuje hlásenia prijaté prostredníctvom jednotného informačného systému kybernetickej bezpečnosti podľa osobitného predpisu.9g)". Odôvodnenie: Technicko-legislatívne spresnenie charakteru výkonu predpokladaných činností (s dôrazom na presnejšiu formuláciu predchádzajúcu možnému nesprávnemu výkladu v osobitnej povinnosti "hlásiť" (osobitne) Centru pre kybernetickú obranu Slovenskej republiky). | O | A |  |
| **MKSR** | **Čl. III bod 2**  V odseku 1 odporúčame nahradiť slovo "vykonávania" slovom "vykonávanie". | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol preformulovaný. |
| **MKSR** | **Čl. I § 2**  V odseku 1 odporúčame upraviť druhú vetu. Ak osobitný predpis ustanovuje vyššie požiadavky na zabezpečenie sietí a informačných systémov mal by sa použiť povinne (nie ako možnosť). | O | A |  |
| **MKSR** | **Čl. I § 22**  V odseku 1 odporúčame vložiť za slová "fyzická osoba" spojovník. | O | A |  |
| **MKSR** | **Čl. I § 17** V odseku 1 odporúčame vložiť za slová "všeobecne záväzným právnym predpisom" slová "ktorý vydá úrad podľa § 33 písm. b)" a za slovo "ktorým" slovo "je". V odseku 2 písm. a) odporúčame spresniť, koho názov a sídlo sa uvedie. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu nedodržania legislatívnej techniky. |
| **MKSR** | **Čl. I § 11**  V odseku 2 odporúčame nahradiť slová "ods. 1 písmeno b)" slovami "odseku 1 písm. b)". | O | A |  |
| **MKSR** | **Čl. I § 2**  V odseku 2 písm. a) odporúčame vypustiť slová "o ochrane utajovaných". | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že je legislatívno-technicky nesprávna. |
| **MKSR** | **Čl. I § 10** V odseku 2 písm. j) odporúčame nahradiť slovo "odsek" slovom "ods." a v odseku 4 slová "ods. 2 písmeno j)" slovami "odseku 2 písm. j)". | O | A |  |
| **MKSR** | **Čl. I § 15**  V odseku 5 odporúčame nahradiť slová "odsek 7" slovami "ods. 7". | O | A |  |
| **MKSR** | **Čl. I § 28**  V odseku 5 odporúčame nahradiť slovo "poskytovateľ" slovom "poskytovateľovi". | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **MKSR** | **Čl. I § 13**  V odseku 5 odporúčame nahradiť slovo "spravidla" slovom "najviac". Odôvodnenie: Navrhnuté znenie je neurčité. | O | A |  |
| **MKSR** | **Čl. I § 18**  V odseku 6 odporúčame presunúť odkaz 23 za slová "osobitného predpisu". | O | A |  |
| **MKSR** | **Čl. I § 1**  V písmene e) odporúčame použiť inú legislatívnu skratku ako "jednotka CSIRT". | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že legislatívna skratka "jednotka CSIRT" je zaužívaná skratka jasne definujúca predmet, uvedená v smernici, odvodená od začiatočných písmen názvu a tým nezameniteľná a zaužívaná v celej EÚ. |
| **MKSR** | **Čl. I § 3**  V písmene h) odporúčame vložiť za slovami "fyzické osoby" spojovník (to platí aj pre písmeno j)), pred slová "každý správca" odporúčame vložiť slovo "a" a slová "a sú" nahradiť slovami "a ktorí". | O | A |  |
| **MKSR** | **Čl. II**  V úvodnej vete čl. II odporúčame doplniť všetky novely a vypustiť slovo "mení". | O | A |  |
| **MKSR** | **Čl. VII** V úvodnej vete odporúčame nahradiť slovo "predpisov" slovom "zákonov", v bode 1 slovo "odsek" slovom "ods." a bod 3 upraviť takto: "3. V § 71 ods. 7 úvodná veta znie:...". | O | A |  |
| **MKSR** | **Príloha č. 2** Za slová "Príloha č. 2" odporúčame vložiť slová "k zákonu č. .../2017 Z. z.". Táto pripomienka platí aj pre prílohu č. 3. V prílohe č. 2 odporúčame doplniť názov prílohy: "Zoznam digitálnych služieb". | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a zapracovaná z dôvodu že text bol preformulovaný v zmysle pripomienok iných pripomienkujúcich subjektov. |
| **MKSR** | **Čl. I § 23** Za slová "všeobecne záväzným právnym predpisom" odporúčame vložiť slová "ktorý vydá úrad podľa § ... písm. ...". Táto pripomienka platí aj pre § 24 ods. 1, § 25 ods. 1, § 28 ods. 9 písm. c) | O | N | Vaša pripomienka nebola akceptovaná a znenie bolo vypustené. Právna úprava bola premietnutá v preformulovanej podobe s obsahom aj jednotlivých kriteriálnych parametrov v rámci § o hlásení kybernetických bezpečnostných incidentov. Parametre sú v súlade so smernicou NIS na určenie závažného kybernetického bezpečnostného incidentu. Jednotlivé kategórie sú odstupňované od závažnosti od 1 po 3, v záujme flexibilného reagovania na bezpečnostné prostredie je nevyhnutné špecifikáciu prenechať do vykonávacieho predpisu |
| **MKSR** | **Čl. I § 36** Za slovom "záväzné" odporúčame vypustiť slovo "právne". | O | A |  |
| **MOSR** | **K Čl. I, § 10 ods. 5 písm. h)** § 10 ods. 5 písm. h) žiadam vypustiť. Odôvodnenie: „Partneri Národnej jednotky CSIRT“ nie sú nikde v zákone definovaní. Zákon prakticky umožní sprístupniť časť systému akejkoľvek tretej strane, čo je neakceptovateľné. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **K Čl. I, § 10 ods. 5 písm. j)** § 10 ods. 5 písm. j) žiadam vypustiť. Odôvodnenie: Zákon prakticky umožní sprístupniť „neverejnú“ časť systému akejkoľvek tretej strane, čo je neakceptovateľné. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | N | Úrad na základe žiadosti preformuloval ustanovenie na „orgány verejnej moci“, aby nevznikol dojem, že prístup je možný komukoľvek. Po vysvetlení bol rozpor odstránený. |
| **MOSR** | **K Čl. I, § 10 ods. 6** § 10 ods. 6 žiadam dopracovať. Odôvodnenie: Návrh zákona uvádza v § 34 ods. 2 iba zverejnenie elektronického formulára. Návrh zákona nedefinuje rozhrania aplikácie, to aké informácie a údaje a v akom rozsahu a formáte sa majú poskytovať úradu, ani aké skutočnosti majú byť ich obsahom. Dostatočná špecifikácia je nevyhnutná vzhľadom na to, aby bolo možné plniť si zákonom stanovené povinnosti a vyhnúť sa prípadným sankciám. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | N | MOSR bolo úradom vysvetlené, že v tomto prípade pôjde o nastavenie formuláru, ktorý sa tohto času nedá definovať. Zadefinovanie v zákone v čase, keď IS ešte nie je vytvorený by mohlo spôsobiť následnú prekážku pri jeho kreovaní a mohlo by spôsobiť ďalšie náklady povinným subjektom zo zákona. Pri kreovaní IS a definovaní formulárov sa úrad zaviazal na intenzívnu spoluprácu s príslušnými dotknutými subjektami. Po vysvetlení bol rozpor odstránený. |
| **MOSR** | **K Čl. I, § 16 ods. 2 písm. a)** § 16 ods. 2 písm. a) odporúčam vypustiť. Odôvodnenie: Navrhované ustanovenie odporúčam vypustiť, nakoľko „spoluprácu s ostatnými jednotkami CSIRT“ nie je možné považovať za preventívnu službu, ktorá je poskytovaná klientele (rozumej inštitúciám/organizáciám v rámci sektora). | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že spolupráca predstavuje vymieňanie si informácií dôležitých na zabezpečenie kybernetickej prevencie. |
| **MOSR** | **K Čl. I, § 23** § 23 žiadam prepracovať a doplniť. Odôvodnenie: Navrhované ustanovenie nemá žiadnu výpovednú hodnotu. Nie je jasné z čoho predkladateľ návrhu zákona vychádzal pri definovaní názvov kategórií, nakoľko tie nezodpovedajú štandardným kategóriám (napr. nízka, stredná, vysoká úroveň). Chýba všeobecne záväzný právny predpis, ktorý definuje spôsob klasifikácie bezpečnostných kybernetických incidentov. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | N | Vaša pripomienka nebola akceptovaná a znenie bolo vypustené. Právna úprava bola premietnutá v preformulovanej podobe s obsahom aj jednotlivých kriteriálnych parametrov v rámci ustanovenia o hlásení kybernetických bezpečnostných incidentov. Parametre sú v súlade so smernicou NIS na určenie závažného kybernetického bezpečnostného incidentu. Jednotlivé kategórie sú odstupňované od závažnosti od 1 po 3, v záujme flexibilného reagovania na bezpečnostné prostredie je nevyhnutné špecifikáciu prenechať do vykonávacieho predpisu. Po vysvetlení bol rozpor odstránený. |
| **MOSR** | **K Čl. I, § 24 ods. 5** § 24 ods. 5 žiadam z dôvodu vnútorného rozporu s predchádzajúcimi ustanoveniami návrhu zákona preformulovať. Odôvodnenie: Na základe tohto ustanovenia úrad uzatvára s PZS dohodu o spôsobe a forme hlásenia na jednej strane a na strane druhej podľa § 10 ods. 6 je PZS povinná poskytnúť informácie spôsobom určeným funkcionalitou jednotného informačného systému. Uvedené žiadam zosúladiť. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **K Čl. I, § 34 ods. 4** § 34 ods. 4 žiadam upraviť vo vzťahu k prílohe č. 1 k návrhu zákona. Odôvodnenie: Predkladateľ návrhu zákona definovaním sektorov a zodpovedných vecne príslušných autorít zavádza duplicity a nejednoznačnosť v legislatíve, čo zároveň priznáva a navrhuje riešiť neakceptovateľným spôsobom, t. j. navrhuje, že sa vecne príslušné autority „dohodnú“, alebo rozhodne úrad. Výklad zákona musí byť jednoznačný a úrad nerozhoduje o kompetenciách ostatných ústredných orgánov štátnej správy. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **K Čl. I, § 6 ods. 2** § 6 ods. 2 žiadam vypustiť. Odôvodnenie: Povinne zverejňované zmluvy sú definované v zákone 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií), bez možnosti negatívneho vymedzenia v osobitnom zákone. Z tohto dôvodu nie je možné úpravu vykonať tak, ako to navrhuje predkladateľ návrhu zákona, keďže by to znamenalo nepriamu novelizáciu zákona. Zároveň zabezpečovanie plnenia úloh vyplývajúcich z medzinárodných zmlúv dohodami o spolupráci s fyzickými osobami a právnickými osobami považujem za neakceptovateľné. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | ČA | Pripomienka bola čiastočne akceptovaná. Pri uzatváraní dohôd, ktoré odpovedajú na konkrétne požiadavky zabezpečenia bezpečnosti nejde o svojvoľné poskytovanie informácií, ale o dodržanie všetkých princípov aplikovaných v rámci režimu ochrany utajovaných skutočností. Osobe teda budú poskytnuté informácie v rozsahu need to know, osoba bude musí byť držiteľom platného osvedčenia NBÚ na oboznamovanie sa s utajovanými skutočnosťami v požadovanom rozsahu. Právnické osoby boli z textu vypustené. Rovnako bolo vypustené ustanovenie o nezverejňovaní dohôd podľa zákona č. 211/2000 ZZ. MOSR vznieslo požiadavku, aby rovnakú možnosť mali aj ústredné orgány, čomu úrad vyhovel. Po vysvetlení bol rozpor odstránený. |
| **MOSR** | **K Čl. I, § 30** 1. Odporúčam upraviť text poznámky pod čiarou k odkazu 32, nakoľko ten sa odkazuje na zákon č. 357/2015 Z. z. o finančnej kontrole a audite, ktorý však neupravuje vykonávanie auditov zameraných na kybernetickú bezpečnosť, ale na finančné riadenie. 2. Odporúčam preformulovať odsek 3, keďže chýba právny predpis, ktorý upravuje získanie spôsobilosti vykonávať audity informačných systémov. | O | A |  |
| **MOSR** | **K Čl. IV, body 3 až 5** Body 3 až 5 žiadam vypustiť. Odôvodnenie: Plánovanie kybernetickej obrany je súčasťou plánovania obrany štátu. Samostatný plán kybernetickej obrany nemá opodstatnenie, MO SR predkladá na rozhodnutie vláde SR plány použitia ozbrojených síl SR v čase vojnového stavu a v čase vojny a ich súčasťou bude aj obrana kybernetického priestoru Slovenskej republiky. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A | Po vysvetlení rozpor odstránený. MO SR predložilo návrh noviel dotknutých právnych predpisov vo svojej pôsobnosti, ktoré budú súčasťou návrhu zákona o kybernetickej bezpečnosti. |
| **MOSR** | **Všeobecne** Cieľom návrhu zákona o kybernetickej bezpečnosti v zmysle legislatívneho zámeru zákona o informačnej bezpečnosti, na ktorý sa predkladateľ odvoláva, malo byť vytvorenie všeobecného právneho rámca pre ochranu celého kybernetického priestoru Slovenskej republiky. Predkladateľ návrhu zákona nezohľadňuje v dostatočnej miere už existujúcu legislatívu a odvolávajúc sa na transpozíciu smernice „NIS“ zavádza duplicity na jednej strane a nepokrýva niektoré dôležité oblasti na strane druhej (napr. podporné systémy pre KII, sektory mimo definovaných prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb). Na základe uvedeného žiadam návrh zákona dopracovať. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **K Čl. VII** Do čl. VII žiadam vložiť nový bod 2., ktorý znie: „2. § 60 sa dopĺňa odsekom 9, ktorý znie: „(9) Na poskytovanie utajovaných skutočností medzi ozbrojenými silami Slovenskej republiky a ozbrojenými silami iného štátu, aliančného a koaličného partnera alebo partnera vo vojenskej operácii v rámci spolupráce uskutočňovanej podľa osobitného predpisu23a) sa odseky 3 až 6 nevzťahujú; v takýchto prípadoch s poskytnutím utajovaných skutočností musí súhlasiť minister obrany, o čom vedie evidenciu.“. Poznámka pod čiarou k odkazu 23a znie: „23a) § 11 ods. 1 zákona č. 321/2002 Z. z. o ozbrojených silách Slovenskej republiky v znení neskorších predpisov.“. Odôvodnenie: Navrhovaným ustanovením sa právne upraví medzinárodná spolupráca ozbrojených síl SR v oblasti výmeny utajovaných skutočností pre potreby plnenia úloh kolektívnej obrany SR a to aj v oblasti kybernetickej bezpečnosti a kybernetickej obrany. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **Všeobecne** Návrh zákona odporúčame upraviť po jazykovej, gramatickej a legislatívno-technickej stránke. Napríklad: V § 2 ods. 2 písm. a) odporúčame na konci pripojiť slová „skutočností“. V § 3 písm. i) odporúčame vypustiť slovo „je“. V § 8 odporúčame slovo „severoatlantickej“ nahradiť slovom „Severoatlantickej“, slovo „reportingové“ odporúčame nahradiť vhodným slovenským pojmom, slová „medzinárodným organizáciám“ odporúčame nahradiť slovami „medzinárodnými organizáciami“. V § 10 odporúčame v odseku 2 písm. j) slovo „odsek“ nahradiť slovom „ods.“ a v odseku 4 odporúčame slová „ods. 2 písmeno j)“ nahradiť slovami „odseku 2 písm. j)“. V § 11 ods. 2 odporúčame slová „ods. 1 písmeno b)“ nahradiť slovami „odseku 1 písm. b)“. V § 17 ods. 1 odporúčame za slovo „ktorým“ vložiť slovo „je“. V § 28 ods. 5 odporúčame slovo „poskytovateľ“ nahradiť slovom „poskytovateľovi. V § 29 ods. 3 odporúčame slovo „môžu“ nahradiť slovom „môže“. V § 32 ods. 1 odporúčame slová „§ 18 ods. 2 a 3 a ods. 5 a 6“ nahradiť slovami „§ 18 ods. 2, 3, 5 a 6“. V § 32 ods. 3 odporúčame slovo „od.“ nahradiť slovom „ods.“. V čl. III odporúčame v navrhovanom § 101a ods. 1 slovo „vykonávania“ nahradiť slovom „vykonávanie“ (táto pripomienka sa primerane vzťahuje aj na čl. X bod 2). | O | A | Text upravený v zmysle pripomienok pripomienkujúcich subjektov. |
| **MOSR** | **K Čl. I, § 3** Návrh zákona sa koncepčným riešením terminológie nezaoberá, ale vyberá pojmy z prekladu smernice NIS a iných zdrojov, čo vedie k nekonzistencii terminológie. Konkrétne zákon nedefinuje základné pojmy ako aktívum, zraniteľnosť, hrozba, nositeľ hrozby, útok, dopad, hodnota rizika, akceptovateľné riziko, analýza rizík, bezpečnostný projekt, politika informačnej bezpečnosti (politika kybernetickej bezpečnosti neexistuje), dôvernosť, integrita, dostupnosť, autentickosť a i. Na základe uvedeného odporúčam tieto pojmy v návrhu zákona vymedziť. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná. Bol upravený celý § 3 a boli zavedené nové pojmy. |
| **MOSR** | **K Čl. X** Podľa Čl. X návrhu zákona plat štátneho zamestnanca podľa § 124 zákona č. 55/2017 z. z. o štátnej službe a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 55/2017 Z. z.“) bude tvoriť aj príplatok za výkon špecializovanej činnosti. Nariadením vlády SR č. 113/2017 Z. z., ktorým sa ustanovujú odbory štátnej služby, bol v § 3 Špeciálne obory ustanovený aj nový odbor štátnej služby 2.27 – Kybernetická bezpečnosť. Nakoľko bude do systému odmeňovania štátnych zamestnancov zavedený nový príplatok za výkon špecializovanej činnosti a vzhľadom na nový odbor štátnej služby, žiadam vložiť nový bod 2., ktorým sa do prílohy č. 2 k zákonu č. 55/2017 Z. z. doplnia aj činnosti podľa návrhu tohto zákona, aby bolo možné jasne určiť, komu patrí príplatok za výkon špecializovanej činnosti. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | N | Pripomienka UVSR akceptovaná a ustanovenie vypustené bez náhrady, pripomienku teda nemožno akceptovať. |
| **MOSR** | **K Doložke vybraných vplyvov a Analýze vplyvov na rozpočet verejnej správy** Predložený návrh zákona bude mať dosah na rozpočet kapitoly MO SR. V súčasnej etape prípravy návrhu zákona však nie je možné kvantifikovať potreby rozpočtového krytia opatrení na zabezpečenie plnenia úloh určených do pôsobnosti MO SR. Predmetný návrh zákona zavádza pre MO SR nové úlohy s reálnym predpokladom vzniku požiadaviek na vyčlenenie a na vytvorenie potrebných materiálnych a personálnych zdrojov. Potrebu finančných zdrojov na rozpočtové zabezpečenie plnenia úloh v pôsobnosti MO SR bude možné kvantifikovať až v procese realizácie jednotlivých opatrení na základe konkretizácie a špecifikácie požiadaviek na materiálne a personálne zdroje určené na ich zabezpečenie. Predpokladáme, že špecifikáciu a kvantifikáciu potrebných materiálnych a personálnych zdrojov, ktoré nie sú v pôsobnosti MO SR ešte vytvorené a rozpočtovo zabezpečené, bude možné vykonať až v priebehu roku 2018 s následným reálnym dopadom na rozpočet kapitoly MO SR v roku 2019 a v nasledujúcich rokoch. Z uvedeného dôvodu bude MO SR požadovať navýšenie finančných zdrojov pre kapitolu MO SR z titulu realizácie povinností vyplývajúcich z predloženého návrhu zákona pri tvorbe návrhu štátneho rozpočtu na roky 2019 – 2021. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **K Čl. I, § 10** Predmetný systém má okrem iného obsahovať registre dotknutých subjektov, slúžiť ako komunikačný systém pre hlásenie a riešenie bezpečnostných incidentov a centrálny systém včasného varovania. Na základe uvedeného je zjavné, že systém bude koncentrovať informácie o subjektoch zabezpečujúcich „kritické spoločenské a hospodárske činnosti“ a citlivé informácie týkajúce sa bezpečnosti SR. Takto koncipovaný systém by nemal byť „verejný“, nakoľko už len samotný zoznam subjektov poskytujúcich kritické služby spĺňa podmienky ochrany stupňa utajenia „Vyhradené“ v zmysle zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. | O | A | Vaša pripomienka bola akceptovaná a zapracovaná. Samotný systém bude budovaný na základe príslušného stupňa ochrany a bude takýmto spôsobom aj zabezpečený. |
| **MOSR** | **K Čl. I, § 8** Slová „organizáciami vzájomnej kolektívnej bezpečnosti“ odporúčame nahradiť slovami „Organizáciou Severoatlantickej zmluvy“, prípadne iným vhodným pojmom. Odôvodnenie: V prvej časti vety sa používa pojem „Organizácia severoatlantickej zmluvy“ na účely zabezpečenia spolupráce Úradu s členskými štátmi Európskej únie a Organizácie Severoatlantickej zmluvy. V druhej časti vety sa však pri spolupráci Úradu s tam uvedenými orgánmi na účely zabezpečenia kybernetickej bezpečnosti používa označenie „organizácie vzájomnej kolektívnej bezpečnosti“. Upozorňujeme, že organizácia vzájomnej kolektívnej bezpečnosti je iba jedna (Organizácia Spojených národov). Pokiaľ sa nemá na mysli OSN, predkladateľ mal pravdepodobne v úmysle označiť „organizáciu kolektívnej obrany“, ktoru je NATO. V takomto prípade však aj z hľadiska používaného jazyka navrhujeme ako vhodnejšie použiť slová „Organizácia Severoatlantickej zmluvy“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený a zaradený medzi úlohy úradu z dôvodu duplicitnej úlohy v zákone na účely konkrétnej definície stanovených opatrení v oblasti medzinárodných vzťahov a spolupráce. |
| **MOSR** | **K prílohe č. 1** Tabuľka vykazuje veľké množstvo nedostatkov. Požadujeme zdôvodniť a náležite upraviť. Odôvodnenie: Tabuľka 3, ktorá má byť Prílohou 1 Zákona: 1) nie je odôvodnená v Dôvodovej správe, 2) nie je zdôvodnené, prečo je oproti analogickej prílohe Smernice NIS rozšírená o tri sektory, 3) podsektory „obrana“, „bezpečnosť“ a „utajované skutočnosti“ sú veľmi špecifické a z hľadiska priameho dopadu ich narušenia na hospodárske funkcie štátu ťažko posúditeľné, 4) nie je jasné, aký je vzťah tabuľky k sektorom kritickej infraštruktúry, 5) nie je jasné, prečo sektor Digitálna infraštruktúra nie je zaradený ako podsektor sektora elektronických komunikácií a priradený Ministerstvu dopravy, keď prvkami tohto sektora sú internetové prepojovacie uzly, správa TLD Internetu, ktorého technologická časť spadá prirodzene pod Elektronické komunikácie, 6) existuje rozpor so zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy (ISVS) vo veci určenia VPA pre ISVS, 7) NBÚ vystupuje v troch (pod)sektoroch, ako ústredný orgán štátnej správy zodpovedný za riadenie a kontrolu a zároveň aj ako VPA. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A | Vysvetlené na rozporovom konaní, vyčerpávajúce odôvodnenie bude uvedené v dôvodovej správe. |
| **MOSR** | **K Čl. I, § 10 ods. 1** V § 10 ods. 1 za slovo „správcom“ žiadam vložiť slová „a prevádzkovateľom“. Odôvodnenie: Uvedenou úpravou sa ustanovenie zosúlaďuje s § 6 ods. 1 písm. p). Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **K Čl. I, § 12 ods. 1** V § 12 ods. 1 odporúčam vypustiť druhú vetu. Odôvodnenie: Mlčanlivosť je dostatočne ustanovená v platnej legislatíve SR aj na účely tohto zákona. Napríklad: Zákonník práce, zákon č. 552/2003 Z. z. o výkone práce vo verejnom záujme v znení neskorších predpisov, zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 45/2011 Z. z. o kritickej infraštruktúre, zákon č. 281/2015 Z. z. o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov. V prípade neakceptovania tejto pripomienky odporúčame v poznámke pod čiarou k odkazu 16 vložiť slová „Zákon č. 281/2015 Z. z. o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov.“. | O | A | Bol akceptovaný druhý variant Vašej pripomienky. |
| **MOSR** | **K Čl. I, § 13 ods. 8** V § 13 ods. 8 žiadam slovo „môže“ nahradiť slovami „je povinný“ a slová „Ak úrad akreditáciu uzná, vydá o tom“ žiadam nahradiť slovami „O uznaní akreditácie úrad vydá“. Odôvodnenie: V medzinárodnom prostredí pôsobia v oblasti kybernetickej/informačnej bezpečnosti aj iné typy jednotiek CSIRT/CERT (komerčné, akademické), ktoré návrh zákona obchádza a nerieši ich. Pri zachovaní navrhovaného ustanovenia môže dôjsť k situácií, kedy jednotka CSIRT certifikovaná medzinárodnou certifikačnou autoritou (Trusted Introducer, FIRST), nebude uznaná v zmysle platnej legislatívy SR. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A | Upravený text, podľa ktorého úrad na základe žiadosti uzná aj akreditáciu jednotky CSIRT, ktorá bola akreditovaná podľa predpisov iného štátu alebo medzinárodnej organizácie, ak je zabezpečené splnenie podmienok akreditácie jednotky CSIRT podľa tohto zákona s výnimkou § 14 písmeno a) (požadované technické, technologické a personálne vybavenie podľa osobitného predpisu, ktorý vydá úrad). Z uvedenej úpravy vyplýva, že úrad nebude nanovo posudzovať technické, technologické a personálne spôsobilosti jednotky CSIRT, ktoré už boli posúdené kompetentným zahraničným subjektom. |
| **MOSR** | **K Čl. I, § 14 ods. 1 písm. d)** V § 14 ods. 1 písm. d) odporúčame slovo „zabezpečenom“ nahradiť slovom „chránenom“ v súlade s terminológiou používanou vo vyhláške Národného bezpečnostného úradu č. 336/2004 Z. z., na ktorú sa odkazuje. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že textácia je v súlade so smernicou NIS. |
| **MOSR** | **K Čl. I, § 16 ods. 3** V § 16 ods. 3 žiadam za písmeno b) vložiť nové písmeno c), ktoré znie: „c) reakcia na kybernetické bezpečnostné incidenty,“. Doterajšie písmená c) až e) žiadam označiť ako písmená d) až f). Odôvodnenie: Z uvedeného vyplýva, že CSIRT analyzuje vzniknutý kybernetický bezpečnostný incident, poskytuje podporu, koordinuje reakciu, navrhuje opatrenia na zabránenie jeho ďalšieho pokračovania, ale nemá aktívne zasahovať do prebiehajúceho kybernetického bezpečnostného incidentu. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **K Čl. I, § 27 ods. 6** V § 27 od. 6 odporúčam vysvetliť pojem ochranné opatrenie. Odôvodnenie: V predmetnom ustanovení sa používa pojem „ochranné opatrenie“, pričom návrh zákona nedefinuje jeho význam.. | O | A | Vaša pripomienka bola akceptovaná a ustanovenie bolo doplnené. |
| **MOSR** | **K Čl. I, § 27 ods. 4** V § 27 ods. 4 žiadam doplniť okrem núdzového stavu, ďalšie krízové situácie, ktoré môžu nastať. Odôvodnenie: Ustanovuje sa vykonanie reaktívneho opatrenia iba počas núdzového stavu. Dôvodová správa neobsahuje a z návrhu zákona nevyplýva, prečo nemôžu byť vykonané reaktívne opatrenia napr. aj v čase výnimočného stavu alebo vojnového stavu. Ustanovenie navrhujem upraviť tak, aby sa reaktívne opatrenia a ďalšie opatrenia uvedené v § 27 vykonávali aj v ďalších krízových situáciách. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | N | Vaša pripomienka nebola akceptovaná. Úrad nahradil v celom texte núdzový stav a výnimočné stavy pojmom krízová situácia. Z textu bolo vypustené ustanovenie o vyhlasovaní núdzového stavu kybernetickej bezpečnosti bez náhrady a text bol upravený tak, aby v kontexte návrhu zákon upravoval „civilný“ stav zachovania bezpečnosti bez akéhokoľvek kompetenčného presahu na zákony, ktorých gestorom je MOSR a ktoré sa týkajú obrany Slovenskej republiky. Po vysvetlení bol rozpor odstránený. |
| **MOSR** | **K Čl. I, § 28 ods. 1** V § 28 ods. 1 žiadam spresniť podmienky na vyhlásenie stavu kybernetického ohrozenia. Odôvodnenie: V § 28 ods. 1 sa ustanovujú podmienky kybernetického ohrozenia, pričom sa nevychádza z § 23, ktorý ustanovuje kategorizáciu kybernetických bezpečnostných incidentov. Podmienky vzniku stavu kybernetického ohrozenia nie sú v návrhu zákona presne vymedzené a nie sú dostatočne presne vymedzené aj v spojitosti s uvedeným narušením bezpečnosti podľa čl. 1 ods. 3 ústavného zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení neskorších predpisov (ďalej len „zákon č. 227/2002 Z. z.“). Nie je uvedené, či budú obmedzené základné práva a slobody alebo ukladané povinnosti a ich rozsah. Zároveň poznamenávam, že ak príde k narušeniu bezpečnosti a k splneniu podmienok na vyhlásenie núdzového stavu, výnimočného stavu alebo vojnového stavu podľa citovaného zákona, príslušný stav môže byť vyhlásený alebo bude vypovedaná vojna, a to bez ohľadu na ustanovenie odseku 7, ktoré umožňuje NBÚ požiadať vládu Slovenskej republiky o vyhlásenie krízovej situácie. Vláda môže vyhlásiť núdzový stav len za podmienok ustanovených v čl. 5 ústavného zákona č. 227/2002 Z. z. Z dôvodovej správy k návrhu zákona nevyplýva potreba zmeny ďalších všeobecne záväzných právnych predpisov. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | ČA | Vaša pripomienka nebola akceptovaná. Úrad nahradil v celom texte núdzový stav a výnimočné stavy pojmom krízová situácia. Z textu bolo vypustené ustanovenie o vyhlasovaní núdzového stavu kybernetickej bezpečnosti bez náhrady a text bol upravený tak, aby v kontexte návrhu zákon upravoval „civilný“ stav zachovania bezpečnosti bez akéhokoľvek kompetenčného presahu na zákony, ktorých gestorom je MOSR a ktoré sa týkajú obrany Slovenskej republiky. Po vysvetlení bol rozpor odstránený. MO SR predložilo návrh noviel dotknutých právnych predpisov vo svojej pôsobnosti, ktoré budú súčasťou návrhu zákona o kybernetickej bezpečnosti. |
| **MOSR** | **K Čl. I, § 28 ods. 7** V § 28 ods. 7 odporúčam vypustiť slovo „vláda“. Odôvodnenie: Vyhlasovanie krízových situácií patrí do kompetencie nielen vlády SR, ale aj prezidenta SR. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **MOSR** | **K Čl. I, § 28 ods. 8** V § 28 ods. 8 žiadam vypustiť slová. „alebo môže byť použitý ako prostriedok teroristického útoku.“ Odôvodnenie: Bezpečnostný incident nie je možné použiť ako prostriedok teroristického útoku. Toto tvrdenie nie je sémanticky správne, nakoľko sa jedná o cielenú aktivitu útočníka. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | ČA | Úrad nahradil v celom texte núdzový stav a výnimočné stavy pojmom krízová situácia. Z textu bolo vypustené ustanovenie o vyhlasovaní núdzového stavu kybernetickej bezpečnosti bez náhrady a text bol upravený tak, aby v kontexte návrhu zákon upravoval „civilný“ stav zachovania bezpečnosti bez akéhokoľvek kompetenčného presahu na zákony, ktorých gestorom je MOSR a ktoré sa týkajú obrany Slovenskej republiky. Úrad upravil nové ustanovenie v ktorom v súvislosti s vašou pripomienkou uviedol, že ak situácia nasvedčuje, že môže ísť o kybernetický terorizmus, bezodkladne o tok upovedomí MOSR a následne aj BRSR. Po vysvetlení bol rozpor odstránený. MO SR predložilo návrh noviel dotknutých právnych predpisov vo svojej pôsobnosti, ktoré budú súčasťou návrhu zákona o kybernetickej bezpečnosti. |
| **MOSR** | **K Čl. I, § 28 ods. 9 písm. c)** V § 28 ods. 9 písm. c) žiadam vypustiť slová. „alebo môže byť použitý ako prostriedok teroristického útoku.“ Odôvodnenie: Odôvodnenie totožné s odôvodnením uvedeným k pripomienke k § 28 ods. 8. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | ČA | Po vysvetlení rozpor odstránený. MO SR predložilo návrh noviel dotknutých právnych predpisov vo svojej pôsobnosti, ktoré budú súčasťou návrhu zákona o kybernetickej bezpečnosti. |
| **MOSR** | **K Čl. I, § 28 ods. 9** V § 28 ods. 9 žiadam v úvodnej vete slová „vykonáva v potrebnom rozsahu štátnu správu“ nahradiť slovami „riadi a koordinuje výkon štátnej správy“. Odôvodnenie: Kybernetická bezpečnosť je zabezpečovaná prostredníctvom ochrany kybernetického priestoru a obrany štátu aj v kybernetickom priestore. Opatrenia ochrany kybernetického priestoru musia byť vykonávané aj pri obrane štátu (v čase vojnového stavu a vojny). Štátnu správu v čase núdzového stavu, výnimočného stavu alebo mimoriadnej situácie aj v oblasti kybernetickej bezpečnosti vykonávajú príslušné ústredné orgány štátnej správy v súlade s kompetenčným zákonom. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | ČA | Po vysvetlení rozpor odstránený. MO SR predložilo návrh noviel dotknutých právnych predpisov vo svojej pôsobnosti, ktoré budú súčasťou návrhu zákona o kybernetickej bezpečnosti. |
| **MOSR** | **K Čl. I, § 29 ods. 6** V § 29 žiadam vypustiť odsek 6. Odôvodnenie: Umožniť príslušníkom úradu v súvislosti s výkonom kontroly a v rozsahu potrebnom na jej vykonanie vstupovať do komunikačných a informačných systémov do úrovne správcu systému, vrátane oprávnenia dočasne zmeniť hardvérovú alebo softvérovú konfiguráciu považujem za neprimerané a nad rámec kompetencií úradu. Pri prístupe do systémov hrozí, že sa príslušník úradu oboznámi s citlivými informáciami nad rámec svojich oprávnení. Zároveň, vzhľadom na § 6 ods. 2, ktorý umožňuje NBÚ najať akúkoľvek osobu na vykonávanie úloh podľa tohto zákona, môžu sa kontroly zúčastňovať aj tretie strany. Je potrebné taktiež ustanoviť zodpovednosť za škodu spôsobenú zásahmi príslušníka úradu do systému. Treba zároveň brať do úvahy, že zásahom do systému môžu byť porušené zmluvné dohody a prevádzkovateľ stratí záruku u dodávateľa. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **K Čl. I, § 3 písm. d)** V § 3 písm. d) odporúčam upraviť definíciu pojmu kybernetická bezpečnosť. Odôvodnenie: Chybná definícia pojmu, nakoľko podľa tohto ustanovenia je kybernetická bezpečnosť stav, čo nie je pravdou, pretože stav je statický pojem a kybernetická bezpečnosť je súhrn procesov, vzťahov, ... Takto zadefinovaný pojem spôsobuje nekonzistenciu celého zákona, napr.: - v názve zákona „Zákon o kybernetickej bezpečnosti“ je vlastne „Zákon o stave“, pričom celý zákon je o procesoch a nie o stave. - podľa § 6 písm. d) úrad vypracúva národnú stratégiu „o stave...“ a ročnú správu o stave „stavu...“ v Slovenskej republike, - podľa § 8 je úrad národným kontaktným miestom pre „stav...“ pre zahraničie, - podľa § 9 ods. 4 vláda schvaľuje „Národnú stratégiu „stavu...odolávania proti kybernetický útokom...“. | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **MOSR** | **K Čl. I, § 3 písm. e)** V § 3 písm. e) odporúčam upraviť definíciu pojmu „riziko“. Odôvodnenie: Chybná definícia pojmu, nakoľko predkladateľ návrhu zákona zamenil definíciu pojmu riziko za hrozbu. | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **MOSR** | **K Čl. I, § 3 písm. f)** V § 3 písm. f) odporúčam upraviť definíciu pojmu „kybernetický bezpečnostný incident“. Odôvodnenie: Chybná definícia pojmu, nakoľko podľa tohto ustanovenia je kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je .... vysoká pravdepodobnosť kompromitácie činností základnej alebo digitálnej služby alebo ohrozenie informácií. Incidentom nie je „žiadna pravdepodobnosť“, pretože incident sa musí reálne udiať. | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **MOSR** | **K Čl. I, § 3 písm. g) a h)** V § 3 písm. g) odporúčam upraviť definíciu pojmu „základná služba“ a v písm. h) odporúčam upraviť definíciu pojmu „prevádzkovateľ základnej služby“. Odôvodnenie: Chybná definícia pojmov, nakoľko pojmy základná služba a jej poskytovateľ nie sú v návrhu zákona dostatočne zadefinované. Navrhujeme zosúladiť definíciu so smernicou NIS, z ktorej predkladateľ návrhu zákona pri spracovaní návrhu zákona vychádzal (článok 5 smernice NIS: „an entity that provides a service which is essential for maintenance of critical societal and/or economic activities...“). | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **MOSR** | **K Čl. I, § 3 písm. k)** V § 3 písm. k) odporúčam upraviť definíciu pojmu „riešenie kybernetického bezpečnostného incidentu“. Odôvodnenie: Chybná definícia pojmu, nakoľko tento nezahŕňa činnosti spojené s reakciou v priebehu bezpečnostného incidentu. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná. Bol upravený celý § 3 a boli zavedené nové pojmy. |
| **MOSR** | **K Čl. I, § 4 ods. 2** V § 4 ods. 2 sa ustanovujú podmienky zásahu do základných práv a slobôd, a to v rozsahu nevyhnutnom na zabezpečenie ochrany kybernetického priestoru. Poznamenávame, že návrh zákona neupravuje ochranu kybernetického priestoru komplexne, pracuje s pojmom kybernetická bezpečnosť (napr. spoločný nadpis „systém zabezpečenia kybernetickej bezpečnosti“). V návrhu zákona žiadam vymedziť ochranu kybernetického priestoru a aj obranu kybernetického priestoru. Odôvodnenie: Ochrana kybernetického priestoru musí byť zabezpečená nepretržite aj v čase, keď je tento priestor bránený, pretože nemôže byť bránený pred všetkými bezpečnostnými incidentmi. Vymedzenie rozsahu zasiahnutia do základných práv a slobôd nemá normatívny charakter. Odporúčam predmetný rozsah doplniť príp. aj odkazom na príslušný všeobecne záväzný právny predpis. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | N | Pripomienka nebola akceptovaná z dôvodu, že text bol vypustený bez náhrady. Po vysvetlení bol rozpor odstránený. |
| **MOSR** | **K Čl. I, § 6 ods. 1 písm. b)** V § 6 ods. 1 písm. b) žiadam vypustiť slovo „záväzné“ a slovo „záväznú“. Odôvodnenie: Je sporné akým spôsobom bude posudzovaná záväznosť metodiky a záväznosť politiky, keďže jej obsah nie je súčasťou zákona a ani vykonávacieho predpisu. Žiadame uvedené ustanovenie zosúladiť z právnou praxou SR. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **K Čl. I, § 6 ods. 1 písm. k)** V § 6 ods. 1 písm. k) odporúčam zosúladiť s § 27 ods. 6. Odôvodnenie: V predmetnom ustanovení chýba výzva NBÚ navrhnúť ochranné opatrenie. | O | A |  |
| **MOSR** | **K Čl. I, § 6 ods. 1 písm. l)** V § 6 ods. 1 písm. l) odporúčam za slovo „republiky“ vložiť slová „a ministerstvom obrany“. Odôvodnenie: Zabezpečenie úloh kybernetickej bezpečnosti v oblastiach výskum, vývoj a vzdelávanie plní Ministerstvo obrany Slovenskej republiky a to prostredníctvom svojej vojenskej vysokej školy. Právna úprava navrhovaná v § 6 návrhu zákona vytvára dojem, že vzdelávanie, výskum a vývoj v oblasti kybernetickej bezpečnosti môžu vykonávať, resp. majú kompetencie len NBÚ a MŠVVŠ SR. Doplnením predmetného ustanovenia sa vytvorí inštitucionálny rámec na realizáciu opatrení a úloh vyplývajúcich pre MO SR z Koncepcie kybernetickej bezpečnosti SR na roky 2015-2020 a z Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti SR na roky 2015-2020, ktoré schválila vláda SR. V pôsobnosti MO SR je štátna vojenská vysoká škola, ktorá štúdiom vo všetkých troch stupňoch vysokoškolského vzdelávania pripravuje odborníkov na výkon štátnej služby profesionálnych vojakov. Študujú na nej aj civilní študenti. Okrem vysokoškolského vzdelávania je vojenská vysoká škola aj garantom celoživotného vzdelávania profesionálnych vojakov, poskytuje aj odborné vzdelávania v oblasti obrany a bezpečnosti pre zamestnancov štátnej a verejnej správy. Vojenská vysoká škola plní úlohy výskumu a vývoja pre MO SR a OS SR v oblastiach, ktoré spadajú do ich pôsobnosti a korešpondujú s ich potrebami. Doplnením predmetného ustanovenia sa vytvorí priestor na aktívne zapájanie a účasť vojenskej vysokej školy na realizáciu politiky SR v oblasti kybernetickej bezpečnosti a to v súlade s vyššie uvedenými koncepčnými dokumentmi – Koncepciou a Akčným plánom kybernetickej bezpečnosti. | O | A | Upravvené v § 9 návrhu zákona. |
| **MOSR** | **K Čl. I, § 6 ods. 1 písm. p)** V § 6 ods. 1 písm. p) žiadam slovo „vedie“ nahradiť slovami „spravuje a prevádzkuje“. Odôvodnenie: Jednotný informačný systém kybernetickej bezpečnosti predstavuje kritický systém, ktorý bude koncentrovať informácie o subjektoch zabezpečujúcich kritické spoločenské a hospodárske činnosti a citlivé informácie týkajúce sa bezpečnosti SR. Jasné definovanie úloh je nutnosťou pre zabezpečenie transparentnej a bezpečnej prevádzky a správy predmetného systému. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **K Čl. V, bod 4** V bode 4 odporúčam upraviť § 4e ods. 3, pretože nemá normatívny charakter (slová „orgán štátu, ktorý obmedzenie vykonal“). | O | A | Upravené v zmysle pripomienok MOSR. |
| **MOSR** | **K Čl. VIII, bod 4** V bode 4 v prílohe č. 3 k zákonu č. 45/2011 Z. z. žiadam ponechať pôvodné znenie alebo upraviť vo vzťahu k sektoru „Elektronické komunikácie“. Zadefinovanie nového sektora kritickej infraštruktúry považujem za nelogické. Odôvodnenie: Kybernetická bezpečnosť nepredstavuje sektor hospodárstva, ale prierezovú problematiku naprieč všetkými definovanými sektormi hospodárstva. Prakticky každý prvok kritickej infraštruktúry je závislý na informačných a komunikačných technológiách, teda kybernetický priestor nemôže byť považovaný za sektor rovnocenný so zdravotníctvom, priemyslom, energetikou atď. Výsledkom tohto návrhu je kompetenčný rozpor, pretože ak bude NBÚ zodpovedným orgánom za „Kybernetický priestor“ podľa definície v § 3 písm. b), dostane sa do rozporov so štátnymi orgánmi, ktoré zodpovedajú za oblasti, v ktorých sú kritické informačné systémy a siete prevádzkované. Vytvárajú sa tak duplicity v koordinácii, štruktúre riadenia, kontrole, ukladaní povinností a uplatňovaní sankčných mechanizmov. Predkladateľ pôvodný podsektor „Internet” nahrádza podsektorom „Kybernetický priestor”, nie je však jasné, aký dopad bude mať táto zmena na prvky, ktoré patrili do podsektoru „Internet”. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **K Čl. V, bod 4** V bode 4 žiadam upraviť § 4e ods. 1. Odôvodnenie: Pojem „neutralizácia útočníka kybernetického útoku“ nie je v návrhu zákona vymedzený. V návrhu zákona sa používajú rôzne pojmy napr. aktivity a ohrozenia v kybernetickom priestore, na inom mieste je to kybernetický bezpečnostný incident. Vymenovanie pôvodcov odporúčam vypustiť, pretože nie je úplný a namiesto pôvodcu odporúčame špecifikovať príslušné kybernetické bezpečnostné incidenty alebo činnosť ozbrojených síl na základe určených štandardov. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A | Po vysvetlení rozpor odstránený. MO SR predložilo návrh noviel dotknutých právnych predpisov vo svojej pôsobnosti, ktoré budú súčasťou návrhu zákona o kybernetickej bezpečnosti. |
| **MOSR** | **K Čl. V, bod 4** V bode 4 žiadam upraviť alebo vypustiť § 4e ods. 4. Odôvodnenie: Rozhodovanie o použití opatrenia podľa § 4e ods. 2 ministrom obrany alebo iným ministrom je neodôvodnené, je zbytočné a nie je v súlade so zákonom č. 321/2002 Z. z. o ozbrojených silách. O použití ozbrojených síl rozhoduje vláda Slovenskej republiky (rozhoduje o plánoch použitia ozbrojených síl v čase vojny vojnového stavu). Je potrebné presne vymedziť bezpečnostné incidenty, pri ktorých sa ozbrojené sily použijú, a to v systéme, v ktorom vykonáva štátnu správu úrad (NBÚ), funguje národná jednotka CSIRT, Centrum pre kybernetickú obranu, ďalšie jednotky CSIRT a vecne príslušné autority. Na základe presne určených štandardov sa v príslušnom pláne použitia ozbrojených síl, o ktorom rozhoduje vláda SR, určia aj kybernetické bezpečnostné incidenty, pri ktorých sa ozbrojené sily použijú. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A | Po vysvetlení rozpor odstránený. MO SR predložilo návrh noviel dotknutých právnych predpisov vo svojej pôsobnosti, ktoré budú súčasťou návrhu zákona o kybernetickej bezpečnosti. |
| **MOSR** | **K Čl. V, bod 4** V bode 4 žiadam z dôvodu nepresnosti upraviť § 4e ods. 2. Odôvodnenie: Text „Na účely kybernetickej obrany, ak je to nevyhnutné pre bezpečnosť a obranu štátu“ duplicitne vyjadruje obranu štátu, obrana v kybernetickom priestore je súčasťou obrany štátu. Nasledujúca podmienka vyjadrená slovami „a bezprostredne hrozí ujma na živote a zdraví“ je irelevantná v podmienkach vedenia kybernetického útoku, ktorý napr. spôsobí iba značné škody na majetku. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A | Po vysvetlení rozpor odstránený. MO SR predložilo návrh noviel dotknutých právnych predpisov vo svojej pôsobnosti, ktoré budú súčasťou návrhu zákona o kybernetickej bezpečnosti. |
| **MOSR** | **K Čl. IV, bod 6** V bode 6 v § 7 ods. 2 odporúčam doplniť nové písmená g) a h), ktoré znejú: „g) vykonáva výskum a vývoj, h) zabezpečuje vysokoškolské vzdelávanie a celoživotné vzdelávanie.“. Odôvodnenie: Uvedenou úpravou sa ustanovenie zosúlaďuje s § 6 ods. 1 písm. l) návrhu zákona o kybernetickej bezpečnosti. Odôvodnenie je totožné s odôvodnením k pripomienke k čl. I § 6 ods. 1 písm. l). | O | A | Upravené v zmysle pripomienok MOSR. |
| **MOSR** | **Čl. IV, bod 6** V bode 6 v § 7 ods. 2 žiadam vypustiť písmená c) a g). Odôvodnenie: Ak SR zabezpečuje svoju obranu aj v kybernetickom priestore – je súčasťou obrany štátu a vzťahuje sa na ňu proces obranného plánovania, pričom toto plánovanie už je v predmetnom zákone upravené. Navrhované ustanovenie je nejednoznačné, nakoľko požíva pojmy „v odôvodnených prípadoch“ a „informácie získané“, čo umožňuje ľubovoľný výklad týchto pojmov, čím nie je zabezpečená istota odstupovania potrebných informácií. V aplikačnej praxi je využitím osobitných zákonov (zákon o SIS a zákon o VS) toto odstupovanie možné zabezpečiť aj bez špeciálnej úpravy. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A | Upravené v zmysle pripomienok MOSR. |
| **MOSR** | **K Čl. IV, bod 6** V bode 6 v § 7 ods. 3 žiadam vypustiť slová „obranného plánovania,“. Odôvodnenie: Odôvodnenie je totožné s odôvodnením k pripomienke k čl. IV § 7 od. 2 písm. c). Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A | Po vysvetlení rozpor odstránený. MO SR predložilo návrh noviel dotknutých právnych predpisov vo svojej pôsobnosti, ktoré budú súčasťou návrhu zákona o kybernetickej bezpečnosti. |
| **MOSR** | **K Čl. IV, bod 6** V bode 6 v § 7 ods. 5 slová „infraštruktúry9e)“ odporúčam nahradiť slovami „infraštruktúry9f)“. Odôvodnenie: Úprava textu z dôvodu jeho nesprávnosti. | O | A | Upravené v zmysle pripomienok MOSR. |
| **MOSR** | **K Čl. VI** V Čl. VI žiadam vložiť nový bod 2., ktorým sa v prílohe č. 1 k zákonu č. 553/2003 Z. z. o odmeňovaní niektorých zamestnancov pri výkone práce vo verejnom záujme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 553/2003 Z. z.) do charakteristiky platových tried pre pracovné činnosti s prevahou duševnej práce pri výkone práce vo verejnom záujme doplnia charakteristické činnosti vyplývajúce z návrhu predmetného zákona. Následne žiadam doplniť konkrétne názvy činností do jednotlivých platových tried v nariadení vlády Slovenskej republiky č. 341/2004 Z. z., ktorým sa ustanovujú katalógy pracovných činností pri výkone práce vo verejnom záujme v znení neskorších predpisov (napr. do časti 07 Informatika) a žiadam vypracovať aj príslušné analytické listy. Odôvodnenie: Zamestnanci pri výkone práce vo verejnom záujme sú podľa zákona č. 553/2003 Z. z. zaradení do jednotlivých platových tried na základe najnáročnejšej vykonávanej pracovnej činnosti. Návrh zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov zavádza do systému odmeňovania týchto zamestnancov nové druhy pracovných činností, preto je nevyhnutné, aby tieto činnosti boli zachytené aj v prílohe č. 1 k zákonu č. 553/2003 Z. z. a boli aj konkretizované v citovanom nariadení vlády SR. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | N | Pripomienka UVSR akceptovaná a ustanovenie vypustené bez náhrady, pripomienku teda nemožno akceptovať Záver: bez rozporu. |
| **MOSR** | **K dôvodovej správe** V osobitnej časti dôvodovej správy k § 2 odporúčam upraviť znenie posledného odseku. Odôvodnenie: Súčasné znenie vo vzťahu k slovám „Ustanovenia tohto zákona sa z povahy jeho predmetnej úpravy ...“, evokuje, že predmetný zákon ako celok sa nebude vzťahovať na činnosti SIS a MO SR. Aby bolo zrejmé, že je to len v súvislosti s ustanovením § 2. | O | A |  |
| **MOSR** | **K prílohe č. 1** V prílohe č. 1 žiadam vypustiť podsektor spravodajské služby. Odôvodnenie: Spravodajské služby neposkytujú služby, ktoré majú zásadný význam z hľadiska zachovania kľúčových spoločenských a hospodárskych činností (distribúcia elektrickej energie, dodávka pitnej vody, doprava, atď.). Začlenenie SIS a VS medzi prevádzkovateľov základných služieb, resp. VPA je z tohto dôvodu neopodstatnené. Zároveň uvádzame, že zákon č. 184/1993 Z. z. upravuje krmivá. Nie je jasný súvis s problematikou spravodajských služieb. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A | Úrad zaradil Vojenské spravodajstvo medzi subjekty podľa § 4 písmeno b) a prispôsobil znenie prílohy č. 1. Rozpor bol odstránený. |
| **MOSR** | **Všeobecne** Z návrhu zákona nie je možné identifikovať prevádzkovateľov základných služieb, ktorým však tento návrh zákona ukladá povinnosti. Je legislatívne neprípustné, aby zákon ukladal povinnosti subjektom, ktoré budú známe až po určení kritérií vykonávacími predpismi vydanými v budúcnosti. Rovnako nie sú známe bezpečnostné opatrenia a rozsah ich implementácie. Predkladateľ návrhu zákona ustanovuje iba hrubý rámec riešenia problematiky bezpečnosti v kybernetickom priestore a definovanie kľúčových oblastí odkladá do budúcna, čím sa stáva zákon nezrozumiteľný a nefunkčný. Na základe uvedeného žiadam návrh zákona dopracovať. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **Nad rámec návrhu** Za čl. IX žiadam vložiť nový čl. X, ktorý znie: „Čl. X Zákon č. 281/2015 Z. z. o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov v znení zákona č. 378/2015 Z. z. a zákona č. 125/2016 Z. z. sa mení a dopĺňa takto: 1. V § 156 ods. 1 sa za písmeno h) vkladá nové písmeno i), ktoré znie: „i) príplatok za výkon špecializovanej činnosti,“. Doterajšie písmená i) až k) sa označujú ako písmená j) až l). 2. V § 156 od. 2 sa slová „písm. a) až i)“ nahrádzajú slovami „písm. a) až j)“. 3. Za § 164 sa vkladá § 164a, ktorý vrátane nadpisu znie: „164a Príplatok za výkon špecializovanej činnosti (1) Profesionálnemu vojakovi, ktorý vykonáva činnosť, ktorá vyžaduje vykonávanie osobitne významných úloh alebo mimoriadne náročných úloh v oblasti kybernetickej bezpečnosti, možno priznať príplatok za výkon špecializovanej činnosti až do výšky 90 % jeho hodnostného platu. (2) Funkcie a výšku príplatku podľa odseku 1 ustanoví služobný predpis. (3) Príplatok podľa odseku 1 sa zaokrúhľuje na 50 eurocentov nahor. Doterajší článok X sa označuje ako článok XI. Odôvodnenie: Vo všeobecnej časti dôvodovej správy sa uvádza, že návrh zákona komplexným spôsobom rieši odmeňovanie zamestnancov na strane štátu tak, aby bol štát schopný zamestnávať odborníkov v oblasti kybernetickej bezpečnosti a tým konkurovať súkromným spoločnostiam. V tejto súvislosti medzi týchto zamestnancov treba zaradiť aj profesionálnych vojakov, ktorí vykonávajú významné úlohy na úseku kybernetickej bezpečnosti. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A |  |
| **MOSR** | **K Čl. I, § 4** Zmysel tohto paragrafu nie je jasný. Zákon by mal ukladať konkrétne povinnosti, pričom v tomto ustanovení sú viac formulované predstavy, ktoré nie sú v aplikačnej praxi vykonateľné. Na základe uvedeného odporúčam celý § 4 prepracovať alebo vypustiť. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **MOSR** | **K Čl. IV, bod 1** Znenie bodu 1 žiadame nahradiť znením: „1. V § 2 ods. 2 sa za slovo „štátu“ vkladá čiarka a slová „ktorej súčasťou je aj obrana štátu v kybernetickom priestore (ďalej len „kybernetická obrana“),1a)“. Poznámka pod čiarou k odkazu 1 znie: „1a) Zákon č. .../2017 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“. Odôvodnenie: Vytváranie samostatného systému obrany štátu v kybernetickom priestore v existujúcom systéme obrany štátu, ktorý je súčasťou bezpečnostného systému Slovenskej republiky, nemá opodstatnenie. Systém obrany štátu zahŕňa všetky prvky a opatrenia potrebné na zabezpečenie obrany štátu. V predloženom návrhu zákona slová „aktívnych a pasívnych opatrení“ nie sú vymedzené. Nie je ustanovené, ktoré zložky plnia predmetné opatrenia ako je tomu v písmene a) návrhu, kde sú pri boji s terorizmom uvedené napr. spravodajské služby a súdy. Túto pripomienku považuje Ministerstvo obrany SR za zásadnú. | Z | A | Po vysvetlení rozpor odstránený. MO SR predložilo návrh noviel dotknutých právnych predpisov vo svojej pôsobnosti, ktoré budú súčasťou návrhu zákona o kybernetickej bezpečnosti. |
| **MPRVSR** | **§ 22 ods. 3**  na začiatku vety "Ak je poskytovateľ digitálnej služby usadený v Slovenskej republike..." odporúčame slovo "usadený" nahradiť iným, legislatívne vhodnejším slovom, napr. "má sídlo". | O | A |  |
| **MPRVSR** | **§ 11 ods. 1 písm. g)** Navrhujeme vypustiť slovo "vykonávanie" na začiatku ustanovenia pre nadbytočnosť. | O | A |  |
| **MPRVSR** | **§ 2 ods. 1**  Navrhujeme vypustiť v prvej vete slovo "súbor" navrhované znenie: "(1) Tento zákon ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti" | O | A |  |
| **MPRVSR** | **dôvodovej správe, všeobecnej časti** Odporúčame legislatívne skratky "PZS" a "PDS" nahradiť skratkami "prevádzkovateľ" a "poskytovateľ". | O | A |  |
| **MPRVSR** | **§ 31 ods. 3** Odporúčame na konci vety nahradiť slová " všeobecný predpis o priestupkoch" slovami "osobitný predpis". | O | N | Vaša pripomienka nebola akceptovaná z dôvodu legislatívnej praxe. |
| **MPRVSR** | **§ 32 ods. 8** Odporúčame na začiatku vety pred slová "obratom" vložiť slová "Celkovým ročným", doplniť vetu o údaj, že ide súčet všetkých tržieb, výnosov alebo príjmov z predaja tovaru alebo služieb bez nepriamych daní za konkrétne obdobie (t.j. rok) a na konci vety zvoliť poradie slov "poskytnutá finančná pomoc." namiesto "finančná pomoc poskytnutá". | O | N | Vaša pripomienka nebola akceptovaná z dôvodov uvedených v dôvodovej správe. |
| **MPRVSR** | **§ 9 ods. 2 písm. a)** Odporúčame nahradiť slová "iných relevantných aktérov" legislatívne vhodnejšími slovami. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že relevantné je vhodné slovo na pomenovanie pre významné alebo dôležité subjekty a je svojim smerovaním neutrálne. |
| **MPRVSR** | **§ 32 ods. 13** Odporúčame nahradiť vetu "Na konanie sa vzťahuje všeobecný predpis o správnom konaní." touto vetou "Na konanie o ukladaní pokút podľa tohto zákona sa vzťahuje správny poriadok" | O | N | Vaša pripomienka nebola akceptovaná, pretože Správny poriadok sa na právne vzťahy vzťahuje, ak nie je uvedené inak. |
| **MPRVSR** | **odkaz na poznámku pod čiarou 23** Odporúčame pripojiť na konci poznámky pod čiarou slová "v znení zákona č. 247/2015 Z. z." | O | A |  |
| **MPRVSR** | **§ 3 písm. d)** Odporúčame vypustiť slovo "je" z dôvodu nadbytočnosti. | O | A |  |
| **MPRVSR** | **§ 3 písm. f)** odporúčame zaradiť písmeno f) pred písmeno d), nakoľko sa v písmene d) už používa slovné spojenie "kybernetický bezpečnostný incident". | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **MPRVSR** | **poznámkam pod čiarou všeobecne** Poznámky pod čiarou k odkazom je potrebné zosúladiť s bodom 23.7 a 23.8 Legislatívnych pravidiel vlády: "23.7. Ak sa v poznámke pod čiarou uvádza taxatívny výpočet právnych predpisov, jednotlivé citácie právnych predpisov sa uvádzajú pod sebou ako samostatné vety v zostupnom poradí podľa stupňa právnej sily, vykonávacie právne predpisy v poradí nariadenie vlády, vyhláška, výnos a opatrenie, a následne v chronologickom poradí, pričom skôr prijatý právny predpis sa cituje ako prvý. 23.8. Ak sa v poznámke pod čiarou uvádza demonštratívny výpočet právnych predpisov, poznámka sa začína slovom „Napríklad“ a citácie právnych predpisov sa uvádzajú za sebou, oddeľujú sa čiarkou a bodka sa kladie až na koniec poslednej citácie. Na poradie citovania viacerých právnych predpisov sa vzťahuje primerane bod 23.7." | O | A |  |
| **MPRVSR** | **§ 2 ods. 2 písm. a)** Pre nadbytočnosť je potrebné vypustiť slová "o ochrane utajovaných". | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že je legislatívno-technicky nesprávna. |
| **MPRVSR** | **§ 8**  Slová "medzinárodným organizáciám" je potrebné dať do príslušného gramatického tvaru, a to "medzinárodnými organizáciami" Ďalej odporúčame medzi slovami "organizáciami vzájomnej kolektívnej bezpečnosti" a "inými medzinárodnými organizáciami" nahradiť spojku "alebo" spojkou a. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený a zaradený medzi úlohy úradu z dôvodu duplicitnej úlohy v zákone na účely konkrétnej definície stanovených opatrení v oblasti medzinárodných vzťahov a spolupráce. |
| **MPRVSR** | **§ 19 ods. 1** V druhej vete odporúčame doplniť odkaz na osobitný predpis, ktorý sa v texte vety spomína. | O | A | Vaša pripomienka bola akceptovaná a znenie bolo vypustené. |
| **MPRVSR** | **§ 5**  v písmene c) odporúčame pre duplicitu vypustiť bod 1, nakoľko v písmene b) je NBÚ spomenutý. Ďalej odporúčame nahradiť slovo "autorita/autority" iným, vhodnejším slovom v celom texte návrhu. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že úrad vystupuje aj ako vecne príslušný subjekt aj ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť a na základe toho má teda dve oddelené úlohy. |
| **MPRVSR** | **§ 17 ods. 1** V prvej časti vety odporúčame doplniť odkaz o aký všeobecne záväzný predpis ide. detto v § 24 ods. 1, § 24, § 25 ods. 1, § 28 ods. 9 písm. c). | O | A |  |
| **MPRVSR** | **§ 21 ods. 5** za slovami "digitálnej služby" je potrebné vypustiť slovo "je" pre nadbytočnosť. | O | A |  |
| **MPSVRSR** | **Všeobecná pripomienka** Odporúčame predkladaný materiál legislatívno-technicky upraviť, napríklad v § 2 ods. 2 písm. a) odporúčame na konci pripojiť slovo „skutočností“ a odkaz 2 umiestniť nad slovo „skutočností“; v § 3 odporúčame vo vzťahu k úvodnej vete § 3 upraviť písmená d), h) a i); v § 4 ods. 5 odporúčame slová „je kľúčovým prvkom kultúry riadenia rizík“ nahradiť napríklad slovami „sú kľúčovými prvkami systému riadenia rizík“, „sú kľúčovými prvkami v riadení rizík“, „sú kľúčovými prvkami pri riadení rizík“; v § 17 ods. 1 odporúčame upraviť vetu za bodkočiarkou; v prílohe č. 1 odporúčame skratky „PZS“ a „VPA“ nahradiť plným znením skracovaných slov. Odôvodnenie: Legislatívno-technická pripomienka. | O | A |  |
| **MPSVRSR** | **K § 17 ods. 1**  Odporúčame v § 17 ods. 1 špecifikovať, o aké prahové hodnoty kritérií ide, prípadne ktorý všeobecne záväzný právny predpis ich ustanovuje. Odôvodnenie: Z dôvodu potreby jednoznačnej a presnej právnej úpravy. | O | A | Vaša pripomienka bola akceptovaná a bola upravená v novom ustanovení. |
| **MSSR** | **§ 12 ods. 1** Bodku na konci prvej vety požadujeme nahradiť bodkočiarkou a pripojiť tieto slová: „povinnosť mlčanlivosti sa nevzťahuje na oznámenie kriminality alebo inej protispoločenskej činnosti.16)“. V poznámke pod čiarou k odkazu 16 je potrebné uviesť citáciu § 3 písm. b) a c) zákona č. 583/2008 Z. z. o prevencii kriminality a inej protispoločenskej činnosti a o zmene a doplnení niektorých zákonov, pričom sa prečíslujú ostávajúce odkazy a poznámky pod čiarou. V súvislosti s prijatím zákona č. 307/2014 Z. z. o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov došlo v právnom poriadku Slovenskej republiky k výraznému posunu chápania mlčanlivosti a „prelamovania“ povinnosti mlčanlivosti na účely prechádzania, odhaľovania, vyšetrovania a stíhania kriminality v tom význame, že porušením zákonom ustanovenej povinnosti mlčanlivosti nie je oznámenie kriminality alebo inej protispoločenskej činnosti. Z uvedeného dôvodu trváme na tom, aby predkladateľ rešpektoval tento trend a nebránil odhaľovaniu kriminality zavádzaním fakticky neobmedzenej povinnosti mlčanlivosti (podľa odseku je koncipovaná možnosť a nie povinnosť zbavenia mlčanlivosti). | Z | A |  |
| **MSSR** | **§ 11 ods. 1 písm. f)** Časť ustanovenia za bodkočiarkou požadujeme presunúť do § 17 ods. 1, keďže z hľadiska systematiky nepatrí do vymedzenia pôsobnosti vecne príslušnej autority. Ustanovenie o vymedzení pôsobnosti vecnej autority má upravovať rozsah tejto pôsobnosti a nie to ako sa táto pôsobnosť vykonáva. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ide o úlohu vecne príslušného subjektu, ktorá je technicky zaradená správne do ustanovenia týkajúceho sa verejne príslušného subjektu. |
| **MSSR** | **§ 5 a nasl.** Jedným z orgánov vykonávajúcim pôsobnosť v oblasti kybernetickej bezpečnosti je podľa návrhu aj vláda Slovenskej republiky. Vzhľadom na systematiku zákon, ktorý po § 5 upravuje pôsobnosť týchto orgánov, požadujeme za § 5 vložiť nový § 6, ktorý vymedzí konkrétnu pôsobnosť vlády Slovenskej republiky v oblasti kybernetickej bezpečnosti. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ide o zbytočnú úpravu. Vláda SR schvaľuje Národnú stratégiu kybernetickej bezpečnosti a úrad informuje vládu v čase stavu kybernetického ohrozenia. Úlohy vlády vyplývajú z iných predpisov a strategických dokumentov a tak by v tejto súvislosti išlo len o duplicitu, ktorá je nežiaduca. |
| **MSSR** | **§ 5 – nadpis**  Nadpis požadujeme upraviť nasledovne: „Organizácia a pôsobnosť orgánov verejnej moci v oblasti kybernetickej bezpečnosti“, a to aj s ohľadom na znenie § 1 písm. a). Je žiaduce doplniť nadpis o slová „v oblasti kybernetickej bezpečnosti“, keďže zákon neupravuje organizáciu a pôsobnosť orgánov verejnej moci vo všeobecnosti, ale na vymedzenom úseku štátnej správy, ktorou je kybernetická bezpečnosť. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že zákon o kybernetickej bezpečnosti nemôže už len z povahy príslušnosti upravovať pôsobnosť v inom sektore ako je jeho predmet pôsobnosti. Ide o legislatívnu techniku. |
| **MSSR** | **K § 12 ods. 7** Navrhujeme vypustiť celý odsek spolu s odkazom na poznámku pod čiarou č. 18. Odôvodnenie: Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov nie je právny predpis, ktorý by komplexne upravoval ochranu osobných údajov. Zákon č. 211/2000 Z. z. obsahuje ako dôvod nesprístupnenia ochranu osobných údajov (§ 9 ods. 2) avšak v odseku 3 prelamuje princíp ochrany osobných údajov v záujme informovania verejnosti napr. o verejnom funkcionárovi, odborníkovi plniacom úlohy pre člena vlády Slovenskej republiky a pod. Ministerstvo spravodlivosti SR nevidí spoločensky legitímny dôvod na to, aby dochádzalo k zrušeniu prelomenia ochrany osobných údajov len preto, že sa tieto osobné údaje nachádzajú v jednotnom informačnom systéme kybernetickej bezpečnosti. Dôvody (motívy) návrhu ustanovenia § 12 ods. 7 o špeciálnej úprave v oblasti bezpečnosti (nahlasovanie kybernetických bezpečnostných incidentov) sú podľa názoru Ministerstva spravodlivosti SR nepresvedčivé. Návrh ustanovenia § 12 ods. 7 je zároveň nepriamou novelizáciou zákona č. 211/2000 Z. z., ktorá je podľa čl. 9 ods. 1 Legislatívnych pravidiel vlády Slovenskej republiky neprípustná. | Z | A |  |
| **MSSR** | **§ 32 ods. 2, 4, 8 a 9** Požadujeme doplniť právnu úpravu tak, aby z nej bolo zrejmé, že ide o celkový ročný obrat za predchádzajúci účtovný rok poskytovateľa základnej služby, ktoré sa pokuta týka. Bez tohto doplnenia je právna norma neurčitá. | Z | A |  |
| **MSSR** | **K § 34 ods. 1**  Predkladateľ vylučuje aplikáciu správneho poriadku, pokiaľ navrhovaná právna úprava neurčuje inak. V tejto súvislosti požadujeme doplniť procesné ustanovenia (napr. doručovanie, plynutie lehôt a pod.), nakoľko tieto v dôsledku vylúčenia pôsobnosti správneho poriadku v návrhu zákona absentujú. Prípadne požadujeme aby predkladateľ v § 34 ods. 1 výslovne vylúčil aplikáciu konkrétnych ustanovení správneho poriadku, ktorých aplikácia nie je vzhľadom na predmet úpravy účelná. Upozorňujeme predkladateľa na to, že zvolený koncept vylúčenia všeobecnej právnej úpravy bez dopracovania osobitnej právnej úpravy spôsobí, že zákon v oblasti rozhodovania o právach a povinnostiach bude nevykonateľný. | Z | A |  |
| **MSSR** | **§ 33 písm. a) a e)** Predkladateľovi odporúčame vypustiť slovo „podrobnosti“ a primerane podľa tohto upraviť dikciu dotknutých ustanovení. Tak ako sú aktuálne koncipované splnomocňovacie ustanovenia, tak je zrejmé, že cieľom nie je úprava podrobností, ale úprava samotného technického, technologického a personálneho vybavenia v prípade § 33 písm. a); analogicky to platí aj pre § 33 písm. e). Túto pripomienku si síce neuplatňujeme ako zásadnú pripomienku, ale samotný legislatívny proces k vykonávacím predpisom si doslova pýta spochybnenie návrhu vykonávacieho predpisu z hľadiska čl. 123 Ústavy Slovenskej republiky a nevykonateľnosť zákona. | O | A |  |
| **MSSR** | **Príloha č. 1** V zákone nie je špecifikovaný zoznam použitých skratiek. Napr. pojem ,,VPA“ (Vecne príslušná autorita) podľa § 11 použitý v Prílohe č. 1 je potrebné uviesť v zozname skratiek. | O | A |  |
| **MSSR** | **§ 29 ods. 4** Za slová ,,Úrad vykoná kontrolu u“ odporúčame doplniť slová ,,poskytovateľa základných služieb a“. Odôvodnenie: Ide o doplnenie textu. Ministerstvo spravodlivosti Slovenskej republiky síce nespadá medzi povinné subjekty vymedzené v § 5 písm. c) , ale spadá pod Sektor 8, tab. 1 (prevádzkovatelia ISVS), a je prevádzkovateľom základných služieb (§ 3 písm. g)). Ak poskytovatelia základných služieb nie sú doteraz v odseku 4 uvedení, znamená to, že kontrola u nich môže byť vykonaná aj bez dôvodného podozrenia, alebo môže byť vykonávaná len v pravidelných intervaloch definovaných inými predpismi (t.j. nie v prípade incidentu). | O | N | Vaša pripomienka nebola akceptovaná, pretože uvedené ustanovenie bolo vypustené. Pripomienka bola nejednoznačná a text bol zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov, preto bol text preformulovaný, pričom vysvetlenie sa nachádza v dôvodovej správe. |
| **MSSR** | **§ 32 ods. 13** Za slovo „konanie“ požadujeme doplniť slová „o správnom delikte“; pripomienkou sa sleduje spresnenie a určitosť navrhovanej právnej normy. | O | A |  |
| **MSSR** | **K § 2 ods. 2 písm. c) a tabuľke zhody** Zásadne požadujeme aby predkladateľ v § 2 ods. 2 písm. c) normatívnym spôsobom vyjadril, ktoré konkrétne právne vzťahy nie sú týmto zákonom dotknuté, nakoľko použitá formulácia ,,osobitné predpisy“ spolu s odkazom na zákon č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákon č. 398/2015 Z. z. o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov nedávajú zmysel. Upozorňujeme na to, že v Slovenskej republike sú trestne zodpovedné aj fyzické osoby. Zmienka v poznámke pod čiarou v zákone o európskom ochrannom príkaze v trestných veciach nemá súvis s Čl. 1 ods. 4 smernice 2016/1148/EÚ. V Čl. 1 ods. 4 smernice 2016/1148/EÚ sú citované dva právne akty EÚ trestnoprávneho charakteru, ktoré majú za cieľ postihnúť špecifické formy trestnej činnosti, zákon o európskom ochrannom príkaze v trestných veciach nie je transpozičným predpisom vo vzťahu ani k jednému z týchto právnych aktov. Rovnako ani dôvodová správa nedáva odpoveď na to, čo chce vlastne predkladateľ takouto formuláciou vyjadriť. V tejto nadväznosti žiadame upraviť aj tabuľku zhody v časti k Čl. 1 ods. 4 smernice 2016/1148/EÚ, nakoľko uvádzané znenie našej právnej úpravy v tabuľke nekorešponduje so znením vlastného materiálu (napr. v tabuľke sa uvádza, že výsledkom transpozície je § 2 ods. 3, pričom z vlastného materiálu je zrejmé, že predmetný § 2 má len dva odseky a pod.). | Z | A |  |
| **MSSR** | **§ 31 a 32** Zásadne požadujeme doplniť do ustanovení upravujúcich pokuty dolnú hranicu pokuty. Koncept návrhu zákona umožňuje aj absurdný výklad, či postup kedy sa uloží pokuta vo výške 1 eura a pod. Zákony, ktoré neobsahujú dolnú hranicu pokuty vytvárajú priestor pre korupčné správanie sa adresátov právnych noriem. Preto doplnenie adekvátnych dolných hraníc pokút bude pôsobiť z tohto pohľadu pôsobiť preventívne. | Z | A | Upravené do požadovanej podoby. |
| **MSSR** | **§ 6 ods. 2** Zásadne žiadame vypustiť tretiu vetu spolu s odkazom na poznámku pod čiarou č. 11. Odôvodnenie:Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov obsahuje komplexnú úpravu povinne zverejňovaných zmlúv. Ustanovenie § 5a spolu s inými systematicky prepojenými ustanoveniami zákona tak tvorí prehľadnú, transparentnú a logicky uzavretú štruktúru právnej úpravy povinne zverejňovaných zmlúv. Ustanovenie § 5a ods. 5 obsahuje taxatívny a negatívny výpočet druhov (typov) zmlúv, ktoré nie sú povinne zverejňované. Okrem odseku 5 § 5a žiadna iná norma v právnom poriadku SR obsiahnutá mimo zákona č. 211/2000 Z. z. neobsahuje negatívny výpočet povinne zverejňovanej zmluvy. Navrhovaná tretia veta by spolu s odkazom na poznámku pod čiarou bola v právnom poriadku legislatívnym precedensom toho ako netransparentne dochádza k zúženiu ústavného práva občanov na informácie. Ústava Slovenskej republiky v čl. 26 garantuje každému slobodu prejavu a právo na informácie. Ak povinná osoba podľa zákona obmedzuje ústavné právo vyhľadávať a šíriť informácie, môže tak vykonať iba v súlade so zákonom a len ak ide o opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti. Okrem Ústavy Slovenskej republiky právo na informácie je garantované i ustanovením čl. 10 Dohovoru o ochrane ľudských práv a základných slobôd, podľa ktorého: „Každý má právo na slobodu prejavu. Toto právo zahŕňa slobodu zastávať názory a prijímať a rozširovať informácie alebo myšlienky bez zasahovania štátnych orgánov a bez ohľadu na hranice.“ Ministerstvo spravodlivosti SR nevidí spoločensky legitímny dôvod (napr. opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti), aby verejnosť nemohla spoznať obsah zmluvy s fyzickou osobou alebo právnickou osobou, ktorá by sa uzatvorila na účely zabezpečenia plnenia úloh podľa zákona o kybernetickej bezpečnosti. Zabezpečenie sietí a informačných systémov kybernetickou bezpečnosťou si vyžaduje nemalé verejné prostriedky vynakladané verejným sektorom a preto máme za to, že by zmluvné plnenia ako aj ich cena mala byť prístupná verejnosti. Dôvody (motívy) návrhu ustanovenia § 6 ods. 2 tretej vety nemožno bližšie zistiť ani z dôvodovej správy. Návrh ustanovenia § 6 ods. 2 tretej vety je zároveň nepriamou novelizáciou zákona č. 211/2000 Z. z., ktorá je podľa čl. 9 ods. 1 Legislatívnych pravidiel vlády Slovenskej republiky neprípustná. | Z | A |  |
| **MŠVVaŠSR** | **čl. I § 33** Navrhujeme - v materiály návrhu zákona uviesť v súlade s čl. 17 ods. 1 Legislatívnych pravidiel vlády znenie vykonávacieho predpisu, pretože z návrhu vyplýva, že vykonávací predpis nadobudne účinnosť spolu so zákonom, - úvodnú vetu formulovať štandardným spôsobom, - v písmene g) slovo "vymieňaní" nahradiť minimálne vo vzťahu k osobným údajom slovami "cezhraničnom prenose" alebo slovami "vzájomnom poskytovaní" v súlade s § 4 ods. 3 zákona č. 122/2013 Z. z. | O | A |  |
| **MŠVVaŠSR** | **čl. I § 10** Navrhujeme - výslovne uviesť, či bezpečnostné incidenty bude môcť nahlasovať CSIRT ľubovoľná osoba alebo poverený zamestnanec orgánu verejnej moci, - v odseku 7 formulovať poslednú vetu inak, pretože nie je zrejmé, čo všetko môže byť považované za verejný záujem vzhľadom na právne následky takéhoto zverejnenia. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že k prvej časti - systémové nastavenie CSIRTu dobrovoľné hlásenie fyzických osôb je upravené v texte zákona. K druhej časti - verejný záujem je záujem, ktorý prináša prospech všetkým alebo mnohým občanom, ide o "verejné blaho" formou ustanoveným zákonom resp. ústavou. |
| **MŠVVaŠSR** | **čl. II** navrhujeme v položke 276 sadzobníka doplniť na konci názvu položky slová "okrem jednotky CSIRT zriadených orgánmi verejnej moci", pretože nie je účelné, aby bola uvedená služba poskytovaná orgánom verejnej moci odplatne. | O | N | Orgány verejnej moci sú oslobodené od správnych poplatkov, uvedená veta by teda nebola v súlade s legislatívnymi pravidlami vlády. |
| **MŠVVaŠSR** | **čl. I § 2** Odporúčame - v odseku 1 v druhej vete za slovom "ustanovenia" vložiť slovo "tohto" z dôvodu spresnenia, - v odseku 2 písm. a) na konci vložiť chýbajúce slovo "skutočností". | O | A |  |
| **MŠVVaŠSR** | **čl. I § 9 ods. 2** Odporúčame - v písmene a) slovo "aktérov" nahradiť slovom "subjektov"; slovo "aktér" nie je terminologicky správne, - v súvislosti s určením vzdelávacích programov, programov na budovanie bezpečnostného povedomia , zvyšovanie informovanosti a odbornej prípravy podľa písmena f ) doplniť možnosť získania kvalifikácie na výkon špecializovanej činnosti s názvom „špecialista kybernetickej bezpečnosti“ na základe kvalifikačného a hodnotiaceho štandardu ustanoveného v karte kvalifikácii a na základe jeho zverejnenia v Národnej ústave kvalifikácií. | O | A |  |
| **MŠVVaŠSR** | **čl. I § 28** Odporúčame - v poznámke pod čiarou k odkazu 26 slovo "Ústavný/ písať s malým začiatočným písmenom v súlade s pokynom na citáciu právnych predpisov, - v odseku 2 číslo 10 nahradiť slovom v súlade s legislatívno-technickým pokynom na uvádzanie čísel. | O | A | Ustanovenie bolo vypustené. |
| **MŠVVaŠSR** | **prílohe č. 3** Odporúčame citovať v transpozičnej prílohe preberanú smernicu v súlade s Legislatívnymi pravidlami vlády SR. | O | A |  |
| **MŠVVaŠSR** | **čl. I § 3** Odporúčame doplniť definíciu pojmu „informačná bezpečnosť“, ktorý sa v zákone používa, podľa definície, ktorá sa nachádza v terminologickom slovníku krízového riadenia. Odôvodnenie: Zákon by sa mal vo svojich ustanoveniach zaoberať aj problematikou informačnej bezpečnosti ako jednej z oblastí, ktorá je súčasťou komplexnej oblasti kybernetickej bezpečnosti, pričom pri definícii pojmu sa musí vychádzať z trvale platných pojmov uvádzaných v terminologickom slovníku krízového riadenia. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná. Bol upravený celý § 3 a boli zavedené nové pojmy. |
| **MŠVVaŠSR** | **čl. III bodu 2** Odporúčame na konci novelizačného bodu doplniť chýbajúce úvodzovky. | O | A |  |
| **MŠVVaŠSR** | **čl. I § 6 ods. 1 písm. g)** Odporúčame na konci prvého bodu vložiť chýbajúcu čiarku. | O | A |  |
| **MŠVVaŠSR** | **čl. I § 13 ods. 4** Odporúčame nespisovné slovo "stanovenej" nahradiť slovom "určenej". | O | A |  |
| **MŠVVaŠSR** | **čl. I bodu 32** Odporúčame prehodnotiť výšku pokút, ktorá je príliš vysoká a môže mať nepriaznivý vplyv na chod orgánu verejnej moci. | O | A |  |
| **MŠVVaŠSR** | **čl. I § 22 ods. 3** Odporúčame slová "a kontroly" vypustiť ako nadbytočné, pretože pojem "štátna správa" zahŕňa automaticky aj oblasť kontroly. | O | A |  |
| **MŠVVaŠSR** | **čl. I § 30 ods. 1** Odporúčame spresniť pôsobnosť zákona č. 375/2015 Z. z. o finančnej kontrole a audite. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu vypustenia namietaného textu. |
| **MŠVVaŠSR** | **čl. I § 14 ods. 1** Odporúčame text v písmene d) začať slovesom, ako je zaužívané v legislatívnej praxe. | O | A |  |
| **MŠVVaŠSR** | **prílohe č. 1** Odporúčame uviesť označenie prílohy č. 1 v súlade s Legislatívnymi pravidlami vlády SR. | O | A |  |
| **MŠVVaŠSR** | **čl. V bodu 4** Odporúčame v § 4e ods. 4 slovo "Dopravy" uviesť s malým začiatočným písmenom. | O | A |  |
| **MŠVVaŠSR** | **čl. I § 18 ods. 2 a prechodné ustanovenia** Odporúčame v prechodných ustanoveniach návrhu zákona upraviť režim už uzatvorených zmlúv. | O | A |  |
| **MŠVVaŠSR** | **čl. I bodu 19 ods. 1** Odporúčame v prvej vete slovo "oblasti" vložiť za slovo "technickej". Ide o správny slovosled. | O | A |  |
| **MŠVVaŠSR** | **čl. I § 24 ods. 4 a § 25 ods. 3** Odporúčame v texte jednotlivých písmen jednotne uvádzať sloveso na prvom mieste, ako je zaužívaná legislatívna prax. | O | A | Vaša pripomienka bola akceptovaná a znenie bolo preformulované. |
| **MŠVVaŠSR** | **čl.I § 7** Odporúčame v zákone spresniť postavenie existujúceho národného CSIRT zriadeného Ministerstvom financií SR voči národnej jednotke CSIRT podľa návrhu zákona. Zo znenia § 7 ani z prechodných ustanovení nie je zrejmé, či ide o tú istú inštitúciu. | O | A | Vaša pripomienka bola akceptovaná. CSIRT Ministerstva financií je v pôsobnosti vecne príslušného subjektu. Vysvetlenie poskytuje aj dôvodová správa. |
| **MŠVVaŠSR** | **čl. I § 9 a prechodné ustanovenia** Odporúčame vymedziť postavenie Národnej stratégie kybernetickej bezpečnosti podľa § 9 návrhu zákona voči existujúcej koncepcii kybernetickej bezpečnosti a akčnému plánu vychádzajúceho z nej. | O | A | Vaša pripomienka bola akceptovaná a vysvetlená v dôvodovej správe. |
| **MŠVVaŠSR** | **čl. I § 17 ods. 1** Odporúčame za slovom "ktorý" vložiť chýbajúce slovo "je". | O | A |  |
| **MŠVVaŠSR** | **§ 12** Odporúčame - v odseku 4 za slovami "v tomto zákone" doplniť chýbajúcu čiarku, - v odseku 7 slová "osobitné predpisy" nahradiť slovami : "osobitný predpis"., pretože ide len o jeden predpis. | O | A |  |
| **MŠVVaŠSR** | **čl. I § 6 písm. l)** Žiadame jednoznačne definovať úlohy MŠVVaŠ SR v oblasti budovania bezpečnostného povedomia a vykonávania a zabezpečovania vzdelávania a zosúladiť ich v zmysle úloh vyplývajúcich pre MŠVVaŠ SR v tejto oblasti podľa akčného plánu pre kybernetickú bezpečnosť vychádzajúceho z aktuálnej koncepcie kybernetickej bezpečnosti. V tejto súvislosti na ilustráciu uvádzame, že budovanie bezpečnostného povedomia a vzdelávanie v rámci vysokého školstva musí rátať s autonómiou vysokých škôl, MŠVVaŠ SR nepredpisuje obsah vysokoškolského vzdelávania. Túto pripomienku považuje Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky za zásadnú. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že úlohy Ministerstva školstva, vedy, výskumu a športu SR sú zadefinované v príslušných predpisoch upravujúcich vzdelávanie, vedu a techniku, definujú vzdelávacie programy, princípy a ciele vzdelávania na Slovensku. Oblasť vzdelávania je teda konkretizovaná v príslušnej legislatíve a spolupráca s NBÚ bude prebiehať na základe doplnenia existujúceho vytvoreného systému vzdelávania a budovania povedomia na úrovni kybernetickej bezpečnosti. Po vysvetlení bol rozpor odstránený. |
| **MŠVVaŠSR** | **Všeobecne k celému materiálu** Žiadame predložený materiál návrhu zákona dôkladne prepracovať a doplniť s ohľadom na závery Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020 a z dôvodu potreby upraviť v zákone komplexné zabezpečenie informačnej bezpečnosti v rámci orgánov verejnej moci, nielen organizáciu a postavenie jednotiek CSIRT. Odôvodnenie: Materiál po obsahovej stránke nerieši kybernetickú zodpovednosť komplexne a zameriava sa hlavne na transpozíciu smernice Európskeho parlamentu a rady(EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov Únie. V sprievodných dokumentoch materiálu je uvedené , že je vypracovaný v súlade s Koncepciou kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020. Zámery tejto koncepcie sú z pohľadu MŠVVaŠ SR zapracované do návrhu zákona iba čiastkovo. V návrhu zákona napríklad absentuje definícia inštitucionálneho riadenia kybernetickej bezpečnosti, ktorý bol navrhnutý v uvedenej koncepcii. V návrhu zákona rovnako absentuje postavenie Výboru pre kybernetickú bezpečnosť ktorý je súčasťou Bezpečnostnej rady SR Vlády SR. Rovnako aj oblasť vzdelávania, vedy a výskumu v oblasti kybernetickej bezpečnosti je potrebné rozšíriť v zmysle záverov koncepcie. Túto pripomienku považuje Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky za zásadnú. | Z | A | Vaša pripomienka bola akceptovaná a zapracovaná a text návrhu zákona bol doplnený a zmenený v rámci cieľa uvedeného v pripomienke. |
| **MŠVVaŠSR** | **čl. I § 6 písm. m)** Žiadame spresniť kompetenciu NBÚ vykonávať výskum a vývoj, pretože ústredným orgánom štátnej správy pre výskum je MŠVVaŠ SR. Túto pripomienku považuje Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky za zásadnú. | Z | A | Vaša pripomienka bola akceptovaná. |
| **MŠVVaŠSR** | **čl. I § 29 ods. 6** Žiadame vypustiť slová "vrátane oprávnenia dočasne zmeniť hardvérovú alebo softvérovú konfiguráciu". Odôvodnenie: Výkon uvedeného oprávnenia predstavuje hrubé zasahovanie do vlastníckeho práva prevádzkovateľa. Túto pripomienku považuje Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky za zásadnú. | O | A |  |
| **MVSR** | **všeobecne** 1. Odporúčame zvážiť používanie pojmu „kybernetická bezpečnosť“ alebo používať pojem tak, ako je v názve smernice Európskeho parlamentu a Rady 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica NIS“). Cieľom smernice NIS je zvýšiť úroveň ochrany voči incidentom, rizikám a hrozbám v oblasti sieťovej a informačnej bezpečnosti, ale nie na podniky poskytujúce verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby, ktoré podliehajú osobitným požiadavkám. Naviac, názov a terminológia navrhovaného zákona nekorešponduje so smernicou NIS, keďže nikde v tejto smernici nie je spomenutá kybernetická bezpečnosť. Zbytočne sa vytvára problém s pojmom kybernetickej bezpečnosti, pretože v súčasnosti je veľa pojmov s predponou „cyber“. Nemá to logiku, lebo kybernetika = veda o riadení v živých organizáciách a strojoch (Wiener, Ashby, Ampér). Začína to byť zbytočne terminologický problém, pretože pojmy cyberspace a cybersecurity vznikli v USA, citujem: „Cybersecurity is the use of various technologies and processes to protect networks, computers, programs and data from attack, damage or unauthorized access. Since all computer systems rely on operating systems and networks to function, those areas are often targeted for attack and are the main sources of many security vulnerabilities. Information security involves protecting information from unauthorized access, use, disruption, modification or destruction, regardless of whether the information is stored electronically or physically. Cybersecurity is a subset of the larger area of information security.“. Zdroj: http://www.floridatechonline.com/resources/cybersecurity-information-assurance/cybersecurity-vs-information-security/#.VFfkXclaZBQ. | O | N | Vaša pripomienka nebola akceptovaná, pojmy predstavujú transpozíciu smernice a vychádzajú z platných štandardov upravujúcich oblasť KB a pojmov schválených v koncepcii. |
| **MVSR** | **čl. I** 10. V § 9 ods. 3 navrhujeme preformulovať slová „v požadovanom rozsahu“ napr. na „v potrebnom rozsahu“, keďže „v požadovanom rozsahu“ je príliš široký pojem a vytvára riziko svojvoľného určenia rozsahu informácie nad rámec nevyhnutnosti a z dôvodu vysokého stupňa centralizácie citlivých informácií predstavuje zbytočné bezpečnostné riziko. | O | A |  |
| **MVSR** | **čl. I** 11. V § 10 navrhujeme a) doplniť úpravu poskytovania informácií orgánom činným v trestnom konaní z jednotného informačného systému kybernetickej bezpečnosti, nakoľko nie je upravený prístup orgánov činných v trestnom konaní k údajom zo systému na účely trestného stíhania páchateľov počítačovej trestnej činnosti, ktorá priamo súvisí s týmto návrhom, b) v odseku 5 písm. h) užšie definovať partnerov Národnej jednotky CSIRT; vzhľadom na vysoké riziko spojené s priamym prístupom v elektronickej podobe v reálnom čase do neverejnej časti jednotného informačného systému kybernetickej bezpečnosti navrhujeme obmedziť možnosti prístupu len výslovným uvedením subjektov v navrhovanom zákone, c) v odseku 5 písm. j) vypustiť slová „iný subjekt na základe rozhodnutia úradu“ vzhľadom na vysoké riziko spojené s priamym prístupom v elektronickej podobe v reálnom čase do neverejnej časti jednotného informačného systému kybernetickej bezpečnosti navrhujeme obmedziť možnosti prístupu len výslovným uvedením subjektov v navrhovanom zákone, d) v odseku 6 doplniť vetu v znení: „Na tento účel úrad poskytne povinnému bezodplatne a bezodkladne všetky potrebné informácie o spôsoboch určených funkcionalitou jednotného informačného systému a zabezpečí ich dostupnosť.“, pretože na pripojenie funkcionality systému je nevyhnutne potrebné zabezpečiť aj súčinnosť správcu jednotného informačného systému. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že informácie z informačného systému budú slúžiť výlučne na účely uvedené v zákone. To samozrejme nevylučuje, aby informácie na vstupe poskytované prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb neboli zdieľané na požadované účely. Z uvedeného vyplýva, že informácie požadované orgánmi činnými v trestnom konaní budú k dispozícii priamo u oznamovateľa incidentu. Proces je zabezpečený v § 12, kde sa uvádza, že mlčanlivosť sa nevzťahuje pre prevádzkovateľa základných služieb a poskytovateľa digitálnych služieb v konaní aj pred orgánmi verejnej moci. Jednotný informačný systém kybernetickej bezpečnosti nie je referenčný register údajov, ale nástroj na riešenie kybernetických bezpečnostných incidentov a zabezpečenia kybernetickej bezpečnosti formou garantovania absolútnej dôvery. |
| **MVSR** | **čl. I** 12. V § 12 ods. 7 je potrebné vypustiť výnimku na spracúvanie osobných údajov vrátane poznámky pod čiarou k odkazu 18, pretože ochrana práv fyzických osôb pred neoprávneným zasahovaním do ich súkromného života pri spracúvaní ich osobných údajom musí byť zaručená, čo priamo vyplýva aj z čl. 2 smernice NIS. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že konštrukcia ochrany osobných údajov bola preformulovaná podľa požiadaviek nariadenia GDPR v súlade so smernicou NIS pri využití obmedzení podľa čl. 23 nariadenia GDPR. |
| **MVSR** | **čl. I** 13. Ustanovenia § 12 ods. 5 a 10 sa javia ako navzájom protichodné a nejasné, preto je potrebné ich preformulovať tak, aby poskytovali jasný a jednoznačný výklad o mlčanlivosti podľa zákona o kybernetickej bezpečnosti a mlčanlivosti podľa osobitných zákonov. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že odsek 5 hovorí o výnimke zo všeobecnej povinnosti zachovávať mlčanlivosť pre všetky subjekty, čo však podľa odseku 10 neznamená, že uvedené informácie nechráni na účely iných zákonov a nie na účely kybernetickej bezpečnosti. |
| **MVSR** | **čl. I** 14. V § 13 navrhujeme a) v odseku 1 doplniť text, že akreditácia sa vykonáva na základe žiadosti; odsek 2 sa odvoláva na žiadosť podľa odseku 1, pričom v odseku 1 žiadosť uvedená nie je, b) v odseku 4 sa nevymedzuje, čo musí žiadosť o akreditáciu obsahovať, aby bola považovaná za úplnú, pritom § 13 ods. 4 stanovuje postup v prípade, keď žiadosť je neúplná, považujeme za potrebné, aby zákon stanovil náležitosti samotnej žiadosti o akreditáciu, c) v odseku 5 by malo byť rozhodnutie o akreditácii vydané na dobu neurčitú, najmä pre orgány verejnej moci, z dôvodu zníženia administratívnej záťaže na opätovnú akreditáciu; neexistuje dôvod v prípade fungujúcich jednotiek ich opätovne akreditovať, keďže nefunkčnosť jednotiek je už riešená v § 15 ods. 4, d) odsek 10 navrhujeme vypustiť ako nadbytočný, pretože daná poplatková povinnosť vyplýva zo zákona o správnych poplatkov. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná. Neakceptovaná bola časť pripomienky o časovo neobmedzenej akreditácii. Akreditácia nepredstavuje administratívnu záťaž ale nevyhnutnú úlohu v systéme riadneho zabezpečenia kybernetickej bezpečnosti. |
| **MVSR** | **čl. I** 15. Zákon striktnými podmienkami v § 14 ods. 1 písm. b) až d) neprimerane limituje vznik jednotiek CSIRT (nad rámec potrieb vyplývajúcich z tohto zákona) a zároveň neupravuje kompetencie jednotiek CSIRT na úrovni sektora alebo podsektora. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že jednotky CSIRT v zmysle smernice NIS musia využívať infraštruktúru, ktorá je zabezpečená (príloha 1). Fyzická bezpečnosť a bezpečnosť prostredia je teda imanentnou súčasťou jednotky CSIRT, rovnako tak systém klasifikácie incidentov predpokladá existenciu utajovanej skutočnosti. Jednotka CSIRT predstavuje kanál dôvery a dôvera používateľov sa bez primeranej ochrany prostredia, v ktorom sa nachádzajú informácie, nedá budovať. K druhej časti pripomienky uvádzame, že jednotka CSIRT predstavuje tím expertov, ktorý odhaľuje bezpečnostné incidenty, koordinuje a kooperuje pri ich riešení a pôsobí preventívne proti vzniku ďalších hrozieb. CSIRT je expertný orgán, ktorý poskytuje svoje služby určitej zložke alebo skupine zložiek, na ktorých ochranu je zameraný. Vymedzovanie kompetencií je preto irelevantné, jednotka CSIRT poskytuje služby a tie sú v zákone jasne definované. |
| **MVSR** | **čl. I** 16. Povinnosti prevádzkovateľov základnej služby a poskytovateľov digitálnej služby v § 18 a § 21 sú nejednoznačne definované, preto ich navrhujeme zadefinovať konkrétnejšie a jednoznačnejšie; takéto formulácie môžu znížiť právnu istotu prevádzkovateľov základnej služby a poskytovateľov digitálnej služby. | O | A | Vaša pripomienka bola akceptovaná a text bol preformulovaný v zmysle Legislatívnych pravidiel vlády. |
| **MVSR** | **čl. I** 17. V § 29 žiadame vypustiť odsek 6. Doterajšie odseky 7 až 12 sa označia ako odseky 6 až 11. Odôvodnenie: Navrhované oprávnenia príslušníkov úradu sú neprimerane rozsiahle vzhľadom na účel, ktorý sa má dosiahnuť. | Z | A |  |
| **MVSR** | **čl. I** 18. V § 31 ods. 1 odporúčame vypustiť písmeno d), pretože za takéto konanie sa nemá ukladať pokuta za priestupok (navyše v neprimeranej výške do 5 000 eur), ale poriadková pokuta podľa § 29 ods. 9. | O | A |  |
| **MVSR** | **čl. III** 19. V súvislosti s navrhovaným zavedením osobného platu v zákone č. 73/1998 Z. z. je potrebné tento plat previazať so zákonom č. 328/2002 Z. z. sociálnom zabezpečení policajtov a vojakov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, ktorý osobný plat nepozná, pričom dávky sociálneho zabezpečenia a vymeriavací základ poistného sa viaže na služobný plat, resp. služobný príjem. | O | N | Text preformulovaný po vzájomnej konzultácii. |
| **MVSR** | **všeobecne** 2. Konkrétne subjekty, ktoré budú prevádzkovateľmi digitálnych služieb a základných služieb, budú určené až vykonávacou vyhláškou, ktorej návrh nie je súčasťou predloženého materiálu. Navrhujeme na účely bezproblémovej identifikácie subjektov, ktorých sa zákon týka, aby bol najskôr vytvorený zoznam základných služieb. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že do návrhu zákona bolo vložené nové ustanovenie identifikujúce prahové kritériá na určenie základnej služby, teda adresnosť predpisu je jednoznačnejšia. Došlo k úprave prílohy č. 1. Podrobnosti ustanoví vykonávací predpis. |
| **MVSR** | **čl. III** 20. V bode 2 § 101a ods. 2 je potrebné vypustiť slová „alebo na základe výsledku služobného hodnotenia za kalendárny rok“. Takéto znenie nie je v súlade so súčasnou platnou úpravou služobného hodnotenia podľa § 27 a nasl. zákona č. 73/1998 Z. z., ktorý nepozná služobné hodnotenie za kalendárny rok, ako ani jeho priame dôsledky v podobe zvýšenia, resp. zníženia platových náležitostí. | O | N | Text preformulovaný. |
| **MVSR** | **čl. IV** 21. V bode 6 § 7 ods. 4 písm. b) žiadame vypustiť druhý bod vrátane poznámky pod čiarou k odkazu 9e. Uvedená pripomienka priamo súvisí so zásadnou pripomienkou k čl. I § 2 ods. 3. | Z | A |  |
| **MVSR** | **čl. IV** 22. V bode 6 § 7 ods. 5 sa dávajú Ministerstvu obrany SR značne široké kompetencie a prevádzkovatelia prvkov kritickej infraštruktúry sú povinní poskytnúť tomuto ministerstvu široký rozsah informácií bez predošlého definovania, o aké informácie by malo ísť. Výklad tohto ustanovenia splnomocňuje ministerstvo žiadať takmer akékoľvek informácie, preto je potrebné vyšpecifikovať konkrétny rozsah požadovaných informácií. | O | A | Preformulovaný celý čl. IV v zmysle doručených pripomienok. |
| **MVSR** | **čl. VIII** 23. V čl. VIII žiadame na začiatok vložiť nový prvý bod, ktorý znie: „1. V § 1 sa vypúšťa odsek 2. Doterajšie body 1 až 4 sa označujú ako body 2 až 5.“. Odôvodnenie: Navrhujeme odstrániť neprípustnú a nežiaducu nepriamu novelu zákona č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov. | Z | A | Po vysvetlení rozpor odstránený. |
| **MVSR** | **čl. VIII** 24. V čl. VIII žiadame vložiť nový tretí bod, ktorý znie: „3. V § 9 sa vypúšťa odsek 4.“ Doterajšie body 3 až 5 sa označujú ako body 4 až 6.“. Odôvodnenie: Navrhujeme vypustiť predmetné ustanovenie, pretože nespĺňa náležitosti splnomocnenia na vydanie všeobecne záväzného právneho predpisu a je nevykonateľné z dôvodu, že nemožno všeobecne záväzným právnym predpisom nižšej právnej sily nahrádzať zákonnú úpravu. Ak bude potrebné na základe aplikačnej praxe zaviesť pravidlá na poskytovanie finančného príspevku subjektom na plnenie povinností súvisiacich s vykonaním bezpečnostných opatrení na ochranu prvku kritickej infraštruktúry, takáto právnu úprava bude zavedená zákonom. Predmetné ustanovenie sa navrhuje vypustiť aj z dôvodu, že umožňuje použiť rozdielne pravidlá pri poskytovaní finančného príspevku právnickým osobám a príslušným ústredným orgánom štátnej správy. | Z | A | Po vysvetlení rozpor odstránený. |
| **MVSR** | **čl. VIII** 25. V bode 4 prílohe č. 3 žiadame nahradiť sektory 2 a 4 novým sektorom takto: „Sektor: Informačno-komunikačné technológie Podsektor: elektronické komunikácie, internet, siete a informačné systémy“ s príslušnou zodpovednosťou ústredných orgánov podľa kompetenčného zákona. Odôvodnenie: Pretože sektor informačno-komunikačné technológie a elektronické komunikácie je to isté, navrhujeme vytvoriť jeden sektor s označením Informačno-komunikačné technológie, pretože legislatíva Slovenskej republiky o IKT bezpečnosti je aplikovateľná na „cyber“ bezpečnosť. Čiže táto problematika patrí do IKT infraštruktúry aj kompetenčne. Ale nemôže byť samostatný sektor označený ako „kybernetický priestor“. | Z | N | Po vysvetlení rozpor odstránený. |
| **MVSR** | **všeobecne** 3. V návrhu zákona nie je upravená spolupráca s orgánmi činnými v trestnom konaní pri stíhaní páchateľov počítačovej trestnej činnosti, ktorá priamo súvisí s týmto návrhom, absentuje riešenie vzťahu s trestným konaním a zabezpečovaním dôkazov. | O | A |  |
| **MVSR** | **všeobecne** 4. V predkladanom návrhu sa navrhované kompetencie pre Ministerstvo obrany SR v osobitných článkoch môžu prekrývať a kolidovať napr. s kompetenciami navrhovanými pre úrad v oblasti kybernetickej bezpečnosti, súčasnými kompetenciami súdov Slovenskej republiky a Policajného zboru a zároveň môžu navrhované legislatívne zmeny umožniť zásahy do súkromia občanov Slovenskej republiky v rozsahu, ktoré by boli v čase mieru v demokratickom štáte minimálne diskutabilné. Taktiež považujeme za potrebné vysporiadať sa so vzájomným vzťahom zákona o kybernetickej bezpečnosti k zákonu o ochrane osobných údajov (v súčasnosti sa pripravuje úplne nový zákon). | O | A |  |
| **MVSR** | **čl. I** 5. Znenie čl. I odporúčame legislatívno-technicky upraviť, napr.: a) v § 2 ods. 1 slová „môžu sa použiť“ nahradiť slovami „použijú sa“, b) v § 2 ods. 2 písm. a) na konci pripojiť slovo „skutočností“, c) v § 5 ods. 3 slovo „autority“ nahradiť napr. slovami „štátne orgány“, d) v § 5 ods. 3 vypustiť prvý bod, keďže úrad už je uvedený v písmene b), e) v § 6 ods. 1 písm. p) slovo „vedie“ nahradiť slovom „spravuje“ alebo „prevádzkuje“, f) v § 11 ods. 1 písm. g) vypustiť slovo „vykonávanie“, g) v § 17 od. 1 slovo „ktorým“ vložiť slovo „je“, h) v § 21 ods. 5 za slovami „digitálne služby“ vypustiť slovo „je“, i) v § 32 ods. 8 slová „finančná pomoc poskytnutá“ nahradiť slovami „poskytnutá finančná pomoc“, j) doplniť odkazy na osobitné predpisy v poznámkach pod čiarou [§ 11 ods. 1 písm. g), § 17 ods. 1, § 19 ods. 1, § 24 ods. 1, § 25 ods. 1, § 28 ods. 9 písm. c), § 35 ods. 2]. | O | A | Vaša pripomienka bola čiastočne akceptovaná a zapracovaná, upravené v zmysle LPV. |
| **MVSR** | **čl. I** 6. § 2 žiadame doplniť odsekom 3, ktorý znie: „(3) Tento zákon sa nevzťahuje na ochranu prvkov kritickej infraštruktúry.5)“. Poznámka k odkazu 5 znie: „5) Zákon č. 45/2011 Z. z. o kritickej infraštruktúre.“. Odôvodnenie: Smernica NIS, ktorá sa transponuje predmetným zákonom výslovne v čl. 1 ods. 4 uvádza, že uplatňovaním tejto smernice nie je dotknutá smernica Rady 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu. Z navrhovaných „základných“ služieb Ministerstvo vnútra SR už gestoruje „kritické“ služby a kritickú infraštruktúru vrátane väčšiny uvedených sektorov podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre. Právnu úpravu daných skutočností, ako na úrovni EÚ, tak aj na našej národnej úrovni, považujeme za dostatočnú. Subjekty s informačnými systémami kritickej infraštruktúry spĺňajú prísne požiadavky súvisiace s bezpečnosťou, spoľahlivosťou, zálohovaním dát, back-up systémami a pod. Podriadiť tieto subjekty ďalším, zdvojeným požiadavkám a kontrole, resp. dohľadu vykonávanom ďalšími inštitúciami než sú v súčasnosti, považujeme za neprimerané. Toto odvetvie je prísne regulované. Vzhľadom na vyššie uvedené skutočnosti žiadame o vypustenie akejkoľvek zmienky o kritickej infraštruktúre z predmetného zákona. | Z | A | Po vysvetlení rozpor odstránený. |
| **MVSR** | **čl. I** 7. V § 3 absentuje mnoho definícií, ktoré sú následne v texte zákona používané, ako napr. aktivovaný prvok kybernetického priestoru a politika správania sa v kybernetickom priestore. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že bol upravený celý § 3 a boli zavedené nové pojmy. |
| **MVSR** | **čl. I** 8. V § 3 písm. a) žiadame vypustiť slová „informačný systém v sektore kritickej infraštruktúry“, ako aj poznámku pod čiarou k odkazu 7. Uvedená pripomienka priamo súvisí so zásadnou pripomienkou k § 2 ods. 3. | Z | A | Po vysvetlení rozpor odstránený. |
| **MVSR** | **čl. I** 9. Navrhujeme v § 6 ods. 2 doplniť obligatórnu písomnú formu dohody a vypustiť poslednú vetu vrátane poznámky pod čiarou k odkazu 11; nezverejňovaním zmluvy sa vytvára priestor pre netransparentnosť. | O | A |  |
| **MZSR** | **K § 29 ods. 6** Považujeme za neprijateľné, aby príslušníci úradu mali oprávnenie vstupovať do Národného zdravotníckeho informačného systému, ktorý obsahuje zdravotné záznamy obyvateľstva a zároveň nie je možné akceptovať ustanovenie oprávnenia dočasne zmeniť hardvérovú alebo softvérovú konfiguráciu. Odôvodnenie: Vzhľadom na to, že zdravotné záznamy obyvateľstva sú osobitnou kategóriou osobných údajov so zvýšeným stupňom ochrany pri ich spracúvaní, vstup príslušníkov úradu do Národného zdravotníckeho informačného systému a oprávnenie dočasnej zmeny hardvérovej alebo softvérovej konfigurácie má potenciál narušiť dôveru obyvateľstva v celý systém fungovania Národného zdravotníckeho informačného systému. Túto pripomienku považujte za zásadnú. | Z | A | Vaša pripomienka bola akceptovaná a zapracovaná, text upravujúci kontrolu bol vypustený a nahradený novým textom, ktorý neobsahuje napádané ustanovenie. |
| **MZSR** | **K doložke vybraných vplyvov** Z doložky vybraných vplyvov vyplýva, že materiál bude mať negatívny vplyv na rozpočet verejnej správy, ktorý bude rozpočtovo čiastočne zabezpečený. Súčasne je v časti 2. 1. 1. Financovanie návrhu uvedené, že finančné prostriedky vyplývajúce z návrhu zákona budú zabezpečené v rámci schválených limitov rozpočtu v jednotlivých rokoch bez dodatočných požiadaviek na rozpočet. S tvrdením v doložke vybraných vplyvov k návrhu zákona nesúhlasíme. Ministerstvo zdravotníctva Slovenskej republiky pri návrhu rozpočtu na roky 2018 až 2020 nepredpokladalo zvýšené nároky na rozpočet v súvislosti s prijatím zákona o kybernetickej bezpečnosti. Z prideleného rozpočtu na roky 2018 až 2020 nie je možné uvedenú problematiku zabezpečiť. Na základe vyššie uvedeného považujeme za dôležité vyčísliť náklady za rezort zdravotníctva a za nevyhnutné navýšenie finančných zdrojov pre kapitolu zdravotníctva v súvislosti v prijatím zákona o kybernetickej bezpečnosti. Túto pripomienku považujte za zásadnú. | Z | A |  |
| **MZVaEZSR** | **§ 10** § 10 navrhujeme doplniť novým odsekom, ktorý znie takto: „Úrad poskytne bezodplatne povinným subjektom všetky súčasti potrebné na pripojenie do jednotného systému správy kybernetického priestoru.“. Odôvodnenie: Keďže povinné subjekty sú prevažne orgány verejnej moci považujeme za praktické zaťažiť štátny rozpočet jednorazovo prostredníctvom úradu, bez potreby požiadavky jednotlivých subjektov na navýšenie finančných prostriedkov zo štátneho rozpočtu. Túto pripomienku považujeme za zásadnú. | Z | A |  |
| **MZVaEZSR** | **§ 8** § 8 navrhujeme preformulovať takto: „(1) Úrad je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami iných členských štátov Európskej únie a Organizácie severoatlantickej zmluvy, poskytuje im potrebné informácie, plní notifikačné a reportingové povinnosti voči príslušným orgánom Európskej únie a Organizácie severoatlantickej zmluvy a na účely zabezpečenia kybernetickej bezpečnosti spolupracuje s jednotkami CSIRT a obdobnými orgánmi a inštitúciami iných štátov. Úrad rozvíja medzinárodnú spoluprácu v súčinnosti s ministerstvom zahraničných vecí v rozsahu podľa § 6 ods.1, písm. f). (2) Ministerstvo zahraničných vecí a) zodpovedá za plnenie úloh v oblasti kybernetickej diplomacie zameranej na presadzovanie zahraničnopolitických záujmov SR a partnerov v rámci Európskej únie a Organizácie severoatlantickej zmluvy v kybernetickom priestore, b) zastupuje Slovenskú republiku pri formovaní a presadzovaní medzinárodných zámerov súvisiacich s bezpečnosťou kybernetického priestoru v súlade so Spoločnou bezpečnostnou a obrannou politikou EÚ, zastupuje Slovenskú republiku v politickom dialógu s medzinárodnými partnermi a medzinárodnými organizáciami ako Rada Európy, Organizácia spojených národov, Organizácia pre bezpečnosť a spoluprácu v Európe, Organizácia pre ekonomickú spoluprácu a rozvoj a prispieva k predchádzaniu konfliktom, k zmierňovaniu hrozieb v oblasti kybernetickej bezpečnosti, c) priebežne analyzuje medzinárodnú bezpečnostnú situáciu z pohľadu možnosti jej prejavov a hrozieb v kybernetickom priestore.“. Odôvodnenie: Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky je podľa § 14 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a ústredných orgánov štátnej správy v znení neskorších predpisov ústredným orgánom štátnej správy pre oblasť zahraničnej politiky a vzťahy Slovenskej republiky k ostatným štátom, medzinárodným organizáciám a zoskupeniam a európskym inštitúciám a vykonáva pôsobnosť v oblasti určovania a presadzovania politiky Slovenskej republiky a jej záujmov v zahraničnopolitickej oblasti, rozvoja medzinárodnej spolupráce, ako aj sledovania dopadov vývoja v zahraničnopolitickej oblasti na záujmy Slovenskej republiky a jej najbližších partnerov, a to aj v oblasti kybernetickej bezpečnosti. Túto pripomienku považujeme za zásadnú. | Z | ČA | Vaša pripomienka bola čiastočne akceptovaná. Text 8 bol vypustený a zaradený medzi úlohy úradu z dôvodu duplicitnej úlohy v zákone na účely konkrétnej definície stanovených opatrení v oblasti medzinárodných vzťahov a spolupráce. Záver: Rozpor bol odstránený. |
| **MZVaEZSR** | **§ 28 ods. 6** Navrhujeme na konci vety pripojiť slová „a vecne príslušný štátny orgán.“. Odôvodnenie: Pri vzniku stavu kybernetického ohrozenia je nevyhnutne potrebné zabezpečiť vzájomnú informovanosť z dôvodu efektívnej koordinácie aktivít. Túto pripomienku považujeme za zásadnú. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Text bol preformulovaný. Záver: Rozpor bol odstránený. |
| **MZVaEZSR** | **§ 5 písm. c)** Navrhujeme rozšíriť zoznam vecne príslušných štátnych orgánov, ktoré vykonávajú pôsobnosť v oblasti kybernetickej bezpečnosti o Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky. Odporúčame zaviesť legislatívnu skratku „Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky (ďalej len „ministerstvo zahraničných vecí“)“. Taktiež navrhujeme v Prílohe č. 1 v tabuľke bod 8. Verejná správa do tretieho stĺpca tretieho riadku doplniť text „správcovia a prevádzkovatelia vybraných medzinárodných bezpečnostných systémov“ a do štvrtého stĺpca doplniť text „ministerstvo zahraničných vecí“. Odôvodnenie: Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky je podľa § 14 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a ústredných orgánov štátnej správy v znení neskorších predpisov ústredným orgánom štátnej správy pre oblasť zahraničnej politiky a vzťahy Slovenskej republiky k ostatným štátom, medzinárodným organizáciám a zoskupeniam a európskym inštitúciám a vykonáva pôsobnosť v oblasti určovania a presadzovania politiky Slovenskej republiky a jej záujmov v zahraničnopolitickej oblasti, rozvoja medzinárodnej spolupráce, ako aj sledovania dopadov vývoja v zahraničnopolitickej oblasti na záujmy Slovenskej republiky a jej najbližších partnerov, a to aj v oblasti kybernetickej bezpečnosti. Zoznam vecne príslušných štátnych orgánov vychádza z klasického chápania kritickej infraštruktúry (na účely návrhu zákona o kybernetickej bezpečnosti mierne doplneného) v zmysle úlohy štátu zabezpečiť v krízových situáciách pre svojich občanov vybrané nevyhnutne potrebné služby, implicitne na území štátu. V súčasnosti značný počet občanov Slovenskej republiky sa priebežne fyzicky zdržiava mimo územia Slovenskej republiky. Aj týchto občanov sa môžu dotknúť krízové situácie, a to nielen tie, ktoré vznikli na území Slovenskej republiky. Je preto žiaduce klasické chápanie kritickej infraštruktúry rozšíriť o zabezpečenie vybraných nevyhnutne potrebných služieb štátu aj pre občanov dočasne sa zdržujúcich mimo územia štátu, resp. rodiny ktorých časť príslušníkov sa dočasne zdržiava mimo územia štátu (sektor vybraných služieb poskytovaných občanom v zahraničí) a adekvátne upraviť (rozšíriť) Prílohu č. 1 návrhu zákona o kybernetickej bezpečnosti a zaradiť Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky medzi vecne príslušné štátne orgány (§5 písm. c) návrhu zákona o kybernetickej bezpečnosti. Okrem vyššie uvedeného je Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky zodpovedné za správu a prevádzku medzinárodných informačných systémov bezpečnostného charakteru. Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky je presvedčené o potrebe jeho zaradenia v predkladanom návrhu zákona medzi vecne príslušné štátne orgány, ktoré vykonávajú pôsobnosť v oblasti kybernetickej bezpečnosti. Túto pripomienku považujeme za zásadnú. | Z | N | Pripomienku v navrhovanej podobe nie je možné akceptovať. Úrad však v rámci rozporových konaní a žiadostí jednotlivých subjektov zaradil do zoznamu orgánov verejnej moci na úseku kybernetickej bezpečnosti ministerstvá a ostatné orgány štátnej správy. Tieto orgány majú významné postavenie v zabezpečovaní úloh kybernetickej bezpečnosti na IS, ktoré má v pôsobnosti, avšak na tieto orgány nie sú kladené náročné informačné, technické a finančné požiadavky ako je to pri subjektoch, ktoré sú „VPA“. Tieto subjekty aplikujú primerané bezpečnostné opatrenia uvádzané v zákone o kybernetickej bezpečnosti, spolupracujú s úradom a inými orgánmi, majú zodpovednosť za svoje IS. S poukazom na ustanovenie § 4 dávame teda do pozornosti rozdiel medzi ústredným orgánom (predtým „VPA“) (§ 4 písm. b)) a ďalším orgánom štátnej správy v rozsahu svojej pôsobnosti (§ 4 písm. c). Ústredný orgánu je prirodzený regulátor v oblasti svojej pôsobnosti (napríklad pre sektor „Doprava“ ministerstvo dopravy a výstavby SR, pre sektor „bankovníctvo“ ministerstvo financií SR, atď.), ďalej je to aj subjekt, ktorého úlohy v oblasti kybernetickej bezpečnosti vyplývajú priamo z právnych predpisov upravujúcich jeho pôsobnosť napr. SIS, VOS – MOSR, NBÚ. Na druhej strane existujú aj ďalšie subjekty (ako napr. ministerstvo zahraničných vecí a európskych záležitostí SR) s osobitným postavením na úseku kybernetickej bezpečnosti, ktoré majú povinnosť starať sa o svoje IS, avšak zaradenie každého takéhoto subjektu medzi ústredné orgány (VPA) by však narušilo dlho deklarovaný a schválený koncept „VPA“. Ak by došlo k Vami navrhovanej úprave, znamenalo by to okrem akceptácie pripomienok vo Vašej podobe aj iným subjektom a následne povinné a regulované zriadenie jednotiek CSIRT a ústredných orgánov naprieč celému spektru subjektov verejnej správy, čo by značne ovplyvnilo celú dlhodobo avizovanú logiku zákona o kybernetickej bezpečnosti. Z uvedeného dôvodu preto došlo po vyhodnotení ďalších zásadných pripomienok pripomienkujúcich subjektov ku kompromisnej úprave ustanovenia § 4 (pôvodného § 5) a to tak že sa doplnilo písmenom c), o ďalšie orgány štátnej správy v rozsahu svojej pôsobnosti. Záver: Úrad považuje rozpor za odstránený. |
| **MZVaEZSR** | **§ 6 ods. 1 písm. e)** Navrhujeme vypustiť slová „úlohy vyplývajúce z medzinárodných zmlúv, reprezentuje Slovenskú republiku na medzinárodnej úrovni“. Odôvodnenie: V záujme zabezpečenia efektívneho presadzovania politík a zamedzenia duplicít v širšom kontexte presadzovania politických a ekonomických záujmov Európskej únie úlohy v oblasti kybernetickej bezpečnosti patria do kompetencie Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky. Túto pripomienku považujeme za zásadnú. | Z | A |  |
| **MZVaEZSR** | **§ 3** Odporúčame doplniť vymedzenie pojmu „citlivá informácia“. Odôvodnenie: Pojem citlivá informácia nie je definovaný v právnom poriadku Slovenskej republiky a to aj napriek potrebám aplikačnej praxe kategorizovať informácie, ktoré nie je potrebné chrániť v zmysle zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností, ale nie je žiaduce, aby boli verejnosti sprístupnené v súlade so zákonom č. 211/2000 Z. z. o slobodnom prístupe k informáciám. Ako príklad si dovoľujeme uviesť komplexnú dokumentáciu k informačnému systému, ktorej zverejnenie by mohlo viesť ku kybernetickému útoku s rozsiahlymi následkami. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že bol upravený celý § 3 a boli zavedené nové pojmy. |
| **MZVaEZSR** | **§ 4 ods. 2** Odporúčame druhú vetu preformulovať takto: „Do základných práv a slobôd možno zasiahnuť len v miere nevyhnutnej na vykonanie opatrení na ochranu kybernetického priestoru podľa tohto zákona alebo osobitného predpisu.“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **MZVaEZSR** | **§ 2 ods. 1** Odporúčame nahradiť slová „môžu sa použiť ustanovenia osobitného predpisu“ slovami „použijú sa ustanovenia osobitného predpisu“. Odôvodnenie: vychádzame z toho, že pokiaľ osobitný predpis ustanovuje prísnejšie požiadavky na zabezpečenie sietí a informačných systémov, musia byť tieto požiadavky splnené. V prípade ak ide len o špeciálne úpravy považujeme za vhodnú možnosť ustanovenie týkajúce sa prednosti vypustiť úplne a len v dôvodovej správe osobitnej časti odkázať na interpretačné pravidlo lex specialis derogat legi generali. | O | A |  |
| **MZVaEZSR** | **§ 14 ods. 1 písm. d)** Odporúčame nahradiť slovo „dokumentáciu“ slovom „dokumentácia“ a slová „v zabezpečenom priestore“ nahradiť slovami „v chránenom priestore“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že textácia je v súlade so smernicou NIS. |
| **MZVaEZSR** | **predkladacej správe** Odporúčame nahradiť slovo „poníma“ slovom „upravuje“. | O | A |  |
| **MZVaEZSR** | **§ 13 ods. 3** Odporúčame nahradiť slovo „požiadaviek“ slovom „povinností“. Zosúladenie s § 15. | O | A | Vaša pripomienka bola akceptovaná a zapracovaná. |
| **MZVaEZSR** | **§ 13 ods. 1** Odporúčame preformulovať. Napríklad takto: „Jednotky CSIRT akredituje úrad na základe žiadosti po splnení podmienok podľa § 14 a všeobecne záväzných právnych predpisov vydaných na vykonanie tohto zákona.“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ide o legislatívno-technickú úpravu, ktorú úrad navrhuje a je v podmienkach úradu zaužívaná. |
| **MZVaEZSR** | **§ 13 ods. 2** Odporúčame prehodnotiť použitie vnútorného odkazu, nakoľko v predloženom návrhu § 13 ods. 1 neustanovuje nič o žiadosti. | O | A | Vaša pripomienka bola akceptovaná a znenie bolo preformulované. |
| **MZVaEZSR** | **§ 13 ods. 5** Odporúčame prvú vetu preformulovať takto: „Úrad akredituje jednotku CSIRT do 90 dní od začiatku konania.“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že lehota 90 dní je určená na vydanie rozhodnutia. Akreditáciu v prípade nesplnenia podmienok úrad udeliť nemôže. |
| **MZVaEZSR** | **§ 4 ods. 1** Odporúčame slová „a koordinácie“ nahradiť slovami „a ich vzájomnej koordinácie“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **MZVaEZSR** | **predkladacej správe** Odporúčame slová „dostatočnej transpozície“ nahradiť slovami „úplnej transpozície“ z dôvodu súladu s doložkou zlučiteľnosti právneho predpisu s právom Európskej únie. | O | A |  |
| **MZVaEZSR** | **dôvodovej správe všeobecnej časti** Odporúčame slová „predpismi Európskej únie“ nahradiť slovami „právom Európskej únie“. Táto pripomienka sa týka aj predkladacej správy. | O | A |  |
| **MZVaEZSR** | **§ 6 ods. 1 písm. i)** Odporúčame slová „priestupok a správny delikt“ nahradiť slovami „priestupok alebo iný správny delikt“. | O | A |  |
| **MZVaEZSR** | **§ 6 ods. 1 písm. i)** Odporúčame slová „rozhodnutia o uložení opatrení“ nahradiť slovami „rozhodnutie o uložení opatrenia“. Taktiež odporúčame slovo „pokuty“ nahradiť slovom „pokutu“. | O | A |  |
| **MZVaEZSR** | **§ 32 ods. 7** Odporúčame slová „uvedených v odsekoch“ nahradiť slovami „uvedených alebo vypočítaných podľa odsekov“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu legislatívnej techniky. |
| **MZVaEZSR** | **§ 5 písm. c)** Odporúčame slovo „autority“ nahradiť slovami „štátne orgány“. Táto pripomienka sa týka celého textu návrhu zákona vrátane sprievodných dokumentov. V prípade ak sa v zmysle návrhu pojem „vecne príslušná autorita“ má vzťahovať aj na subjekty, ktoré nemôžeme označiť za štátne orgány, odporúčame zadefinovať tento pojem v § 3. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol upravený a slovo "autorita" bolo nahradené slovom "subjekt". |
| **MZVaEZSR** | **§ 6 ods. 1 písm. p)** Odporúčame slovo „vedie“ nahradiť slovami „spravuje a prevádzkuje“. | O | A |  |
| **MZVaEZSR** | **§ 17 ods. 1** Odporúčame v poslednej vete za slovo „ktorým“ vložiť slovo „je“. | O | A | Vaša pripomienka bola akceptovaná a zapracovaná. |
| **MZVaEZSR** | **§ 5 písm. c)** Odporúčame vypustiť bod 1., vzhľadom na skutočnosť, že je totožný s ustanovením § 5 písm. b). Ak je potrebné zadefinovať úrad osobitne ako VPA, odporúčame tak urobiť v § 6 novým písmenom a). | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že úrad vystupuje aj ako vecne príslušný subjekt aj ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť a na základe toho má teda dve oddelené úlohy. |
| **MZVaEZSR** | **§ 10 ods. 5** Odporúčame vypustiť písmeno i). Ide o duplicitné uvedenie Ministerstva obrany Slovenskej republiky, ktoré je v návrhu zákona definovaná ako vecne príslušný štátny orgán. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že v tomto prípade je dôležitý osobitný účel. |
| **MZVaEZSR** | **§ 6 ods. 1 písm. b)** Odporúčame vypustiť slová: „a záväznú politiku správania sa v kybernetickom priestore,“. Odôvodnenie: Ministerstvu zahraničných vecí a európskych záležitostí Slovenskej republiky nie je jasná potreba takejto politiky. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že existuje potreba zabezpečiť bezpečné kybernetické prostredie v akomkoľvek okamihu. Vysvetľuje to aj dôvodová správa. |
| **MZVaEZSR** | **§ 32 ods. 13** Odporúčame za slová „Na konanie“ vložiť slová „podľa odsekov 1 až 12“. | O | A |  |
| **MZVaEZSR** | **§ 4 ods. 1** Odporúčame za slovo „bezpečnostné“ vložiť slovo „záujmy“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **MZVaEZSR** | **§ 2 ods. 2 písm. a)** Odporúčame za slovo „utajovaných“ vložiť slovo „skutočností“. | O | A |  |
| **MZVaEZSR** | **K § 4 ods. 1** Odporúčame za slovo „verejného“ vložiť slovo „sektora“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **MZVaEZSR** | **§ 9 ods. 2 písm. b)** Odporúčame za slovo „verejným“ vložiť slovo „sektorom“. | O | A |  |
| **MZVaEZSR** | **§ 6 ods. 1 písm. d)** V odseku 1 navrhujeme upraviť znenie písmena d) takto: „d) v spolupráci s príslušnými štátnymi orgánmi vypracúva národnú stratégiu kybernetickej bezpečnosti,“. Povinnosť úradu vypracovať a predložiť ročnú správu o stave kybernetickej bezpečnosti v Slovenskej republike navrhujeme upraviť v samostatnom písmene. Odôvodnenie: Účasť príslušných štátnych orgánov na tomto procese je žiaduca vzhľadom na účely zohľadnenia špecifickej expertízy jednotlivých orgánov. Účasť ministerstva zahraničných vecí na tomto procese je nevyhnutná taktiež preto, že národná stratégia kybernetickej bezpečnosti komplexne určí strategický prístup štátu k zabezpečeniu kybernetickej bezpečnosti, a to aj v zahraničnopolitickej oblasti. Túto pripomienku považujeme za zásadnú. | Z | A |  |
| **MZVaEZSR** | **§ 6 ods. 1** V odseku 1 navrhujeme za písmeno e) vložiť nové písmeno f), ktoré znie: „f) v spolupráci s ministerstvom zahraničných vecí rozvíja medzinárodnú spoluprácu a sleduje dopady aktivít v oblasti kybernetickej bezpečnosti na zahraničnopolitické záujmy Slovenskej republiky a partnerov v rámci Európskej únie a Organizácie severoatlantickej zmluvy,“. Odôvodnenie: Vzhľadom na kompetencie vymedzené v § 14 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a ústredných orgánov štátnej správy v znení neskorších predpisov Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky sleduje dopady vývoja v zahraničnopolitickej oblasti na záujmy Slovenskej republiky a jej najbližších partnerov, a to aj v oblasti kybernetickej bezpečnosti, a preto považujeme za nevyhnutné zaradenie Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky medzi vecne príslušné štátne orgány, ktoré vykonávajú pôsobnosť v oblasti kybernetickej bezpečnosti. Túto pripomienku považujeme za zásadnú. | Z | A |  |
| **MZVaEZSR** | **dôvodovej správe všeobecnej časti** V odseku 1 odporúčame nahradiť slová „národného právneho poriadku“ slovami „právneho poriadku Slovenskej republiky“. Táto pripomienka sa týka aj predkladacej správy. | O | A |  |
| **MZVaEZSR** | **§ 9 ods. 2** V odseku 2 navrhujeme za písmeno d) vložiť nové písmeno e), ktoré znie: „e) určenie hlavných zahraničnopolitických partnerov,“. Odôvodnenie: Špecifikácia obsahu národnej stratégie kybernetickej bezpečnosti v § 9 bod 2 neobsahuje charakteristiku zahraničnopolitického rozmeru aktivít v oblasti kybernetickej bezpečnosti (určenie hlavných partnerov), preto navrhujeme jeho doplnenie o uvedený rozmer. Túto pripomienku považujeme za zásadnú. | Z | A |  |
| **MZVaEZSR** | **§ 28 ods. 1** Z dôvodu jednoznačnosti textu odporúčame pred slová „bezpečnostnej hrozby“ vložiť slovo „vzniku“. | O | A | Vaša pripomienka bola akceptovaná. Ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **MŽPSR** | **§ 2** 1.V § 2 ods. 2 odporúčame vypustiť slová „o ochrane utajovaných“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že je legislatívno-technicky nesprávna. |
| **MŽPSR** | **Všeobecne** 10. Žiadame dať návrh zákona do súladu s platnou legislatívou a smernicou NIS tak, ako je uvedené v predkladacej správe tohto materiálu (deklaruje sa súlad s Ústavou SR, všeobecne záväznými právnymi predpismi atď.), to znamená odstrániť všetky duplicity v koordinácii, riadení, kontrole, ukladaní povinností a uplatňovaní sankčných mechanizmov. Konflikt predstavuje najmä duplicitné zavedenie nového sektoru do kritickej infraštruktúry - „Kybernetický priestor“ (Sektor č. 4 Príloha č. 3 k zákonu č. 45/2011 Z.z.). Podľa definície v § 3 písm. b) návrhu zákona „kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi týmito entitami“ sa jedná prierezovo prakticky o všetko, čo predstavuje zásah a prienik aj do ostatných sektorov kritickej infraštruktúry. Odôvodnenie: MŽP SR je podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre správcom sektoru „Voda a atmosféra“. Ide o jeden z kľúčových kritických sektorov štátu, v ktorom je prevádzkovaná rozsiahla sieť prvkov kritickej infraštruktúry s už vytvorenými procesmi a systémom koordinácie a riadenia. Smernica NIS uvádza, že pokiaľ sú už procesy a vzťahy v sektoroch upravené osobitnými predpismi, tieto „majú pred smernicou NIS prednosť.“ Návrh zákona teda ide vo svojich ustanoveniach nad rámec smernice NIS a je v rozpore s platnou legislatívou SR, nakoľko vytvára duplicitné štruktúry riadenia, kontroly a pod., čím sa dosiahne opak žiadaného cieľa v sektore. Pokiaľ ide o informačné systémy a siete, tieto by mali logicky patriť pod sektor „elektronické komunikácie“ v rámci sektoru „Digitálna infraštruktúra“. Zmeny obsiahnuté v návrhu zákona vnesú do systému nejednoznačnosť a zmätočnosť. | O | A | Upravené v zmysle legislatívnych pravidiel vlády SR. |
| **MŽPSR** | **§ 10** 10.V § 10 ods. 2 za slovo „verejnej“ vložiť slovo „časti“. | O | A |  |
| **MŽPSR** | **§ 10** 11.V § 10 ods. 2 písm. j) slová „§ 28 odsek 3“ nahradiť slovami „§ 28 ods. 3“. | O | A |  |
| **MŽPSR** | **Všeobecne** 11.Žiadame dopracovať absentujúce časti do návrhu zákona, vrátane nedostatočnej a chybnej terminológie, čo považuje MŽP SR z pohľadu svojich príspevkových a rozpočtových organizácií prevádzkujúcich informačné systémy kritickej infraštruktúry za kľúčové, nakoľko predkladaný návrh zákona nerieši problematiku kybernetickej bezpečnosti komplexne a vyčerpávajúco, tak ako sa uvádza vo viacerých častiach tohto materiálu. Návrh sa zaoberá len vymedzeným rozsahom, a to poskytovateľmi „základných služieb“ a poskytovateľmi „digitálnych služieb“, ktorí sa navyše nedajú z tohto návrhu zákona identifikovať. Terminológia je nekonzistentná, rozporuplná a neúplná (hrozba sa zamieňa za riziko, chýbajú základné pojmy s ktorými návrh pracuje: dôvernosť, integrita, dostupnosť, zraniteľnosť, aktívum, analýza rizík, akceptovateľné riziko, a ďalšie). Odôvodnenie:Chybné definície „kybernetickej bezpečnosti“ a „kybernetického priestoru“, pričom ich substitúciou do jednotlivých ustanovení návrhu zákona sa vytvárajú nelogické a cyklické definície, ako aj nevykonateľné ustanovenia. | O | A | Upravené v zmysle legislatívnych pravidiel vlády SR. |
| **MŽPSR** | **§ 10** 12.V § 10 ods. 4 slová „ods.2 písmeno j)“ nahradiť slovami „odseku písm. j)“. | O | A |  |
| **MŽPSR** | **Všeobecne** 12.Žiadame za účelom kompatibility s EÚ priestorom začleniť do návrhu všetky priority uvedené v dokumente „Stratégia kybernetickej bezpečnosti EÚ“ schválenom v roku 2013 a dať ho do súladu tak, ako sa v predkladanom materiáli uvádza. V opačnom prípade žiadame uviesť, že návrh zákona akceptuje iba jednu (prvú) z priorít tohto strategického materiálu EÚ, prípadne uviesť, aký právny predpis a akým spôsobom bude riešiť ostatné absentujúce časti. „Priority Stratégie EÚ: • dosiahnutie kybernetickej odolnosti, • výrazné zníženie počítačovej kriminality • rozvoj politiky a spôsobilostí v oblasti kybernetickej obrany v rámci spoločnej bezpečnostnej a obrannej politiky EÚ (SBOP) • rozvoj priemyselných a technologických zdrojov určených na zaistenie kybernetickej bezpečnosti • vytvorenie jednotnej medzinárodnej politiky EÚ v oblasti kybernetického priestoru“. Odôvodnenie: Návrh zákona deklaruje súlad so „Stratégiou kybernetickej bezpečnosti EÚ,“ ktorá identifikovala päť základných priorít a ktoré by mali všetky členské štáty prijať. Návrh sa však zaoberá iba jednou prioritou z nich a ostatná štyri nepokrýva. Uvedený súlad zákona s citovaným strategickým materiálom považuje MŽP SR za dôležité v súvislosti s problematikou tvorby, správy a zdieľania registrov geopriestorových informácií potrebných pre výkon činnosti iných rezortov a organizácií. | O | ČA | Upravené v zmysle legislatívnych pravidiel vlády SR. |
| **MŽPSR** | **§ 11** 13.V § 11 ods. 2 slová „ods. 1 písmeno b)“ nahradiť slovami „odseku 1 písm. b)“. | O | A |  |
| **MŽPSR** | **§ 12** 14.V § 12 ods. 4 slová „osobitným predpisom“ nahradiť slovami „podľa osobitného predpisu“. | O | A |  |
| **MŽPSR** | **§ 13** 15.V § 13 ods. 1 odporúčame na koniec pripojiť tieto slová „na základe žiadosti“ v súvislosti s odsekom 2. | O | A |  |
| **MŽPSR** | **§ 13** 16.V § 13 ods. 6 vypustiť slovo „platné“ z dôvodu nadbytočnosti a slová „vzťahuje odsek 1, 2 a 7“ nahradiť slovami „vzťahujú odseky 1, 2 a 7“. | O | A |  |
| **MŽPSR** | **§ 16** 17.V § 16 ods. 3 v úvodnej vete vypustiť slovo „najmä“ a kreatívne služby uvádzať taxatívne alebo doplniť písmeno e) iné služby s príslušným vysvetlením. | O | A |  |
| **MŽPSR** | **§ 17** 18.V § 17 ods. 1 slová „podľa prílohy č. 1“ nahradiť slovami „uvedených v prílohe č.1“. | O | A |  |
| **MŽPSR** | **§ 18** 19.V § 18 ods. 6 odkaz 23 umiestniť nad slovo „predpisu“. | O | A |  |
| **MŽPSR** | **§ 3** 2. V § 3 navrhujeme definovať pojem „kybernetické ohrozenie“, ktorý sa používa napr. v § 6 ods. 1 písm. q). a „kybernetický útok“, ktorý sa používa v návrhu doplnenia zákona č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov. Odôvodenie: Absencia vymedzenia pojmov. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná. Bol upravený celý § 3 a boli zavedené nové pojmy. |
| **MŽPSR** | **§ 3** 2.V § 3 písm. g) slová „podľa prílohy č. 1“ nahradiť slovami „ktoré sú uvedené v prílohe č.1“. Doplniť názov prílohy č. 1. | O | A |  |
| **MŽPSR** | **§ 19** 20.V § 19 za slovo „informačného“ vložiť slovo „systému“ a v odseku 4 v úvodnej vete vypustiť slovo „najmenej“ a bezpečnostné opatrenia uvádzať taxatívne. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že taxatívne vymenovanie je neúčelné. |
| **MŽPSR** | **§ 20** 21.V § 20 ods. 1 za slovo „Poskytovateľ“ vložiť slovo „digitálnej“ a slová podľa prílohy č. 2 „ nahradiť slovami „uvedených v prílohe č. 2“. | O | A | Vaša pripomienka bola akceptovaná a textácia bola upravená v zmysle pripomienky. |
| **MŽPSR** | **§ 21** 22.V § 21 ods. 2 v úvodnej vete vypustiť slovo „najmä“ a taxatívne uviesť to čo poskytovateľ digitálnej služby posudzuje. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že "najmä" predstavuje minimálnu úroveň prijatých opatrení a nepredstavuje obmedzenie prijať a aplikovať aj iné, v zákone definované, bezpečnostné opatrenia. |
| **MŽPSR** | **§ 24** 23.V § 24 ods. 4 a § 25 ods. 6 slovo „Pokiaľ“ nahradiť slovom „Ak“. | O | A |  |
| **MŽPSR** | **§ 27** 24.V § 27 ods. 1 v úvodnej vete vypustiť slovo „najmä“ a následne taxatívne uvádzať spôsoby riešenia kybernetických bezpečnostných incidentov. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že v oblasti zabezpečenia bezpečnosti nie je limitovanie opatrení na riešenie incidentov žiadúce ani efektívne. Absolútny výpočet by nebol možný ani na úrovni vykonávacieho predpisu. |
| **MŽPSR** | **§ 31** 25.V § 31 ods. 2 a § 32 ods. 1 uviesť dolnú hranicu výšky pokuty. | O | A |  |
| **MŽPSR** | **§ 35** 26.V § 35 odporúčame uvádzať konkrétne dátumy. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu potrieb praxe. |
| **MŽPSR** | **prílohe č. 1** 27.V prílohe č. 1 doplniť vysvetlivky k skratkám „PZS“ A „VPA“. | O | A |  |
| **MŽPSR** | **§ 3** 3.V § 3 písm. h) odporúčame vypustiť slovo „každý“ z dôvodu nadbytočnosti. | O | A |  |
| **MŽPSR** | **§ 6** 3.V § 6 ods. 1, písm. l) navrhujeme vypustiť po slove „povedomia“ slová „vykonáva a zabezpečuje“. Odôvodnenie: Odstránenie uvedených slov má gramatický charakter. | O | A |  |
| **MŽPSR** | **§ 4** 4.V § 4 ods. 1 za slovo „verejného“ vložiť slovo „sektora“ a za slovo „bezpečnostné“ vložiť slovo „záujmy. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **MŽPSR** | **§ 6** 4.V § 6 ods. 1 písm. m) navrhujeme slov „vykonáva“ nahradiť slovom „koordinuje“. Odôvodnenie: V zmysle bodu 3.7 „Podpora vedy a výskumu v oblasti kybernetickej bezpečnosti“ schválenej „Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020“ sa uvádza, že „Výskumné aktivity v tejto oblasti bude koordinovať ústredný orgán štátnej správy pre kybernetickú bezpečnosť.“. | O | A |  |
| **MŽPSR** | **§ 5** 5.V § 5 písm. b) vypustiť odkaz 10 a poznámku pod čiarou k odkazu 10 z dôvodu nadbytočnosti a zjednotenia s ostatnými odsekmi a bodmi. | O | A |  |
| **MŽPSR** | **§ 6** 5.V § 6 ods. 2 navrhujeme vynechať poslednú vetu „Dohoda o spolupráci nie je povinne zverejňovanou zmluvou.“ aj s poznámkou pod čiarou č. 11. Následne prečíslovať nasledujúce poznámky pod čiarou. Odôvodnenie: Fyzická osoba alebo právnická osoba bude na základe dohody o spolupráci vykonávať úlohy aj podľa medzinárodných zmlúv, ktorými je Slovenská republika viazaná. Z dôvodu transparentnosti voči zahraničným partnerom by bolo vhodné jej povinné zverejňovanie. | O | A |  |
| **MŽPSR** | **§ 6** 6.V § 6 ods. 1 písm. g) prvom bode na konci vložiť čiarku. | O | A |  |
| **MŽPSR** | **§ 7** 6.V § 7 ods. 1 navrhujeme za slovo „postavenie“ vložiť slovo Národnej“. Odôvodnenie: Upravenie pojmu (NBÚ má postavenie Národnej jednotky CSIRT). | O | A |  |
| **MŽPSR** | **§ 13** 7.V § 13 ods. 3 navrhujeme nahradiť číslo „15” číslom “14”. Odôvodnenie: Domnievame sa, že zákonodarca myslel požiadavky v znení ustanovenia § 14 nie § 15. | O | A |  |
| **MŽPSR** | **§ 7** 7.V § 7 ods. 1 slová „podľa prílohy č. 1 a 2“ nahradiť slovami „uvedené v prílohe č. 1“ . V prílohe č. 2 sú uvedené digitálne služby. | O | A |  |
| **MŽPSR** | **§ 8** 8.§ 8 odporúčame rozdeliť z dôvodu lepšej zrozumiteľnosti. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený a zaradený medzi úlohy úradu z dôvodu duplicitnej úlohy v zákone na účely konkrétnej definície stanovených opatrení v oblasti medzinárodných vzťahov a spolupráce. |
| **MŽPSR** | **§ 29 ods. 6** 9. K § 29 ods. 6 návrhu zákona: „Príslušníci úradu sú v súvislosti s výkonom kontroly a v rozsahu potrebnom na jej vykonanie oprávnení vstupovať do komunikačných a informačných systémov do úrovne správcu systému, vrátane oprávnenia dočasne zmeniť hardvérovú alebo softvérovú konfiguráciu.“ Uvedené oprávnenia príslušníkov úradu považujeme za neprimerané a nad rámec účelu kontroly. Odôvodnenie: V uvedenom prípade by kontrolóri získali oprávnenie až do úrovne správcu systému, čo by znamenalo, žeby títo získali administrátorské oprávnenia umožňujúce im prístup k akejkoľvek informácii v rámci komunikačných a informačných systémov. S takýmito oprávneniami je možné v systéme údaje a informácie modifikovať, vymazať, či kopírovať a zároveň aj uskutočniť zmenu, ktorá by umožnila znížiť úroveň bezpečnosti systému, či útok na daný systém. Pre prípady dočasnej zmeny hardvérovej a softvérovej konfigurácie nie je jasne stanovená zodpovednosť za škody spôsobené zmenou konfigurácie. Zároveň v súčinnosti s navrhovaným ustanovením § 6 ods. 2 toto považujeme za neprípustné. | O | A |  |
| **MŽPSR** | **§ 9** 9.V § 9 ods. 2 v úvodnej vete vypustiť slovo „najmä“ a obsah národnej strategickej kybernetickej bezpečnosti uvádzať taxatívne. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že taxatívne vymedzenie nie je žiadúce. Úprava korešponduje s ustanovením smernice NIS. |
| **MŽPSR** | **Akreditácii jednotkx CSIRT** Je pozitívne, že návrh zákona o kybernetickej bezpečnosti v zmysle dôvodovej správy vo veci právnej absencie podmienok akreditácie jednotky CSIRT odkazuje na existujúci a najmä funkčný model (model aplikovaný v rámci problematiky ochrany utajovaných skutočností). Avšak v § 14 odsek 1 písm. d) odkaz na § 5 vyhlášky Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení vyhlášky č. 315/2006 Z. z. nie je jednoznačný. Toto ustanovenie (§ 5) odkazuje na ochranu objektu a chráneného priestoru určeného na ochranu utajovaných skutočností, pričom úroveň zabezpečenia je závislá od miery rizika a stupňa chránených utajovaných skutočností. Ak (ako uvádza dôvodová správa) informačný a komunikačný systém jednotky CSIRT bude musieť spĺňať spôsobilosti na prenos a spracovanie utajovaných skutočností, na aký stupeň to bude? Ďalšia vec v rámci podmienok akreditácie jednotky CSIRT je skutočnosť, že jednotkou CSIRT môže byť aj iný subjekt, ako orgán verejnej moci. Keďže (v zmysle dôvodovej správy) informačný a komunikačný systém jednotky CSIRT bude musieť spĺňať spôsobilosti na prenos a spracovanie utajovaných skutočností, jedna z podmienok tohto subjektu bude potreba mať potvrdenie o priemyselnej bezpečnosti a personál (aj pokiaľ bude jednotkou CSIRT orgán verejnej moci) v určitom prípade (Dôverné a vyššie) osvedčenie o personálnej bezpečnosti. Previerkový proces trvá určitú lehotu, čo je viac, ako uvedená 90-dňová lehota na rozhodnutie vo veci akreditácie, čiže žiadateľ o akreditáciu jednotky CSIRT musí predložiť platné potvrdenie, resp. osvedčenie už pri podaní žiadosti. Navyše, podľa § 13 ods. 8. úrad môže uznať akreditáciu jednotky CSIRT, ktorá bola akreditovaná podľa predpisov iného štátu alebo medzinárodnej organizácie, ak je zabezpečené splnenie podmienok akreditácie jednotky CSIRT podľa tohto zákona. Čiže subjekt bude spĺňať podmienky akreditácie podľa predpisov iného štátu alebo medzinárodnej organizácie, zákona o akreditácie, avšak kvôli podmienke, že informačný a komunikačný systém jednotky CSIRT bude musieť spĺňať spôsobilosti na prenos a spracovanie utajovaných skutočností, bude potrebne tejto subjekt „doakreditovať“ v zmysle zákona o kybernetickej bezpečnosti (aby spĺňal podmienku atribútu ochrany utajovaných skutočností v zmysle zákona o kybernetickej bezpečnosti), čo je administratívna záťaž a preto dávame na zváženie, či je potrebné, aby informačný a komunikačný systém jednotky CSIRT musel spĺňať spôsobilosti na prenos a spracovanie utajovaných skutočností. Pokiaľ má informačný a komunikačný systém jednotky CSIRT byť „prísnejší“, navrhujeme uviesť explicitne prísnejšie podmienky na jeho zabezpečenie, avšak bez odvolávania sa na aplikovanie podmienok v oblasti ochrany utajovaných skutočností. | O | A | Upravené v zmysle legislatívnych pravidiel vlády SR a vysvetlené v dôvodovej správe. |
| **MŽPSR** | **vecnej a osobnej pôsobnosti** Na jednej strane návrh zákona v § 2 ods. 1 stanovuje, že „tento zákon ustanovuje súbor minimálnych požiadaviek na zabezpečenie kybernetickej bezpečnosti“, pričom podľa § 3 písm. d) návrhu zákona sa kybernetickou bezpečnosťou rozumie „stav, v ktorom sú siete a informačné systémy schopné odolávať kybernetickým bezpečnostným incidentom“. No na strane druhej stanovuje povinnosti iba pre prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb a teda iba pre obmedzený okruh subjektov a ich siete, resp. informačné systémy. Uvedené navrhujeme uviesť do súladu. Odôvodnenie: Kybernetická bezpečnosť je chápaná ako systém, ktorý má v rámci kybernetického priestoru garantovať bezpečnosť nielen sieťam a informačných systémom, ale aj elektronickým komunikačným a riadiacim systémom, ako aj dátam, ktoré sú v nich uchovávané, resp. službám, ktoré sú nimi poskytované. Vymedzenie vecnej pôsobnosti (§ 2 ods. 1 návrhu zákona: „tento zákon ustanovuje súbor minimálnych požiadaviek na zabezpečenie kybernetickej bezpečnosti“) je priamo v rozpore s vymedzením osobnej pôsobnosti návrhu zákona, nakoľko osobná pôsobnosť návrhu zákona (t.j. vymedzenie okruhu osôb, na ktoré sa bude právna norma aplikovať) je zúžený už iba na prevádzkovateľov základných a služieb a poskytovateľov digitálnych služieb a nepokrýva všetky subjekty v rámci kybernetického priestoru. Predkladaný návrh zákona mal podľa uznesenia vlády SR č. 93/2016 riešiť problematiku komplexne, pričom mal vychádzať z legislatívneho návrhu zákona o informačnej bezpečnosti, riešiť problematiku kybernetickej bezpečnosti a transponovať smernicu NIS, tak ako to vyplýva z prvého odseku „Predkladacej správy“ (uznesenie k Akčnému plánu ku Koncepcii kybernetickej bezpečnosti na roky 2015 – 2020), „Dôvodovej správy – všeobecná časť“ (odsek prvý), z odseku za prvou tabuľkou, z odseku za druhou tabuľkou, ako aj z príslušných Doložiek vplyvov. | O | A | Upravené v zmysle LPV a vysvetlené v dôvodovej správe. |
| **MŽPSR** | **§ 11** Podľa § 11 ods. 1 písm. f) návrhu zákona je Ministerstvo životného prostredia SR vecne príslušná autorita. Návrh zákona stanovuje vecne príslušným autoritám veľký rozsah nových povinností (§ 11 návrhu zákona, prevádzka jednotky CSIRT, napojenie do jednotného informačného systému kybernetickej bezpečnosti atď.). Budovanie týchto kapacít a spôsobilostí je značne náročnou finančnou záležitosťou (vyžadujúcou si naviac aj budovanie personálnych kapacít), pričom nie je z doložky vplyvov jasné, koľko finančných prostriedkov (a či zo štátneho rozpočtu alebo financovanie z fondov) bude v rámci vecne príslušných autorít na budovanie kapacít vyčlenených). Navrhujeme preto doplniť podrobnú analýzu vplyvov a v členení na jednotlivé rozpočtové roky vyčísliť finančné náklady potrebné na zavedenie nových povinností. Odôvodnenie: Uvedené doplnenie je nevyhnutné vychádzajúc z Legislatívnych pravidiel vlády SR ako aj z Jednotnej metodiky na posudzovanie vplyvov. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ochrana sietí a IS je existujúca úloha aj v súčasnosti. Tento zákon len upravuje minimálne bezpečnostné opatrenia na toto zabezpečenie, nejde teda o nové kompetencie vyžadujúce si nové kapacity. Po vysvetlení bol rozpor odstránený. |
| **MŽPSR** | **§ 3** Podľa § 3 písm. h) sú „prevádzkovateľom základnej služby orgány verejnej moci, právnické osoby alebo fyzické osoby podnikatelia, ktorí prevádzkujú základnú službu, každý správca informačného systému verejnej správy a sú zároveň zaradení do registra prevádzkovateľov základných služieb“, pričom podľa písm. g) základnou službou je taká „služba, ktorá závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1, ktorá je zaradená v zozname základných služieb“. Podľa § 11 ods. 1 písm. f) návrhu zákona vecne príslušná autorita (ktorou je podľa § 5 písm. c) bod 8 návrhu zákona aj Ministerstvo životného prostredia SR) „zabezpečuje identifikovanie základnej služby a prevádzkovateľa základnej služby spôsobom podľa § 17 ods. 1; ich aktuálny zoznam sa predkladá NBÚ na účely zaradenia do zoznamu základných služieb a registra prevádzkovateľov základných služieb“. Identifikácia prevádzkovateľa základnej služby je však možná iba vtedy (§ 17 ods. 1 návrhu zákona), keď prevádzkovateľ základnej služby zistí, že došlo k prekročeniu prahových hodnôt kritérií ustanovených všeobecne záväzným právnym predpisom. Z ustanovení predloženého zákona však nijakým spôsobom nevieme ako vecne príslušná autorita identifikovať, ktoré subjekty z nám vymedzeného sektora „Dodávka a distribúcia pitnej vody“ (sektor č. 2 prílohy č. 1 k návrhu zákona) budú spadať pod pôsobnosť zákona a ktorých subjektov z našej pôsobnosti sa návrh zákona dotýka. Uvedené považujeme za vážny nedostatok a navrhujeme preto doplniť priamo do zákona identifikačné kritéria, prípadne vykonávací právny predpis určujúci identifikačné kritéria pre prevádzkovateľov základnej služby predložiť súčasne s návrhom zákona, tak aby súčasne s účinnosťou zákona nadobudol účinnosť aj vykonávací predpis. Odôvodnenie: Z ustanovení návrhu zákona tak nie je možné identifikovať, kto je prevádzkovateľom základnej služby, nakoľko prahové hodnoty kritérií majú byť stanovené až vo vykonávacom právnom predpise (ktorý v čase predloženia návrhu zákona nebol daný pripomienkujúcim subjektom k dispozícii) a nie je súčasťou predkladaného návrhu zákona. Uvedené je v rozpore s čl. 17 ods. 1 písm. i) Legislatívnych pravidiel vlády, nakoľko máme za to, že vykonávací predpis stanovujúci prahové hodnoty pre identifikáciu základnej služby musí nadobudnúť účinnosť súčasne so zákonom. Bez ich stanovenia nie je možné presne vymedziť osobnú pôsobnosť zákona, nie je možné stanoviť kto je osobou povinnou zo zákona a nie je teda jasné, kto je v konečnom dôsledku prevádzkovateľom základnej služby povinný plniť úlohy vyplývajúce zo zákona. Uvedené je vo vážnom rozpore aj s požiadavkami stanovenými v čl. 6 ods. 1 Legislatívnych pravidiel vlády. | Z | ČA | Nová príloha č. 1, nová definícia PZS, doplnené identifikačné kritériá na ZS, doplnená dôvodová správa tak, aby vyčerpávajúco vysvetľovala, na koho sa zákon vzťahuje a tézy vyhlášok budú súčasťou schvaľovacieho procesu. Do účinnosti zákona sa predpokladá prijatie vykonávacích predpisov. Po vysvetlení rozpor odstránený. |
| **NBS** | **k čl. I vseobecná pripomeinka** 2. Navrhujeme prehodnotiť navrhovaný distribuovaný model zodpovedností za kybernetickú bezpečnosť vo forme mnohých vecne príslušných autorít (VPA) a jednotiek CSIRT a zvážiť zriadenie jednej autority pre kybernetickú bezpečnosť pre celú Slovenskú republiku, ktorá by sústreďovala tím odborníkov schopných pokryť všetky sektory a podsektory. Zásady kybernetickej bezpečnosti sú viac-menej rovnaké bez ohľadu na sektor. Je efektívnejšie, a zároveň aj reálnejšie vybudovať jeden odborne zdatný tím, ktorý bude túto oblasť koordinovať, ako očakávať, že množstvo VPA a jednotiek CSIRT bude schopné zabezpečiť výkon činností na očakávanej odbornej úrovni v každom sektore kvôli možnému deficitu vysokokvalifikovanej pracovnej sily v tejto oblasti. Taktiež očakávaný počet pracovníkov, ako aj celkové finančné náklady budú pri navrhovanom modeli viacerých autorít vyššie. IT riziká sú porovnateľné prierezovo pre všetky sektory a podsektory. 3. Zo znenia predloženého návrhu zákona nie je zrejmé, jednoznačné právne postavenie jednotky CSIRT (má to byť útvar v rámci VPA, nová inštitúcia) a kto vlastne bude prevádzkovateľom jednotky CSIRT (má to byť útvar VPA, iná inštitúcia). 4. V predloženom návrhu zákona navrhujeme, tam kde je to možné, cudzie slová nahradiť vhodnými slovenskými výrazmi (napríklad v § 3 písm. b) cudzie slová „interakcie”, “entita”, v § 8 cudzie slovo „kooperácia“, v § 10 ods. 6 cudzie slovo „funkcionalita“). 5. Návrh zákona je potrebné upraviť tak, aby všetky jeho ustanovenia mali normatívny charakter a tiež je potrebné upraviť ho gramaticky. | O | ČA | Návrh zákona bol čiastočne preformulovaný v zmysle pripomienky. |
| **NBS** | **Pripomienky k ostatnej dokumentácii** 1. Predkladaciu správu navrhujeme zosúladiť s čl. 18 a čl. 23 ods. 3 písm. a) Legislatívnych pravidiel vlády SR. 2. Do názvu doložky zlučiteľnosti navrhujeme doplniť slovo „návrhu“ pred spojenie „právneho predpisu“, v súlade s Legislatívnymi pravidlami vlády SR. 3. V časti 4. doložky zlučiteľnosti - Záväzky Slovenskej republiky vo vzťahu k Európskej únii chýba časť d), to znamená informácia o právnych predpisoch, v ktorých sú preberané smernice už prebraté spolu s uvedením rozsahu tohto prebratia. 4. Na strane 3 osobitnej časti dôvodovej správy pri § 7 nie je zrejmé, o aké centrum ide, zrejme sa jedná o Národnú jednotku CSIRT. | O | A |  |
| **NBS** | **k § 2** 1. V § 2 ods. 1 znenie druhej vety odporúčame zvážiť vzhľadom k pojmu „môže“, pretože vzťah zákona o kybernetickej bezpečnosti a osobitných predpisov by mal byť vymedzený jednoznačne a nie ponechaný na voľbu príslušného subjektu. Zároveň odporúčame zvážiť, či táto druhá veta je vyjadrením pôsobnosti zákona. 2. V § 2 ods. 2 písm. a) navrhujeme na konci textu písmena doplniť slovo „skutočností“. | O | A |  |
| **NBS** | **k tabulke zhody** 1. V celej tabuľke zhody navrhujeme zjednotiť odkazy k návrhom zákonov, keďže nekorešpondujú so znením návrhu zákona. 2. Pri transpozícii Č:1, O:4 smernice NIS navrhujeme opraviť § 2,O:3, keďže takéto ustanovenie sa v návrhu zákona nenachádza. 3. Pri transpozícii Č:1, O:5 smernice NIS navrhujeme opraviť na §:6, O:1,P:u (namiesto t). 4. Znenie § 12 ods. 1 v tabuľke zhody nekorešponduje so znením tohto ustanovenia v návrhu zákona (chýbajú dohody o spolupráci). 5. Transpozícia Č:1, O:6 smernice NIS nekorešponduje so znením zákona. 6. Pri transpozícii Č:4, O:4 smernice NIS navrhujeme opraviť na §:3,P:h (namiesto k), a taktiež znenie ustanovenia uvedené v tabuľke zhody nie je v súlade so znením návrhu zákona. 7. Pri transpozícii Č:4, O:10 smernice NIS navrhujeme opraviť na §:22,O:1,2 (namiesto §:20,O:1). 8. Na strane 8 a 9 tabuľky zhody navrhujeme v 5. stĺpci spojenie „Príloha č. 2“ nahradiť spojením „Príloha č. 1“ a Príloha č. 3“ nahradiť „Príloha č. 2“. 9. § 6, O:1, P:e, § 11, O:1, P:f, § 18, O:3,4, §:5, §:7, O:1, §:10, O:2,5, §:21, O:1, §:24, O:2, §:27, O:2,3,4,5, §:30, O:1 tabuľky zhody navrhujeme zosúladiť so znením návrhu zákona. 10. Pri Č:6, O:1 navrhujeme prehodnotiť dostatočnosť transpozície do §:24, O:1. 11. Pri transpozícii Č:15, O:4 smernice NIS navrhujeme prehodnotiť uvedené znenie v tabuľke zhody, pretože Úrad na ochranu osobných údajov, ktorý je zrejme príslušný orgán, nie je ústredným orgánom štátnej správy v zmysle zákona č. 575/2001 Z. z. 12. Pri Č:16, O: 1, ako aj pri Č:18 O:1 tabuľky zhody navrhujeme prehodnotiť dostatočnosť transpozície do návrhu zákona. 13. Pri Č:16, O: 10 tabuľky zhody chýba uvedenie transpozície. 14. Pri transpozícii Č:17, O:2 smernice NIS navrhujeme opraviť na §:29 (namiesto §:25). 15. Pri transpozícii Č:20, O:1 smernice NIS navrhujeme opraviť na §:4, O:6. 16. § 31 a § 32 v tabuľke zhody navrhujeme zosúladiť s návrhom zákona, keďže uvedené sankcie sa v oboch dokumentoch líšia. 17. Text prílohy č. 1 v tabuľke zhody navrhujeme zosúladiť s textom prílohy č. 1 návrhu zákona. | O | A |  |
| **NBS** | **K čl. I všeobecná pripomienka** 1. Z dôvodu, že návrh zákona sa dotýka finančných inštitúcií, ide o oblasť pôsobnosti Európskej centrálnej banky (ďalej len „ECB“), a preto predkladateľ návrhu tohto zákona musí ECB požiadať o konzultáciu k návrhu zákona v zmysle čl. 127 ods. 4 Zmluvy o fungovaní EÚ a nadväzného rozhodnutia Rady o poradení sa s Európskou centrálnou bankou národnými orgánmi ohľadom návrhu právnych prepisov (98/415/ES). Táto pripomienka je zásadná. | Z | A | Na rozporovom konaní zástupcovia NBS preformulovali zásadnú pripomienku na obyčajnú, čím bol rozpor odstránený. Úrad berie na vedomie povinnosti, ktoré mu v tejto súvislosti vyplývajú a zabezpečí notifikáciu právneho predpisu. |
| **NBS** | **k § 4** 10. V § 4 odporúčame znenie odsekov 1 až 5 buď preformulovať tak, aby mali normatívny charakter, alebo ich vypustiť. V prípade vypustenia odsekov 1 až 6 je potrebné znenie odseku 6 začleniť do iného paragrafu zákona. 11. V § 4 ods. 1 navrhujeme slová „verejného a súkromného sektora“ nahradiť slovami „verejného sektora a súkromného sektora“ a rovnako navrhujeme upraviť celý návrh zákona. 12. V § 4 ods. 6 navrhujeme doplniť komu majú subjekty oznamovať kybernetické bezpečnostné incidenty (spôsob ich oznamovania). | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **NBS** | **k § 5** 13. V § 5 navrhujeme zvážiť, či je potrebné v nadväznosti na znenie písmena b), Národný bezpečnostný úrad začleniť aj medzi vecne príslušné autority vymenované v písmene c). Navrhnutým členením vznikajú nejasnosti, to znamená úrad má povinnosti a úlohy ako úrad a zároveň si má sebe plniť úlohy ako vecne príslušná autorita (napríklad § 7 ods. 3, § 9 ods. 3, § 10 ods. 5, § 27 ods. 6, § 28 ods. 5). | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že nie je pripomienkou v zmysle Legislatívnych pravidiel vlády. Úrad vystupuje ako vecne príslušný subjekt aj ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť a na základe toho má teda dve oddelené úlohy. |
| **NBS** | **k § 6** 14. V § 6 navrhujeme znenie písmena h) upraviť takto: „h) vedie register prevádzkovateľov základných služieb a register poskytovateľov digitálnych služieb a zoznam základných služieb, zoznam digitálnych služieb a zoznam akreditačných jednotiek CSIRT,“. Primerane je potrebné spresniť aj registre a zoznamy upravené v ďalších ustanoveniach zákona. Zároveň odporúčame zvážiť, či do tohto ustanovenia nie je potrebné doplniť aj register vecne príslušných autorít a register kybernetických bezpečnostných incidentov, respektíve do návrhu zákona doplniť, kto bude viesť tieto dva registre. 15. V § 6 ods. 1 písm. p) navrhujeme slovo „vedie“ nahradiť slovom „prevádzkuje“. 16. V § 6 ods. 1 písm. o) a tiež v ďalších ustanoveniach návrhu zákona je použitý pojem „Národná jednotka CSIRT“, ktorý nie je v návrhu zákona dostatočne zadefinovaný, ani nie je preň zavedená legislatívna skratka obdobne ako pre jednotky CSIRT. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že znenie bolo zmenené z dôvodu precizovania. |
| **NBS** | **k § 7** 17. V § 7 navrhujeme znenie odseku 1 spresniť v nadväznosti na našu pripomienku k § 6 ods. 1 písm. o). Zároveň odporúčame z dôvodu jednoznačnosti v tomto odseku spresniť, kto sa myslí vecne príslušnou autoritou podľa § 11 ods. 2. 18. V § 7 ods. 3 navrhujeme v nadväznosti na znenie § 3 písm. a) slová „k informačným systémom a sieťam“ nahradiť slovami „k sieťam a informačným systémom“. Primeraná pripomienka platí k celému návrhu zákona. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a vysvetlená v dôvodovej správe. |
| **NBS** | **k § 9** 19. V § 9 ods. 2 je potrebné na konci úvodnej vety vypustiť dvojbodku. V odseku 2 písm. a) navrhujeme spresniť, čo sa myslí slovami „ďalších relevantných aktérov“ a primerane upraviť aj písmeno i). V odseku 2 písm. b) odporúčame spresniť, čoho sa má pripravenosť, reakcia a obnova týkať. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a vysvetlená v dôvodovej správe. |
| **NBS** | **k § 10**  20. V § 10 ods. 2 druhej vete navrhujeme slová „verejnej a neverejnej časti“ nahradiť slovami „verejnej časti a neverejnej časti“ a rovnako navrhujeme upraviť celý návrh zákona. V odseku 2 písm. j) je potrebné slovo „odsek“ nahradiť slovo „ods.“. 21. V § 10 ods. 4 navrhujeme slová „podľa ods. 2 písmeno j)“ nahradiť slovami „podľa odseku 2 písm. j)“. | O | A |  |
| **NBS** | **k § 10 ods. 5** 22. V § 10 ods. 5 je potrebné písmeno e) upraviť takto: „e) Národná banka Slovenska, x)“. Znenie poznámky pod čiarou k odkazu x navrhujeme upraviť takto: „x) Napríklad zákon Národnej rady Slovenskej republiky č. 566/1992 Zb. v znení neskorších predpisov, zákon č. 747/2004 Z. z. o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, nariadenie Európskej centrálnej banky (EÚ) č. 468/2014 (ECB/2014/17) zo 16. apríla 2014 o rámci pre spoluprácu v rámci jednotného mechanizmu dohľadu medzi Európskou centrálnou bankou, príslušnými vnútroštátnymi orgánmi a určenými vnútroštátnymi orgánmi (nariadenie o rámci JMD) (Ú. v. EÚ L 141, 14.5.2014), nariadenie Európskeho parlamentu a Rady (EÚ) č. 1092/2010 z 24. novembra 2010 o makroprudenciálnom dohľade Európskej únie nad finančným systémom a o zriadení Európskeho výboru pre systémové riziká (Ú. v. EÚ L 331, 15.12.2010), Protokol (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky (Ú. v. EÚ C 202, 7.6.2016) v platnom znení.“. Zároveň upozorňujeme, že v odseku 5 sú úrad a ministerstvo obrany uvedené duplicitne, to znamená v samostatných písmenách a) a i) a tiež v písmene b) /podľa § 5 písm. c) sú vecne príslušnou autoritou/. V nadväznosti na nami navrhovanú pripomienku je potrebné upraviť číslovanie odkazov a poznámok pod čiarou návrhu zákona. Táto pripomienka je zásadná. | Z | A |  |
| **NBS** | **k § 10 ods. 8** 23. § 10 navrhujeme doplniť odsekom 8, v tomto znení: „(8) Národná banka Slovenska spolupracuje s Európskou centrálnou bankou, s účastníkmi Jednotného mechanizmu dohľadu a s Európskym systémom finančného dohľadu pri výmene informácií aj z neverejnej časti informačného systému kybernetickej bezpečnosti, ak ide o informácie v oblasti kybernetického rizika v sektore bankovníctva a finančného sektora podľa prílohy č. 1.“. Táto pripomienka je zásadná. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že Národná banka Slovenska plní úlohy vyplývajúce z osobitných predpisov a zároveň na základe ustanovení zákona o kybernetickej bezpečnosti plní úlohy na úseku kybernetickej bezpečnosti. Odsek 7 bol z ustanovenia vypustený bez náhrady, čím nie sú kladené prekážky pri zabezpečovaní informácií v potrebnom rozsahu na iné zákonné účely, tak ako navrhujete vo vašej pripomienke. Systém a pracovanie jednotného informačného systému kybernetickej bezpečnosti bol na rozporovom konaní vysvetlený, bolo uvedené, že sa bude budovať na základe dohôd NBÚ a zainteresovaných subjektov, pričom nebude zasahovať do právomocí a pôsobností NBS podľa iných predpisov. Uvedie sa aj v dôvodovej správe tak, aby nevznikali pochybnosti. Záver: Po vysvetlení rozpor odstránený. |
| **NBS** | **k § 11**  24. V § 11 ods. 1 navrhujeme za písmeno d) vložiť nové písmeno e) v tomto znení: „e) vyjadrenie Národnej banky Slovenska k postupu vecne príslušnej autority pri plnení úloh podľa tohto zákona, ak je prevádzkovateľom základnej služby subjekt finančného trhu podliehajúci dohľadu vykonávanému Národnou bankou Slovenska, xx)“. Znenie poznámky pod čiarou k odkazu xx navrhujeme upraviť takto: „xx) § 1 ods. 3 písm. a) zákona č. 747/2004 Z. z. v znení neskorších predpisov.“. V nadväznosti na nami navrhovanú pripomienku je potrebné upraviť v § 11 ods. 1 označenie nasledujúcich písmen a tiež číslovanie odkazov a poznámok pod čiarou návrhu zákona. Táto pripomienka je zásadná. | Z | A | Doplnené do úloh toho subjektu, ktorý plní úlohy jednotky CSIRT (§ 16 ods. 1 písm. c). Uvedenou úpravou sa zabezpečí širší okruh povinných subjektov, ako to bolo uvedené v pripomienke. |
| **NBS** | **k § 11**  25. V § 11 ods. 1 písm. g) odporúčame formou odkazu a poznámky pod čiarou aspoň príkladom uviesť, o aký osobitný predpis ide. Primeraná pripomienka platí aj k § 19 ods. 1. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že vymedzenie osobitných predpisov, ktoré spravujú informačný systém je široké a je doplnené do dôvodovej správy. Uvedenie subjektov príkladmo nemá žiadny regulačný význam. |
| **NBS** | **k § 13** 27. V § 13 je potrebné spresniť nejasné znenie odseku 1. 28. V § 13 ods. 2 navrhujeme za slovo „žiadosť“ doplniť slová „o akreditáciu“ a primerane spresniť aj nasledujúce ustanovenia návrhu zákona. Na konci odseku 2 doplniť slová „(ďalej len „žiadateľ“). 29. V § 13 ods. 3 navrhujeme slová „podľa § 15“ nahradiť slovami „podľa § 14“. 30. V § 13 ods. 4 navrhujeme spresniť o aké konanie ide, pretože v odseku 1, na ktorý sa v odseku 4 odkazuje konanie nie je upravené, (napríklad za slovo „konanie“ odporúčame doplniť slová „o zhode“); slovo „stanovenej“ odporúčame nahradiť slovom „určenej“. Zároveň odporúčame na konci druhej vety odseku 4 doplniť slová „od doručenia výzvy“. 31. V § 13 ods. 5 navrhujeme slová „ak posúdi zhodu jednotky CSIRT“ nahradiť slovami „ak posúdi, že jednotka CSIRT je v zhode s podmienkami akreditácie podľa § 14 a ?, vydá rozhodnutie“. Zároveň odporúčame zvážiť pojem „spravidla na päť rokov“ pre jeho právnu neistotu. 32. V § 13 ods. 6 odporúčame spresniť, koľkokrát „opakovane“ môže byť rozhodnutie o akreditácii predĺžené. | O | A | Vaša pripomienka bola čiastočne akceptovaná a upravená primerane legislatívnej technike. |
| **NBS** | **k § 2**  3. V § 2 ods. 2 navrhujeme za písmeno b) vložiť nové písmeno c) v tomto znení: „c) požiadavky na zabezpečenie sietí a informačných systémov v sektore bankovníctva alebo financií podľa osobitného predpisu, 4) štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Národnou bankou Slovenska, Európskym systémom centrálnych bánk alebo Eurosystémom, 5) ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov,“. Znenie poznámok pod čiarou k odkazom 4 a 5 navrhujeme upraviť takto: „4) Napríklad § 28c, § 28d, § 45 ods. 8 a § 64 ods. 4 zákona č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov (v súčasnosti v legislatívnom procese), nariadenie Európskej centrálnej banky (EÚ) č. 795/2014 z 3. júla 2014 o požiadavkách v oblasti dohľadu nad systémovo dôležitými platobnými systémami (ECB/2014/28) (Ú. v. EÚ L 217, 23.7.2014), usmernenie Európskej centrálnej banky č. ECB/2012/27 (2013/47/EÚ) z 5. decembra 2012 o Transeurópskom automatizovanom expresnom systéme hrubého vyrovnania platieb v reálnom čase (TARGET2) (Ú. v. EÚ L 30, 30.1.2013) v platnom znení, usmernenie Európskej centrálnej banky č. ECB/2012/13 (2012/473/EÚ) z 18. júla 2012 o TARGET2-Securities (Ú. v. EÚ L 215, 11.8.2012) prepracované znenie, nariadenie Európskeho parlamentu a Rady (EÚ) č. 909/2014 z 23. júla 2014 o zlepšení vyrovnania transakcií s cennými papiermi v Európskej únii, centrálnych depozitároch cenných papierov a o zmene smerníc 98/26/ES a 2014/65/EÚ a nariadenia (EÚ) č. 236/2012 (Ú. v. EÚ L 257, 28.8.2014) v platnom znení, nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27.7.2012) v platnom znení, nariadenie Komisie (ES) č. 1287/2006/ES z 10. augusta 2006, ktorým sa vykonáva smernica 2004/39/ES Európskeho parlamentu a Rady, pokiaľ ide o povinnosti pri vedení záznamov pre investičné spoločnosti, oznamovanie transakcií, priehľadnosť trhu, prijatie finančných nástrojov na obchodovanie a vymedzené pojmy na účely tejto smernice (Ú. v. EÚ L 241, 2.9.2006). 5) Napríklad čl. 127 ods. 2 Zmluvy o fungovaní Európskej únie (Ú. v. EÚ C 202, 7.6.2016), čl. 12 ods. 12.1, čl. 22 Protokolu (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky (Ú. v. EÚ C 202, 7.6.2016) v platnom znení, § 2 zákona Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska v znení neskorších predpisov.“. Táto pripomienka je zásadná. Odôvodnenie: Účelom navrhovaného doplnenia návrhu zákona o kybernetickej bezpečnosti je vylúčiť z pôsobnosti tohto zákona platobné systémy a systémy zúčtovania a vyrovnania obchodov s finančnými nástrojmi, ako aj platobné služby (ďalej aj ako „trhové infraštruktúry“) z dôvodu, aby zákon nezasahoval do kompetencií Eurosystému v tejto oblasti. Rozšírenie pôsobnosti zákona o kybernetickej bezpečnosti na systémy prevádzkované ECB alebo Eurosystémom by znamenalo popretie prednosti úniového práva, ako aj princípu nezávislosti centrálnej banky v zmysle čl. 130 Zmluvy o fungovaní Európskej únie. Podľa čl. 127 ods. 2 Zmluvy o fungovaní Európskej únie, jednou zo základných úloh uskutočňovaných ESCB je podporovať plynulé fungovanie platobných systémov. ECB a národné centrálne banky môžu poskytnúť zariadenie a ECB môže vydávať nariadenia na zabezpečenie účinnosti a spoľahlivosti zúčtovacích a platobných systémov v rámci Únie a voči iným krajinám (čl. 22 Štatútu Európskeho systému centrálnych bánk a Európskej centrálnej banky). Aj podľa § 2 ods. 1 písm. c) zákona Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska v platnom znení, je jedným z jej hlavných cieľov podporovať plynulé a hospodárne fungovanie platobných systémov. NBS za týmto účelom vykonáva aj pôsobnosť, činnosti, úlohy, práva a povinnosti vyplývajúce z účasti a cieľov NBS v Európskom systéme centrálnych bánk (ESCB), pričom NBS ako súčasť ESCB postupuje podľa pravidiel platných pre ESCB a ako súčasť Eurosystému postupuje aj podľa pravidiel platných len pre Eurosystém. V zmysle recitálu 13 smernice NIS sú požiadavky na informačné systémy v odvetviach bankovníctva a finančných trhov stanovené vo viacerých právnych aktoch Únie často prísnejšie ako požiadavky stanovené smernicou NIS, a preto by mali byť chápané ako lex specialis, a teda by mali mať prednosť pred národnou transpozíciou smernice NIS. Taktiež, podľa recitálu 14 smernice NIS, táto smernica nemá vplyv na režim Eurosystému pre dohľad nad platobnými a zúčtovacími systémami podľa práva Únie. Z hľadiska požiadaviek na trhové infraštruktúry, vrátane zaistenia bezpečnosti, Eurosystém vychádza z medzinárodných štandardov, konkrétne zo zásad pre infraštruktúry finančného trhu (CPMI-IOSCO Principles for Financial Market Infrastructures – PFMI), ktoré Rada guvernérov ECB v roku 2013 prijala na účely dohľadu Eurosystému nad všetkými druhmi infraštruktúr finančného trhu. V júni 2016 CPMI-IOSCO vydali k PFMI doplňujúce usmernenie týkajúce sa kybernetickej odolnosti infraštruktúr finančného trhu (Guidance on cyber resilience for financial market infrastructures), ktorého požiadavky na kybernetickú bezpečnosť presahujú rámec požiadaviek smernice NIS. Systémovo dôležité platobné systémy podliehajú požiadavkám stanoveným nariadením ECB/2014/28, ktoré sa vzťahuje na systémovo dôležité platobné systémy pre veľké platby a na systémovo dôležité retailové platobné systémy prevádzkované tak centrálnymi bankami, ako aj súkromnými prevádzkovateľmi, pričom tieto systémy podliehajú viacerým právnym požiadavkám týkajúcich sa ich bezpečnosti, najmä prevádzkového rizika (čl. 15). Pokiaľ ide o ostatné platobné systémy (t. j. nie systémovo dôležité), Revidovaný rámec oversightu pre retailové platobné systémy ECB z februára 2016 uplatňuje niektoré z PFMI súvisiace s kybernetickou odolnosťou aj na tieto systémy, konkrétne princíp 2 - Správa, princíp 3 - Rámec pre ucelené riadenie rizík, princíp 8 - Konečné vyrovnanie a princíp 17 - Prevádzkové riziko. Uvedené princípy sa vzťahujú aj na systémy PIRPS (prominently important retail payment systems), medzi ktoré patrí aj platobný systém SIPS prevádzkovaný NBS, určený na klírovanie platieb malých hodnôt. Eurosystém zahŕňa pod dohľad nad platobnými systémami aj platobné služby (platobné karty, úhrady, inkasá a elektronické peniaze) a platobné schémy, keďže sú neoddeliteľnou súčasťou platobných systémov. Taktiež poskytovateľom platobných služieb, v zmysle smernice Európskeho parlamentu a Rady (EÚ) 2015/2366 o platobných službách na vnútornom trhu, ktorá bude transponovaná do právneho poriadku SR novelou zákona č. 492/2009 Z. z. o platobných službách (v súčasnosti v legislatívnom procese), sa stanovujú povinnosti hlásenia závažného prevádzkového alebo bezpečnostného incidentu, ako aj povinnosti súvisiace s prevádzkovým a bezpečnostným incidentom (§ 28d a § 28c návrhu novely zákona o platobných službách). Prevádzkové riziko vo vzťahu k činnosti centrálnych depozitárov cenných papierov upravuje nariadenie Európskeho parlamentu a Rady (EÚ) č. 909/2014 o zlepšení vyrovnania transakcií s cennými papiermi v Európskej únii (CSDR). Centrálne protistrany, ako sa vymedzujú v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 648/2012 a prevádzkovatelia obchodných miest, ako sa vymedzujú v článku 4 bode 24 smernice Európskeho parlamentu a Rady 2014/65/EÚ, taktiež podliehajú vyššie uvedeným zásadám pre trhové infraštruktúry. V nadväznosti na nami navrhovanú pripomienku je potrebné upraviť v § 2 ods. 2 označenie nasledujúcich písmen a tiež číslovanie odkazov a poznámok pod čiarou návrhu zákona. | Z | A | Text preformulovaný podľa požiadaviek aj s ohľadom na ustanovenia o mlčanlivosti. Bolo navrhnuté doplniť novelu zákona, ktorým by bolo sprístupnené bankové tajomstvo na účely hlásenia KBI a jeho riešenia. Text zákona precizovaný za spolupráci s NBS. |
| **NBS** | **k § 14, 15, 16, 17, 18, 19, 20**  33. V § 14 ods. 1 odporúčame úvodnú vetu upraviť takto: „Žiadateľ podľa § 13 ods. 2 (aj ods. 7 ?) je povinný preukázať úradu“; primerane navrhujeme spresniť aj odsek 2. Podľa § 13 ods. 2 žiadosť o akreditáciu predkladá žiadateľ, ktorý má byť prevádzkovateľom jednotky CSIRT, to znamená, že v čase podania žiadosti ešte ním nie je. 34. V § 15 ods. 2 navrhujeme slovo „majúce“ nahradiť slovami „ktoré majú“ a rovnako upraviť aj v ďalších ustanoveniach návrhu zákona. Primeraná pripomienka platí aj k § 19 ods. 5 a 6. 35. V § 15 ods. 5 navrhujeme slová „v zmysle § 13 odsek 7“ nahradiť slovami „podľa § 13 ods. 7“. 36. Znenie § 16 navrhujeme spresniť tak, aby bolo z neho zrejmé, že sa vzťahuje len na „akreditované jednotky CSIRT“. 37. V § 16 ods. 1 navrhujeme slová „reaktívne a preventívne služby“ nahradiť slovami „preventívne služby a reaktívne služby“. 38. V § 16 ods. 2 odporúčame časť úvodnej vety za slovom „incidentov“ uviesť formou písmen. 39. V § 16 navrhujeme úvodnú vetu odseku 3 upraviť takto: „(3) Reaktívne služby sa zameriavajú na riešenie ...incidentov a sú nimi najmä (prípadne formuláciu úvodnej vety a písmen zosúladiť s odsekom 2). 40. V § 17 navrhujeme spresniť čo sa myslí slovom „služba“, pretože zákon v § 3 vymedzuje len pojmy „základná služba“ a „digitálna služba“. 41. V § 17 ods. 1 odporúčame za slová „všeobecne záväzným právnym predpisom“ vložiť slová „ktorý vydá úrad podľa §.... písm. ...“. Táto pripomienka platí primerane pre celý návrh zákona (napríklad § 24 ods. 1, § 25 ods. 1, § 28 ods. 9 písm. c)). V odseku 1 je potrebné za slovom „ktorým“ doplniť slovo „je“. Pokladáme za potrebné, aby všeobecne záväzný právny predpis v súlade so splnomocňovacím ustanovením v § 33 nadobudol účinnosť súčasne so zákonom (1. január 2018), najmä vzhľadom na povinnosti ukladané Prevádzkovateľovi a Vecne príslušnej autorite v prechodných ustanoveniach upravených § 35. 42. V § 17 ods. 2 navrhujeme v písmene a) spresniť o koho názov a sídlo ide a v písmene d) odporúčame spresniť slovo „trh“. 43. V § 18 ods. 2 odporúčame poslednú vetu upraviť takto: „Dohoda tvorí neoddeliteľnú súčasť zmluvy s treťou stranou.“. 44. V § 18 ods. 3 odporúčame za slovo „túto“ doplniť slovo „službu“. 45. V § 18 ods. 4 odporúčame upraviť odkaz na § 23, ktorý je podľa nášho názoru nesprávny. 46. V § 18 ods. 7 odporúčame text za slovom „informovať“ upraviť takto: „tretiu stranu, ak si to osobitné záujmy vyžadujú.“. Primeraná pripomienka platí aj k § 21 ods. 5. 47. V § 19 ods. 1 navrhujeme slová „Bezpečnostné opatrenia predstavujú“ nahradiť slovami „Bezpečnostnými opatreniami sú“. 48. V § 20 odporúčame znenie odseku 4 začleniť do § 21. Ide o primeranú úpravu ako v § 18 ods. 5. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a zapracovaná z dôvodu úpravy text v zmysle pripomienok iných subjektov. |
| **NBS** | **k § 3**  4. V § 3 písm. d) navrhujeme upraviť znenie definície „kybernetická bezpečnosť“ a z hľadiska systematiky navrhujeme písmeno d) uviesť ako písmeno a). Odôvodnenie: Definícia kybernetickej bezpečnosti je sémanticky nesprávna. Výraz „odolávať incidentom“ je nepresný, pretože incident je už len následok „neodolania“, čiže nedostatočných bezpečnostných opatrení. Má ísť o snahu zabrániť incidentu, nie odolávať mu, je potrebné sa vyhnúť udalostiam, ktoré vedú k bezpečnostným incidentom. Okrem toho, stav kybernetickej bezpečnosti môže byť nedostatočný aj bez (indikovaných či viditeľných) incidentov. Podľa US CERT definícia znie takto: „Kybernetická bezpečnosť je stav, v ktorom sú informačné a komunikačné systémy a informácie v nich spracúvané chránené pred poškodením, neoprávneným použitím, neoprávnenou zmenou alebo zneužitím.“. 5. V § 3 písm. f) prvom bode navrhujeme slová „prelomenie integrity“ nahradiť slovami „narušenie integrity“. 6. V § 3 písm. g) navrhujeme spresniť vymedzenie pojmu „základná služba“. Z definície nie je zrejmé, čo sa myslí slovným spojením „služba, ktorá závisí od sietí a je činnosťou aspoň v jednom sektore...“ (napríklad, čo sa na účely tejto definície myslí činnosťou bánk). 7. V § 3 písm. h) navrhujeme za slovom „služby“ vypustiť slovo „sú“. 8. V § 3 písm. i) navrhujeme za slovom „službou“ vypustiť slovo „je“. 9. V poznámke pod čiarou k odkazu 8 navrhujeme na konci doplniť slová „v platnom znení“. | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy |
| **NBS** | **k § 21, 22, 23, 24, 25, 26, 27, 28** 49. V § 21 ods. 1 odporúčame začiatok prvej vety upraviť takto: „Poskytovateľ digitálnej služby je od okamihu zaradenia do registra poskytovateľov digitálnych služieb povinný ...“. Ide o primeranú úpravu ako v § 18 ods. 1. 50. V § 22 ods. 1 navrhujeme začiatok textu upraviť takto: „Zástupcom poskytovateľa digitálnej služby ja právnická osoba, ktorá má sídlo v Slovenskej republike alebo fyzická osoba - podnikateľ, ktorá má miesto podnikania v Slovenskej republike...“. 51. V § 22 ods. 2 navrhujeme pred slovo „službu“ vložiť slovo „digitálnu“ 52. V § 23 je potrebné slovo „určených“ nahradiť slovom „ustanovených“. 53. V § 24 ods. 1 odporúčame slovo „identifikuje“ nahradiť slovami „je povinný identifikovať, že ide o“. 54. V § 24 ods. 2 odporúčame za slovo „povinný“ doplniť slovo „bezodkladne“, respektíve inú vhodnú lehotu. 55. V § 24 ods. 3 sa odkazuje na hlásenie podľa odseku 1, pričom odsek 1 hlásenie neupravuje; z uvedených ustanovení tiež nie je zrejmé, komu a kedy sa má hlásenie podľa odseku 1 zasielať. 56. V § 24 ods. 4 odporúčame slovo „Pokiaľ“ nahradiť slovom „Ak“, za slovo „incidentu“ odporúčame doplniť slová „podľa odsekov 1 a 2 ?“ a slová „alebo c)“ navrhujeme nahradiť slovami „alebo písm. c)“. Primerane odporúčame spresniť aj § 25. 57. V § 27 ods. 5 odporúčame slovo „bez zbytočného odkladu“ nahradiť slovom „bezodkladne“. Ide o zosúladenie pojmu s predchádzajúcimi ustanoveniami návrhu zákona. 58. V § 28 ods. 4 odporúčame spresniť pojem „zverejnením“; ak ide o zverejnenie podľa § 10 (v Jednotnom informačnom systéme kybernetickej bezpečnosti), odporúčame v odseku 4 odkázať na § 10. Slovo „prehlásením“ je potrebné nahradiť slovom „vyhlásením“. | O | N | Vaša pripomienka nebola akceptovaná a text bol preformulovaný v zmysle Legislatívnych pravidiel vlády SR. |
| **NBS** | **k § 29** 60. V § 29 ods. 9 je potrebné spresniť, kto sa myslí pod pojmom "Príslušníci úradu“ a slovami „vedúci kontrolovaného subjektu“. Primeraná pripomienka platí aj k odseku 11. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu nahradenia novým znením textu, ktorý bol preformulovaný aj vzhľadom na pripomienky ostatných subjektov. |
| **NBS** | **k § 32,33,34** 61. V § 32 ods. 1 navrhujeme citáciu na konci odseku upraviť takto: „podľa § 17 ods.1, § 18 ods. 2, 3, 5 a 6 a § 19 ods. 6.“. 62. V § 32 navrhujeme znenie odsekov 3 a 4 upraviť tak, aby nedošlo duplicitne k uloženiu pokuty za ten istý správny delikt, ako je to napríklad za porušenie povinnosti podľa § 21 ods. 1 a 3. 63. V § 32 ods. 8 navrhujeme na konci prvej vety buď spresniť, kým je finančná pomoc poskytnutá (jej poskytovateľa), alebo slová „finančná pomoc poskytnutá“ navrhujeme nahradiť slovami „poskytnutá finančná pomoc“, bez uvedenia jej poskytovateľa. 64. V § 32 ods. 9 navrhujeme spresniť význam slovného spojenia „Ak nie je predchádzajúce účtovné obdobie k dispozícii,“. 65. Znenie § 33 je potrebné zosúladiť s bodom 24.1. Prílohy č. 1 k Legislatívnym pravidlám vlády Slovenskej republiky. 66. V navrhnutom znení § 33 písm. b) navrhujeme za slovo „hodnoty“ doplniť slovo „kritérií“; ide o zosúladenie s § 17 ods. 1 a s § 35 ods. 2 a 3. V navrhnutom písmene h) navrhujeme na konci písmena slová „písm. d)“ nahradiť slovami „písm. e)“. 67. V § 34 ods. 2 odporúčame slová „Informácie a údaje“ nahradiť slovami „Informácie, údaje a hlásenia“. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a zapraocovaná z dôvodu úpravy text v zmysle pripomienok iných subjektov. |
| **NBS** | **k § 36** 68. V § 36 navrhujeme slová „právne akty Európskej únie“ nahradiť slovami „akty Európskej únie“. Primerane je potrebné upraviť aj prílohu č. 3. | O | A |  |
| **NBS** | 69. Označovanie jednotlivých príloh je potrebné upraviť v súlade s bodom 15 Prílohy č. 1 k Legislatívnym pravidlám vlády Slovenskej republiky. | O | A |  |
| **NBS** | **k prílohe č. 1 sektor 1** 70. V prílohe č. 1 v sektore „1. Bankovníctvo“ navrhujeme, aby v kolónke PZS boli uvedené len úverové inštitúcie s odkazom na čl. 4 ods. 1 bod 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 575/2013 tak, ako je to uvedené v smernici NIS, keďže bankou môže byť, podľa právneho poriadku Slovenskej republiky, len úverová inštitúcia podľa uvedeného nariadenia. Zároveň navrhujeme do prílohy č. 1 doplniť vysvetlenie skratiek „PZS“ a „VPA“. Táto pripomienka je zásadná. | Z | A | Text upravený v novej prílohe, ktorá odzrkadľuje prílohu podľa smernice NIS, kopíruje prílohu č. 3 zo zákona o kritickej infraštruktúre a rozširuje o národné špecifiká tak, aby bola pokrytá kompletná kybernetická bezpečnosť. |
| **NBS** | **k prílohe č. 1 sektor 7** 71. V prílohe č. 1, sektor 7. Finančný sektor/Financie navrhujeme, aby pri prevádzkovateľoch obchodných miest a centrálnych protistranách bol uvedený aj odkaz na príslušný právny predpis. V prípade prevádzkovateľov obchodných miest ide o novelu zákona č. 566/2001 Z. z. o cenných papieroch, ktorá je v súčasnosti v legislatívnom procese (číslo parlamentnej tlače 499) a ktorou sa mení aj zákon č. 429/2002 Z. z. o burze cenných papierov (§ 3 ods. 3 písm. y); v prípade centrálnych protistrán ide článok 2 bod 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 648/2012. Táto pripomienka je zásadná. | Z | A | Text upravený v novej prílohe, ktorá odzrkadľuje prílohu podľa smernice NIS, kopíruje prílohu č. 3 zo zákona o kritickej infraštruktúre a rozširuje o národné špecifiká tak, aby bola pokrytá kompletná kybernetická bezpečnosť. |
| **NBS** | **II. K čl. II až X**  Návrhy zákonov je potrebné upraviť v súlade s platnými Legislatívnymi pravidlami vlády SR, napríklad v úvodnej vete čl. II odporúčame slovo „mení“ nahradiť slovom „dopĺňa“, v úvodnej vete čl. V odporúčame vypustiť slová „mení a“, v úvodnej vete čl. VIII odporúčame vypustiť slovo „a dopĺňa“, v úvodnej vete čl. IX odporúčame slová „zákona č. 351/2011 Z. z.“ vypustiť a slová „zákona č. 25/2016 Z. z.“ nahradiť slovami „zákona č. 125/2016 Z. z.“. | O | A |  |
| **NBS** | **k § 12** V § 12 ods. 2 písm. b) je potrebné spresniť slová „ten kto ju vedie“. | O | A |  |
| **NBS** | **k doložke vybraných vplyvov** V časti 9 – Vplyvy navrhovaného materiálu sa uvádza pozitívny aj negatívny vplyv na rozpočet verejnej správy, zatiaľ čo v Analýze vplyvov na rozpočet verejnej správy sú príjmy nulové. Národná banka Slovenska navrhuje zjednotiť vplyv na rozpočet verejnej správy vo všetkých častiach návrhu materiálu. | O | A |  |
| **NBS** | **k § 29** Zo znenia § 29 ods. 6 nie je zrejmé, kto sa myslí pod pojmom „Príslušníci úradu“ a ako bude možné posúdiť odbornosť ich zásahu a kto bude niesť zodpovednosť za možné následky vyvolané týmto zásahom. Žiadame vypustiť možnosť zásahu „príslušníkov úradu“ do akýchkoľvek komponentov SW a HW infraštruktúry. Táto pripomienka je zásadná. | Z | A | Text o kontrole nahradený novým textom. Sporné ustanovenia vypustené bez náhrady. |
| **OAPSVLÚVSR** | **K čl. I § 10 ods. 7** Ustanovenie navrhovaného § 10 ods. 7, zdá sa, predstavuje nepriamu novelu zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov. Žiadame zvážiť, či ide o nepriamu novelizáciu a prípadne vypustiť z čl. I návrhu. | O | A |  |
| **OAPSVLÚVSR** | **K prílohe č. 3** 1. Názov transpozičnej prílohy sa uvádza v súlade s čl. 4 ods. 3 Legislatívnych pravidiel vlády Slovenskej republiky takto: „Zoznam preberaných právne záväzných aktov Európskej únie“. Žiadame upraviť názov prílohy v súlade s Legislatívnymi pravidlami vlády Slovenskej republiky. | O | A |  |
| **OAPSVLÚVSR** | **K transpozícii smernice (EÚ) 2016.1148 (ďalej len „smernica“)** 1. V čl. 2 smernice sa vyžaduje, aby sa spracúvanie osobných údajov podľa smernice vykonávalo v súlade so smernicou Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov v platnom znení. Smernica 95/46/EHS bola transponovaná do zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. V navrhovanom § 12 ods. 7 návrhu zákona sa ustanovuje, že „Na spracúvanie osobných údajov úradom v jednotnom informačnom systéme kybernetickej bezpečnosti a na sprístupňovanie údajov sa nevzťahujú osobitné predpisy. 18)“ s odkazom na zákon č. 122/2013 o ochrane osobných údajov. Navrhované ustanovenie je v rozpore s čl. 2 smernice. Žiadame čl. 2 smernice náležite transponovať a transpozíciu preukázať v tabuľke zhody k smernici. | O | A | Text bol preformulovaný. |
| **OAPSVLÚVSR** | **K prílohe č. 3** 2. Právne záväzný akt Európskej únie sa v zozname preberaných právne záväzných aktov Európskej únie v uvádza tak, že za jeho názov sa vloží odkaz na publikačný zdroj (napríklad: Ú. v. EÚ L ..., .. .. .... dátum publikácie). V predloženom návrhu v prílohe 1. chýba pri citácii smernice odkaz na publikačný zdroj. Žiadame doplniť publikačný zdroj. | O | A |  |
| **OAPSVLÚVSR** | **K transpozícii smernice (EÚ) 2016.1148 (ďalej len „smernica“)** 2. V stĺpci 6 tabuľky zhody k smernici je k ustanoveniu čl. 5 ods. 2 smernice potrebné uviesť ustanovenie slovenského všeobecne záväzného právneho predpisu, do ktorého je ustanovenie smernice prebraté. Pre preukázanie transpozície nestačí uviesť odkaz na všeobecne záväzný právny predpis, v ktorom má byť transpozičné opatrenie obsiahnuté. | O | A | Text bol preformulovaný. |
| **OAPSVLÚVSR** | **K transpozícii smernice (EÚ) 2016.1148 (ďalej len „smernica“)** 3. Z tabuľky zhody nie je zrejmé, ktorým ustanovením slovenského právneho predpisu je ustanovená povinnosť aktualizovať zoznam identifikovaných prevádzkovateľov základných služieb do 9. novembra 2018 a potom každé dva roky, tak ako to vyžaduje ustanovenie čl. 5 ods. 5 smernice. Ustanovenie je potrebné transponovať a transpozíciu preukázať v tabuľke zhody. | O | A | Text bol preformulovaný. |
| **OAPSVLÚVSR** | **K transpozícii smernice (EÚ) 2016.1148 (ďalej len „smernica“)** 4. Z predloženej tabuľky zhody nie zrejmé, či je čl. 6 ods. 1 transponovaný, pretože v stĺpci 6 tabuľky zhody chýba príslušná právna úprava obsahujúca faktory, ktoré sa zohľadňujú pri určovaní závažnosti rušivého vplyvu. Tabuľku zhody je potrebné na tomto mieste doplniť. | O | A | Text bol preformulovaný. |
| **OAPSVLÚVSR** | **K transpozícii smernice (EÚ) 2016.1148 (ďalej len „smernica“)** 5. Na preukázanie transpozície čl. 14 ods. 4 nebude stačiť ako príslušné ustanovenie slovenského právneho poriadku uviesť navrhované splnomocňovacie ustanovenie na vydanie vykonávacieho predpisu. Transpozíciu bude potrebné preukázať konkrétnym ustanovením povinnosti zohľadniť určené parametre pri určovaní závažnosti vplyvu incidentu. Tabuľku zhody je potrebné na tomto mieste doplniť, resp. prepracovať. | O | A | Text bol preformulovaný. |
| **OAPSVLÚVSR** | **K čl. I § 13 ods. 11** Ustanovenie navrhovaného čl. I § 13 ods. 11 navrhujeme vypustiť. Subsidiarita správneho poriadku je už ustanovená v § 1 ods. 1 zákona č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov. Navrhované ustanovenie čl. I § 13 ods. 1 je subsumované v ustanovení § 1 ods. 1 správneho poriadku. | O | A |  |
| **OAPSVLÚVSR** | **K čl. I § 30 ods. 3** V návrhu je potrebné spresniť, kedy je osoba pri výkone auditu „nezávislá“ a „odborne spôsobilá“. Odporúčame podmienky nezávislosti a odbornej spôsobilosti ustanoviť v návrhu zákona. | O | A |  |
| **PMÚSR** | **celému materiálu** bez pripomienok | O | A |  |
| **RÚZSR** | **11. Pripomienka k čl. I., §19, odsek 4** § 19 ods. 4 písm. c) a d) sú duplicitné: | O | A |  |
| **RÚZSR** | **1. Všeobecná pripomienka** Materiál neobsahuje návrh vykonávacieho predpisu, na ktorý sa zákon vo veľkej miere odvoláva, čo je v rozpore s legislatívnymi pravidlami vlády. Práve tento predpis môže mať závažné negatívne dopady na priemysel. | O | A | Text bol preformulovaný. |
| **RÚZSR** | **21. Zásadná pripomienka k Prílohe č. 1** Navrhujeme vypustiť bod 9. z tabuľky. Odôvodnenie Telekomunikačný sektor nie je predmetom Smernice NIS, a to z dôvodu, že je regulovaný vlastným regulačným rámcom pre elektronické komunikácie a zákonom 351/2011, ktorý už obdobné povinnosti ukladá a zároveň spadá pod bod 7. Digitálna infraštruktúra. Telekomunikační operátori by inak podliehali dvom vecne príslušným autoritám NBÚ a MDV SR. Navyše podniky telekomunikačného sektora sú zároveň prevádzkovateľmi základných služieb aj poskytovateľmi digitálnych služieb. | Z | ČA | Na základe vznesenej pripomienky, pri rešpektovaní dohôd uzavretých s vecnými gestormi MDaV SR a ÚpREKaPŠ (aj po spoločnej dohode s MV SR a MF SR) bola formulovaná nová príloha č. 1, a to aj v rámci smernice NIS a rovnako prílohy č. 3 k zákonu o kritickej infraštruktúre. Navrhovaná úprava rovnako vychádza z akceptovania žiadosti iných pripomienkujúcich subjektov riešiť kybernetickú bezpečnosť komplexným spôsobom a pokryť všetky oblasti, pri ktorých zabezpečenie kontinuity je vzhľadom na záujmy štátu Slovenskej republiky strategické. Úrad upravil prílohu č. 1 tak, aby vylúčil podniky v zmysle 351/2011 ZZ, ktoré neposkytujú službu, ktorej zachovanie kontinuity je pre SR dôležité. Inými slovami, vzťahuje sa len na poskytovanie takej služby pre prevádzkovateľa základnej služby, ktorá je v zmysle smernice NIS a zákona považovaná za strategickú, teda základnú. Záver: Na základe vyššie uvedeného považuje úrad uvedené kompromisné riešenie za odstránenie rozporu. |
| **RÚZSR** | **17. Zásadná pripomienka k čl. I.,§ 30** Podľa názoru RÚZ audit by mal vzťahovať aj na poskytovateľa digitálnej služby, pokiaľ PZS alebo PDS nie je certifikovaný ISO 27000. | Z | N | Záver: Po vysvetlení rozpor odstránený. |
| **RÚZSR** | **2. Zásadná pripomienka k čl. I., § 3, písmeno j)**  RÚZ navrhuj uvedené ustanovenie formulovať nasledovne: (j) poskytovateľom digitálnej služby právnická osoba alebo fyzická osoba podnikateľ, ktorá poskytuje digitálnu službu a je zaradený do registra poskytovateľov digitálnych služieb | Z | N | Po vysvetlení rozpor odstránený. |
| **RÚZSR** | **15. Zásadná pripomienka RÚZ k čl. I., § 32 ods. 2 a 4** RÚZ navrhuje ponechať nominálnu hodnotu pokuty v znení: „(2) Úrad uloží pokutu až do výšky 50 000 eur prevádzkovateľovi základnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť podľa § 18 ods. 1 a 4, § 27 ods. 5 a 6 a § 30 ods. 1 alebo ak nevykoná opatrenia na nápravu v lehote podľa záverečnej správy o výsledkoch auditu.“ Odôvodnenie Navrhovaná výška pokuty 5 % z obratu je neprimeraná za neúmyselné omeškanie v nahlásení incidentu, z ktorého nemá povinný subjekt žiadny prospech a ide teda len o administratívne omeškanie. | Z | A |  |
| **RÚZSR** | **7. Zásadná pripomienka k čl. I., §13,** RÚZ navrhuje upraviť názov §13 § 13 Certifikácia Odôvodnenie Návrh je rozporuplný: SNAS by mal akreditovať úrad, ktorý následne môže certifikovať jednotlivé CSIRT. Akreditácia je potvrdením technickej spôsobilosti a certifikácia je potvrdením zhody s požiadavkami normy. Malo by ísť teda o certifikáciu, nie o akreditáciu. | Z | N | Záver: Po vysvetlení rozpor odstránený. Text predstavujú dohodu a kompromisné riešenie všetkých subjektov zúčastnených na rozporovom konaní. |
| **RÚZSR** | **9. Zásadná pripomienka k čl. I., §17, odsek 1 a 2** RÚZ navrhuje uvedené ustanovenia formulovať nasledovne: „(1) Ak prevádzkovateľ služby v sektoroch podľa prílohy č. 1 zistí, že došlo k prekročeniu prahových hodnôt kritérií ustanovených všeobecne záväzným právnym predpisom, oznámi to úradu, a to do 30 dní odo dňa, kedy prekročenie zistil. Odôvodnenie Žiadame spresniť akým spôsobom oznamovať: písomne, elektronicky, využitím jednotného informačného systému kybernetickej bezpečnosti. „(2) Oznámenie podľa odseku 1 obsahuje a) názov a sídlo, b) zoznam služieb, ktorých sa prekročenie prahových hodnôt kritérií týka, c) informáciu o možnom alebo existujúcom cezhraničnom presahu služby, d) percentuálny podiel služby na trhu, e) geografické rozšírenie služby, f) informáciu o alternatívnych možnostiach zachovania kontinuity služby v prípade kybernetického bezpečnostného incidentu, g) kontaktné údaje zástupcu podľa § 22. Odôvodnenie Tak ako pre PDS aj pre PZS by mal byt určený zástupca, resp. kontaktná osoba. Nie je jasné, ako a komu chce úrad posielať varovania a hlásenia? | Z | A | Uvedené v spoločných ustanoveniach vo verzii od MPK. |
| **RÚZSR** | **10. Zásadná pripomienka k čl. I., §18, odsek 2** RÚZ navrhuje uvedené ustanovenia formulovať nasledovne: „(2) Prevádzkovateľ základnej služby je v prípade, že rieši povinnosť prostredníctvom dodávateľa, povinný s dodávateľom na výkon činnosti pre prevádzkovateľa základnej služby (ďalej len „tretia strana“) uzatvoriť dohodu o zabezpečení plnení bezpečnostných opatrení počas celej doby platnosti zmluvy. Dohoda tvorí neoddeliteľnú súčasť zmluvy s dodávateľom na výkon činnosti pre prevádzkovateľa základnej služby. Odôvodnenie V opačnom prípade má navrhované znenie výrazný negatívny finančný dopad. Povinnosť uzatvárať dodávateľské zmluvy by nemala byť v zákone vôbec. Zodpovednosť je na Prevádzkovateľovi, a to, či rieši povinnosti dodávateľsky, je na jeho rozhodnutí. | Z | A |  |
| **RÚZSR** | **6. Zásadná pripomienka k čl. I., §11, odsek 1 písmeno d)** RÚZ navrhuje uvedené ustanovenia formulovať nasledovne: „d) spolupracuje s ostatnými vecne príslušnými autoritami a prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb vo svojej pôsobnosti pri plnení úloh podľa tohto zákona, | Z | N | Záver: Po vysvetlení rozpor odstránený. Text predstavujú dohodu a kompromisné riešenie všetkých subjektov zúčastnených na rozporovom konaní. |
| **RÚZSR** | **5. Zásadná pripomienka k čl. I., §10, odsek 5, doplnenie písmen j) a k)** RÚZ navrhuje uvedené ustanovenia formulovať nasledovne: j) prevádzkovateľ základných služieb k) poskytovateľ digitálnych služieb Odôvodnenie Ak sa má systém využívať na riadenie a riešenie kybernetických bezpečnostných incidentov, mali by mať do systému prístup všetky strany zúčastňujúce sa na riešení. | Z | N | Je obsahom návrhu textu zákona vo verzii od MPK. |
| **RÚZSR** | **4. Zásadná pripomienka k čl. I, §10 odsek 1** RÚZ navrhuje uvedené ustanovenie formulovať nasledovne: „(1) Jednotný informačný systém kybernetickej bezpečnosti je informačný systém, ktorého správcom je úrad a ktorý slúži na efektívne riadenie, evidenciu a kontrolu výkonu štátnej správy v oblasti kybernetickej bezpečnosti a jednotiek CSIRT. Jednotný informačný systém kybernetickej bezpečnosti slúži aj na spracovanie a vyhodnocovanie údajov a informácií. Odôvodnenie Na tento účel je určený EPSIS v rámci hospodárskej mobilizácie. Išlo by o konflikt napr. v oblasti krízového plánovania pre subjekty hospodárskej mobilizácie, ktoré už majú povinnosť spracovávať a vyhodnocovať údaje v inom systéme EPSIS. | Z | N | Záver: Po vysvetlení rozpor odstránený. Text predstavujú dohodu a kompromisné riešenie všetkých subjektov zúčastnených na rozporovom konaní. |
| **RÚZSR** | **12. Zásadná pripomienka k čl. I.,§ 27 ods. 4** RÚZ navrhuje uvedené ustanovenie formulovať nasledovne: (4)Povinnosť vykonať reaktívne opatrenie ukladá úrad rozhodnutím prevádzkovateľovi základnej služby alebo poskytovateľovi digitálnej služby. Za škody spôsobené obmedzením prevádzky siete zodpovedá orgán štátu, na ktorého žiadosť bola prevádzka siete obmedzená. Odôvodnenie Pri kybernetickom útoku neprichádza do úvahy čakanie na uloženie rozhodnutia o reaktívnom opatrení úradu. Z hľadiska kybernetickej bezpečnosti nie je dôvod na rozdiely medzi povinnosťami poskytovateľa digitálnej služby a prevádzkovateľov základnej služby. Núdzový stav sa vyhlasuje len na určitom postihnutom území a PDS v rámci poskytovania služieb nekoná len na určitom území. Definovanie zodpovednosti za škodu, príp. negatívny finančný dopad opatrenia, analogicky so Zákonom o elektronických komunikáciách. § 63 ods. 14 písm. d). Navrhujeme tiež spresniť, akým spôsobom bude opatrenie uložené a doručené. | Z | A |  |
| **RÚZSR** | **19. Zásadná pripomienka k čl. I.,§ 35 odsek 5** RÚZ navrhuje uvedené ustanovenie formulovať nasledovne: „(5) Osoba, ktorá sa stala prevádzkovateľom základnej služby na základe postupu podľa odsekov 2 až 4 je povinná do 24 mesiacov odo dňa účinnosti tohto zákona prijať bezpečnostné opatrenia podľa § 19. Osoba, ktorá sa stala poskytovateľom digitálnej služby na základe postupu podľa odsekov 2 alebo 4 je povinná do 24 mesiacov odo dňa účinnosti tohto zákona prijať bezpečnostné opatrenia podľa § 21.“ Odôvodnenie: Niektoré bezpečnostné opatrenia sú priamo závislé od fungovania Jednotného informačného systému. Lehota na vytvorenie Jednotného informačného systému nemôže byť totožná s lehotou na pripojenie do tohto systému (§ 19 ods. 4 písm. g - Reálne nesplniteľné vzhľadom na odsek 1). Prevádzkovatelia potrebujú dostatočnú časovú lehotu, aby sa oboznámili so systémom a pripravili sa technicky a procesne na jeho využívanie. | Z | A |  |
| **RÚZSR** | **3. Zásadná pripomienka k čl. I, §6, písmeno k)** RÚZ navrhuje uvedené ustanovenie vypustiť alebo zadefinovať ochranné opatrenie. Odôvodnenie: Časová tieseň pri kybernetických bezpečnostných incidentoch neumožňuje schvaľovanie opatrení úradom. Nevidíme dôvod, aby aj v rámci § 27 ods. 6 boli opatrenia schvaľované úradom. Ak sa podnik rozhodne, že ako opatrenie prijme napr. implementovanie IDS alebo DNS sinkole, nebolo by praktické, aby takéto kroky vopred schvaľoval úrad. Navyše ochranné opatrenie nie je definované, § 19 definuje Bezpečnostné opatrenia. | Z | N | Záver: Po vysvetlení rozpor odstránený. Text predstavujú dohodu a kompromisné riešenie všetkých subjektov zúčastnených na rozporovom konaní. |
| **RÚZSR** | **18. Zásadná pripomienka k čl. I.,§ 33, písmeno g)** RÚZ navrhuje uvedené ustanovenie vypustiť Odôvodnenie Všetky spoločnosti, ktoré riešia informačnú bezpečnosť už majú klasifikáciu informácií a kategorizáciu systémov. V každej spoločnosti je určenie priorít individuálne s ohľadom na špecifické riziká a so zreteľom na poskytovanie kľúčových služieb. Preto by zásah zo strany úradu mal výrazný a neopodstatnený negatívny dopad na interné procesy. | Z | A |  |
| **RÚZSR** | **8. Zásadná pripomienka k čl. I., §16, odsek 3 písmeno e)** RÚZ navrhuje v § 16 ods. 3 písm. e) navrhujeme definovať o aké opatrenie ide – ochranné / bezpečnostné a spresniť a definovať ich. | Z | A |  |
| **RÚZSR** | **16. Zásadná pripomienka k čl. I., § 29 ods. 8** RÚZ navrhuje v rámci transparentnosti doplniť navrhovaný odsek 8, ktorý znie: „Kontrolované subjekty sú povinné spolupracovať s úradom v súvislosti s vykonávaním kontroly a poskytovať úradu informácie, doklady, vyjadrenia a ďalšie materiály vzťahujúce sa na plnenie úloh súvisiacich s výkonom kontroly, a informácie potrebné na zabezpečenie prípravy kontroly. Kontrolované subjekty sú povinné dočasne vykonať opatrenia v rámci hardvérovej alebo softvérovej konfigurácie na základe požiadaviek úradu. Opatrenia podľa odseku 8 sa môžu uskutočňovať len v takom rozsahu, ako si to ich účel vyžaduje a nesmú viesť k ujme, ktorá je zrejme neprimeraná predpokladanému následku; za škody spôsobené obmedzením zodpovedá úrad.“ Odôvodnenie Akýmkoľvek zásahom zo strany úradu do HW a SW infraštruktúry, dôjde ku strate integrity systému, a tým prevádzkovateľ nebude schopný zabezpečiť jeho ďalšie fungovanie, tak ako ukladá zákon. Tieto zásahy môžu vyvolať negatívne dopady na poskytované služby, prípadne ich úplne znefunkčniť. Úrad v tomto prípade musí znášať kompletnú zodpovednosť za negatívne dopady. | Z | N | Záver: Po vysvetlení rozpor odstránený. Text kontroly preformulovaný a na rozporovom konaní vysvetlené postupy úrady pri vykonávaní kontroly v zmysle zákona o kontrole. |
| **RÚZSR** | **20. Zásadná pripomienka l čl. IX. Bod 4** RÚZ navrhujem do čl. IX doplniť prechodné ustanovenie – nadobudnutie účinnosti do 24 mesiacov odo dňa účinnosti tohto zákona. Odôvodnenie: Nie je doriešená riešená povinnosť počas obdobia od 1.1.2018 do sprístupnenia jednotného informačného systému. Subjekty nebudú mať kam hlásiť incidenty. | Z | N | Záver: Po vysvetlení rozpor odstránený. Text predstavujú dohodu a kompromisné riešenie všetkých subjektov zúčastnených na rozporovom konaní. |
| **RÚZSR** | **13. Zásadná pripomienka k čl. I.,§ 27 ods. 6** RÚZ v uvedenom ustanovení žiada definovať ochranné opatrenie, § 19 definuje bezpečnostné opatrenia. | Z | A |  |
| **RÚZSR** | **14. Zásadná pripomienka k čl. I., § 29 ods. 6 a 9** RÚZ žiada ods. 6 a 9 vypustiť. Odôvodnenie Akýmkoľvek zásahom zo strany úradu do HW a SW infraštruktúry, dôjde ku strate integrity systému, a tým prevádzkovateľ nebude schopný zabezpečiť jeho ďalšie fungovanie, tak ako ukladá zákon. Tieto zásahy môžu vyvolať negatívne dopady na poskytované služby, prípadne ich úplne znefunkčniť. Úrad v tomto prípade musí znášať kompletnú zodpovednosť za negatívne dopady. Pokuty je možné ukladať kontrolovanému subjektu, ale nie jeho zamestnancovi. Prinajmenšom je nutné ustanovenie zmierniť, napr. v znení: „(6) Príslušníci úradu sú v súvislosti s výkonom kontroly a v rozsahu potrebnom na jej vykonanie oprávnení nahliadať do komunikačných a informačných systémov do úrovne správcu systému.“ „(9) Príslušníci úradu sú oprávnení v súvislosti s výkonom kontroly ukladať zamestnancom kontrolovaného subjektu a vedúcemu kontrolovaného subjektu poriadkovú pokutu do 100 eur za marenie výkonu kontroly alebo neposkytnutie súčinnosti. Poriadkovú pokutu možno uložiť aj opakovane, najviac však úhrnne 500 eur.“ | Z | A | Text kontroly preformulovaný a na rozporovom konaní vysvetlené postupy úrady pri vykonávaní kontroly v zmysle zákona o kontrole. |
| **SBA** | **§12 ods. 3** § 12 ods. 3 navrhujeme vypustiť. Nevztiahnutie povinnosti zachovávať mlčanlivosť na prevádzkovateľa základnej alebo digitálnej služby považujeme za neprimerané, najmä s poukázaním na ods. 2. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že nejde o svojvoľné nakladanie s informáciami, ale práve naopak sa zabezpečí, aby orgány verejnej moci mali vždy k dispozícii informácie potrebné na konanie vo svojej pôsobnosti. |
| **SBA** | **§18 ods. 7** §18 ods. 7 navrhujeme vypustiť, alebo za slovo „ak“ doplniť slová „o tom rozhodne úrad.“ Odôvodenie: navrhované ustanovenie je vágne a ukladá prevádzkovateľovi základnej služby nešpecifikovanú povinnosť, na základe ktorej však môže byť vystavený porušeniu iných právnych predpisov. Je adekvátne očakávať, že ak vyvstane situácia predpokladaná predmetným ustanovením, úrad by mal rozhodnúť o tom, či a koho má prevádzkovateľ základnej služby informovať o kybernetickom bezpečnostnom incidente. | Z | N | Text návrhu precizovaný na rozporovom konaní, na ktorom boli zúčastnení aj zástupcovia NBS, kedy sa dospelo po vysvetlení ku konsenzu. Text naformulovaný negatívne, teda ak úrad nerozhodne inak. Po vysvetlení bol rozpor odstránený. |
| **SBA** | **§29 ods. 1** §29 ods. 1 navrhujeme vypustiť. Nie je adekvátne na výkon kontroly nad súkromnými subjektmi aplikovať základné pravidlá kontroly v štátnej správe. | Z | N | Ustanovenie o kontrole nahradené novým znením, ktoré neobsahuje rozporované ustanovenia. Na stretnutí bolo vysvetlené, ako úrad postupuje pri výkone kontroly a boli ozrejmený aj zákon o kontrole. Po vysvetlení rozpor odstránený. |
| **SBA** | **návrhu zákona** Návrh zákona neobsahuje špecifickejšie podmienky, za ktorých sa budú poskytovať prístupy do jednotlivých častí jednotného informačného systému. | O | A | Text preformulovaný, vysvetlenie v dôvodovej správe. |
| **SBA** | **návrhu zákona** Návrh zákona nereflektuje pripravovanú implementáciu GDPR. Je potrebné, aby sa hlásenie kybernetických bezpečnostných incidentov vykonávalo bez rizika porušovania iných právnych noriem, hoc pripravovaných. | O | A | Text preformulovaný. |
| **SBA** | **návrhu zákona** Návrh zákona nerieši množstvo dôležitých otázok, ktoré odsúva na možnosť vydania všeobecne záväzného právneho predpisu úradom, ktorých obsah nie je známy. To neúmerne zvyšuje právnu neistotu a bráni adekvátnemu hodnoteniu a pripomienkovaniu návrhu zákona. | O | A | Text doplnený a preformulovaný. |
| **SBA** | **návrhu zákona** Návrh zákona nerozlišuje rôzne stupne závažnosti situácie a s tým súvisiace povinnosti prevádzkovateľov základnej, alebo digitálnej služby, oprávnení úradu a druhu sankcií. Tie sú vždy rovnaké bez ohľadu na stupeň závažnosti. | O | A | Text preformulovaný. |
| **SBA** | **návrhu zákona** Návrh zákona obsahuje množstvo neurčitých a nedefinovaných pojmov (napríklad osobitný záujem). | O | A | Text preformulovaný. |
| **SBA** | **§10 ods. 6** Navrhujeme slová „ako nastane skutočnosť“ nahradiť slovami „ako získa poznatky o tom“ Odôvodnenie: Nie je adekvátne požadovať od subjektu pod hrozbou sankcie, aby poskytoval informácie bezodkladne po tom, ako nastane istá objektívna skutočnosť. Napríklad kybernetický útok môže trvať istý čas, kým sa identifikuje a rozlíši. | Z | A |  |
| **SBA** | **§18 ods. 1** Navrhujeme slová „od okamihu zaradenia“ nahradiť slovami „odo dňa doručenia rozhodnutia o zaradení“ Odôvodnenie: Prevádzkovateľ základnej služby sa nemusí dozvedieť okamžite o zaradení do registra, napriek tomu by podľa zákona mal povinnosti, ktoré sú sankcionovateľné. | Z | A |  |
| **SBA** | **§ 10 ods. 2** navrhujeme vložiť nové písmeno k: „k) zoznam subjektov s prístupom do neverejnej časti jednotného systému kybernetickej bezpečnosti.“ Odôvodnenie – zoznam subjektov nie je potrené utajovať. Pre plnenie rôznych ohlasovacích povinností vyplývajúcich z rôznych iných právnych predpisov (napríklad zákon o bankách, GDPR) je nevyhnutné poznať spracovateľa citlivých údajov, ktorý by mal byť adekvátne auditovaný. | Z | N | Pripomienka nebola akceptovaná z dôvodu, že § 10 ods. 5 vymedzuje tieto subjekty, ktoré sú zadefinované priamo v právnej norme. Po vysvetlení bol rozpor odstránený. |
| **SBA** | **§6 ods. 2** Navrhujeme vypustiť poslednú vetu. Odôvodnenie: Pre plnenie rôznych ohlasovacích povinností vyplývajúcich z rôznych iných právnych predpisov (napríklad zákon o bankách, GDPR) je nevyhnutné poznať spracovateľa citlivých údajov, ktorý by mal byť adekvátne auditovaný. Taktiež vzhľadom na povahu a silu oprávnení Úradu je odôvodnené žiadať, aby kontrolované subjekty (ak už nie verejnosť) mali vopred možnosť byť oboznámené, ktoré súkromnoprávne subjekty budú vykonávať prenesený výkon oprávnení Úradu. | Z | A | Na rozporovom konaní bol precizovaný text a vysvetlený zámer predkladateľa. Rovnako návrh zákona obsahuje novelu zákona o bankách. |
| **SBA** | **§16 ods. 3** navrhujeme vypustiť písm. b). Odôvodnenie: Nie je jasné, ako by následná investigatíva pomohla v rámci okamžitej reaktívnej služby. Rovnako nie je zrejmé, na základe akých dát bude analýza založená, nakoľko v zákone nie je priama povinnosť povinných osôb tieto údaje poskytnúť. Na základe neúplných informácií môže CSIRT alebo úrad prísť k chybným záverom a nariadiť povinným subjektom realizovať neaplikovateľné, alebo drakonické opatrenia. | Z | N | Jednotka CSIRT plní úlohy v zmysle štandardu ISO 27002.Po vysvetlení bol rozpor odstránený. |
| **SBA** | **§29 ods. 9** Navrhujeme vypustiť slová „za sťaženie výkonu kontroly alebo“. Termín sťaženie výkonu kontroly je značne vágny a vystavuje kontrolované subjekty právnej neistote. | Z | A |  |
| **SBA** | **§18 ods. 2** Navrhujeme za slovo „dodávateľom“ vložiť slová „na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov“. Odôvodnenie: predpokladáme, že predkladateľ zákona nemal záujem uložiť predmetnú povinnosť uzatvoriť dohodu o zabezpečení bezpečnostných opatrení s každým dodávateľom služieb, napríklad s kuriérskou, alebo upratovacou službou. V opačnom prípade ide o neúnosné časové a administratívne zaťaženie bez adekvátneho efektu. | Z | A |  |
| **SBA** | **§10 ods. 7** Navrhujeme za slovo „úradu“ doplniť slová „ a príslušného oznamovateľa“. Rovnako by predmetné ustanovenie malo obsahovať výnimku z predchádzajúceho písomného súhlasu úradu, ak ide o majetkovo prepojené osoby – napríklad banky a ich materské spoločnosti. | Z | N | Text vypustený bez náhrady. Po vysvetlení bol rozpor odstránený. |
| **SBA** | **§32** Pokuta až do výšky 5% celkového ročného obratu za predchádzajúci účtovný rok je likvidačná a predstavuje neúmernú hrozbu k prípadnému porušeniu povinnosti uvedených v §32 ods. 2 a ods. 4. Navrhujeme použiť iný spôsob určenia stropu výšky pokuty, napríklad pevnou sumou. | Z | A | Pokuty boli preformulované v zmysle požiadaviek |
| **SBA** | **§4 ods. 2** Pri zaisťovaní kybernetickej bezpečnosti nie je potrebné zasahovať do základných ľudských slobôd a práv | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **SBA** | **§19 ods. 1** V §19 ods. 1 nie je špecifikované, čo sa myslí pod osobitným predpisom. | O | A | Vaša pripomienka bola akceptovaná a znenie bolo vypustené. |
| **SBA** | **§29 ods. 6** V §29 ods. 6 návrh zákona dáva príslušníkom úradu rozsiahle právomoci. Aký želaný stav by sa dosiahol oprávnením vstupovať do systémov na úrovni správcu a dokonca dočasne zmeniť hardvérovú alebo softvérovú konfiguráciu sofistikovaných a komplikovaných systémov? Je takýto postup v súlade s navrhovaným §4? Akým spôsobom sa zabezpečí, že prevádzkovateľovi základnej služby nebude spôsobená škoda v dôsledku neznalosti fungovania systému? Zákon dokonca predpokladá, že výkon kontroly by bol prenesený na súkromné subjekty, ktoré by tým pádom mali právo meniť konfigurácie, a to za účelom kontroly. | Z | A |  |
| **SBA** | **§23** V§ 23 sú jednotlivé kategórie kybernetických bezpečnostných incidentov pomenované ťažkopádne a nie je zrejmé odstupňovanie závažnosti jednotlivých kategórií. Rozdiely medzi nimi sú neuchopiteľné a robia zákon nečitateľným. Ich odstupňovanie nie je možné špecifikovať až všeobecne záväzným právnym predpisom podľa §33. | O | A | Vaša pripomienka bola akceptovaná a znenie bolo vypustené. Právna úprava bola premietnutá v preformulovanej podobe s obsahom aj jednotlivých kriteriálnych parametrov v rámci § o hlásení kybernetických bezpečnostných incidentov. Parametre sú v súlade so smernicou NIS na určenie závažného kybernetického bezpečnostného incidentu. Jednotlivé kategórie sú odstupňované od závažnosti od 1 po 3, v záujme flexibilného reagovania na bezpečnostné prostredie je nevyhnutné špecifikáciu prenechať do vykonávacieho predpisu. |
| **SBA** | **§27 ods. 4** Z návrhu zákona nie je zrejmé, akým spôsobom a podľa akého právneho predpisu budú riešené opravné prostriedky voči takémuto rozhodnutiu vydanému podľa §27 ods. 4 a ako budú riešené prípadné spory. | Z | A | Text návrhu precizovaný na rozporovom konaní, na ktorom boli zúčastnení aj zástupcovia NBS, kedy sa dospelo po vysvetlení ku konsenzu. Doplnené ustanovenia o „nezodpovednosti“ PZS za škodu, ktorá vznikne pri plnení úloh podľa § 27. Škodu znáša úrad. Na zákon sa vzťahujú ustanovenia Správneho poriadku, ak v konkrétnych prípadoch nie je uvedené inak. Na miestach s touto absenciou sa následne postupuje poľa nástrojov civilného práva. Po vysvetlení bol rozpor odstránený. |
| **SBA** | **§4 ods. 3** Za slovo navrhujeme "produktoch“ doplniť slová „podľa medzinárodných štandardov“ Odôvodnenie: Deklaratórny charakter ustanovenia je vhodné doplniť aj zadefinovaním rámca v zmysle medzinárodných štandardov, podľa ktorých je nevyhnutné vytvárať prostredie kybernetickej bezpečnosti. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **SIS** | **materiálu ako celku** Slovenská informačná služba podporuje ustanovenie komplexnej úpravy týkajúcej sa problematiky kybernetickej bezpečnosti a vytvorenie funkčného legislatívneho rámca potrebného na efektívnu realizáciu kľúčových opatrení v oblasti bezpečnosti kybernetického priestoru. Hlavným cieľom navrhovanej úpravy však musí byť zaistenie bezpečného fungovania spoločenských a hospodárskych procesov s ohľadom na akceptovateľnú úroveň rizík v kybernetickom priestore, za súčasného rešpektovania hodnôt a len nevyhnutného obmedzovania slobôd používania kybernetického priestoru. Z uvedeného dôvodu je preto potrebné jednoznačne vymedziť okruh oprávnených subjektov plniacich úlohy v oblasti zaisťovania kybernetickej bezpečnosti a ich kompetencie, tak aby rešpektovali štandardný rámec realizácie bezpečnostnej politiky demokratického štátu. V tejto súvislosti Slovenská informačná služby nesúhlasí s úpravou niektorých kompetenčných vzťahov na úrovni štátnej správy v oblasti kybernetickej bezpečnosti, ktorá podľa nášho názoru výrazne zasahuje do kompetencií orgánov štátnej moci a ustanoveného systému riadenia v oblasti bezpečnostnej politiky štátu. V navrhovanom znení zákona o kybernetickej bezpečnosti dochádza k zásadnému rozšíreniu pôsobnosti Ministerstva obrany Slovenskej republiky, ktoré je v zmysle zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov, ústredným orgánom štátnej správy pre, okrem iného, riadenie a kontrolu obrany Slovenskej republiky. Navrhované rozšírenie kompetencií Ministerstva obrany Slovenskej republiky a rovnako s tým súvisiaca úprava ustanovení zákona o ozbrojených silách na účely sledovaného efektívneho zabezpečenia kybernetickej obrany tak vo svojej podstate predstavuje výrazný znak militarizácie riadenia v oblasti realizácie bezpečnostnej politiky štátu a presahuje stanovený rámec mandátu, ktorý v civilne riadenej spoločnosti patrí tomuto ústrednému orgánu štátnej správy a ozbrojeným silám Slovenskej republiky. Navrhované oprávnenia zároveň narúšajú koncept zavedený ústavným zákonom č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení neskorších predpisov, v rámci ktorého je ustanovený systém na úseku bezpečnosti štátu v čase krízových situácií, a to pri odstránení následkov ohrození bezpečnosti nevojenskej povahy a v krízových situáciách, kde ústavne zakotvené podmienky predpokladajú riešenie a odstraňovanie následkov vojenskej povahy. Ako už bolo uvedené, ochrana kybernetického priestoru je súčasťou ochrany bezpečnosti Slovenskej republiky ako takej, a teda aj spôsob výkonu štátnej moci a realizácie bezpečnostných opatrení by mal byť určený tak, aby rozdelil jednotlivé ohrozenia a prispôsobil im zodpovedajúcu pôsobnosť. | Z | A | Text bol preformulovaný. |
| **SIS** | **§ 29 ods. 6** V § 29 ods. 6 sa na konci bodka nahrádza bodkočiarkou a pripájajú sa tieto slová: „to neplatí, ak by mohlo dôjsť k ohrozeniu plnenia úloh podľa osobitného predpisu.15)“. Odôvodnenie: Vstup príslušníkov úradu do komunikačných a informačných systémov spravovaných Slovenskou informačnou službou do úrovne správcu systému a prípadná zmena hardvérovej a softvérovej konfigurácie príslušníkmi úradu by mohli ohroziť plnenie úloh podľa osobitného predpisu, alebo by mohlo dôjsť k ohrozeniu zdrojov, prostriedkov, totožnosti osôb konajúcich v prospech Slovenskej informačnej služby alebo k ohrozeniu medzinárodnej spravodajskej spolupráce. | Z | A |  |
| **SIS** | **čl. IV bod 1 písm. b)** V kontexte vyššie uvedených dôvodov by obranu štátu mal tvoriť súbor aktívnych a pasívnych opatrení zameraných na zabránenie kybernetickému útoku a zmierňovanie jeho následkov, ak takýto útok ohrozuje obranu a obranyschopnosť v kybernetickom priestore. Vo vzťahu k vykonávaniu aktívnych opatrení poukazujeme na skutočnosť, že z dotknutého ustanovenia nie je zrejmé, či tieto nezasiahnu do aplikačného záberu zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov, teda či zahŕňajú aj také technicky realizovateľné zásahy do kybernetického priestoru, ktoré z hľadiska právnej povahy zásahu možno kvalifikovať ako prelomenie ústavne garantovaného práva na súkromie. V tejto súvislosti poukazujeme na skutočnosť, že výkon aktívnych opatrení nemôže zasahovať do aplikačného záberu citovaného zákona z dôvodu duplicitného výkonu opatrení v oblasti bezpečnostnej prevencie a reakcie na bezpečnostné hrozby. Slovenská informačná služba uznáva, že takéto zásahy sú nevyhnutné na zaistenie obrany a bezpečnosti Slovenskej republiky, avšak zároveň poukazuje na skutočnosť, že podmienky za ktorých môže dôjsť k takýmto zásahom musia spĺňať zákonné podmienky ich použitia. V opačnom prípade sú takéto zásahy v demokratickom štáte neprijateľné. Výkon aktívnych opatrení, aj keď len v nevyhnutnom rozsahu, musí spĺňať kritériá proporcionality a zároveň musí byť realizovaný za podmienok výkonu externej kontroly vykonávanej ex ante, inak by vykazoval znaky právnej arbitrárnosti. Za týmto účelom právny poriadok Slovenskej republiky poskytuje vo vzťahu k takýmto zásahom zákonom garantovanú ochranu zákonnosti v podobe možnosti ich realizácie len na základe súhlasu zákonného sudcu. | Z | A | Vaša pripomienka bola akceptovaná a zapracovaná, text vypustený a preformulovaný celý čl. IV v zmysle doručených pripomienok, upravená legislatívna technika v zmysle LPV. |
| **SIS** | **čl. IX** V nadväznosti na predchádzajúcu pripomienku navrhujeme vypustiť z novelizačného čl. IX s ňou súvisiace ustanovenia. | Z | N | Vaša pripomienka nebola akceptovaná, avšak text návrhu bol prepracovaný. Po vysvetlení bol rozpor odstránený. |
| **SIS** | **čl. V bod 4** V navrhovanom § 4e ods. 1 navrhujeme vypustiť slovné spojenie „bezpečnosť alebo“, nakoľko dotknuté ustanovenie vnáša do ochrany kybernetického priestor úplný zmätok a zavádza nekonzistentnosť právnej úpravy, keďže narúša koncept civilného riadenia bezpečnostnej politiky štátu. Pôsobnosť plnenia úloh v oblasti bezpečnosti je primárne zverená do právomocí civilných bezpečnostných zložiek štátu a nie do pôsobnosti Ozbrojených síl Slovenskej republiky, resp. Ministerstva obrany Slovenskej republiky. Vo vzťahu k navrhovanému § 4e ods. 2 až 4 poukazujeme rovnako na zmätočnosť navrhovaného ustanovenia, nakoľko nielenže predstavuje legislatívne neprípustnú nepriamu novelu zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov, ale zároveň vytvára chaos z dôvodu vytvorenia duálnosti právnej úpravy obmedzenia prevádzky verejne siete alebo poskytovania verejnej služby na nevyhnutne potrebný čas a v nevyhnutnom rozsahu. Poukazujeme pritom na skutočnosť, že dikcia platného ustanovenia § 63 ods. 14 písm. d) cit. zákona už v súčasnosti ustanovuje, ak je to nevyhnutné na obranu štátu za zákonom ustanovených podmienok, možnosť realizácie predmetného oprávnenia. Predmetné oprávnenie pritom nie je limitované účelom kybernetickej obrany, ktorá ako taká predstavuje iba jednu zo zložiek obrany štátu. Uvedené navrhované ustanovenia sú kontraproduktívne aj z dôvodu zavedenia osobitného procesu rozhodovania o použití takéhoto opatrenia, ktorý v spojení s neprípustným rozšírením pôsobnosti Ozbrojených síl Slovenskej republiky aj na oblasť bezpečnosti, môže spôsobiť súbežnú realizáciu viacerých opatrení realizovaných na podnet viacerých oprávnených subjektov, avšak vo vzťahu k identickému ohrozeniu. Z uvedeného dôvodu preto navrhujeme uvedené ustanovenia vypustiť z návrhu zákona. | Z | A | Vaša pripomienka bola akceptovaná a zapracovaná, text vypustený a celý čl. V preformulovaný v zmysle doručených pripomienok, upravená legislatívna technika v zmysle LPV. |
| **SIS** | **§ 28 ods. 9 písm. b) a c)** V zmysle navrhovaného znenia ustanovenia § 28 ods. 9 Ministerstvo obrany Slovenskej republiky bude vykonávať riadenie a koordináciu výkonu štátnej správy na úseku kybernetickej bezpečnosti v čase krízovej situácie, ak kybernetický bezpečnostný incident ohrozuje systém obrany štátu a spôsobilosť zabezpečiť obranu štátu alebo ak informácie o kybernetickom bezpečnostnom incidente nasvedčujú, že kybernetický bezpečnostný incident môže byť kybernetickým terorizmom, alebo môže byť použitý ako prostriedok teroristického útoku a prijaté opatrenia neviedli k jeho odstráneniu v čase, ustanovenom pre daný typ ohrozenia alebo daný sektor všeobecne záväzným právnym predpisom. V súvislosti s ustanovením § 28 ods. 9 písm. b) poukazujeme na nejednoznačné vymedzenie kompetencií Ministerstva obrany Slovenskej republiky na uvedenom úseku, nakoľko v kontexte novelizačného čl. IV má obranu štátu tvoriť aj súbor aktívnych a pasívnych opatrení zameraných na zabránenie kybernetickému útoku a zmierňovanie jeho následkov, vrátane činností smerujúcich k vytvoreniu účinného systému obrany štátu v kybernetickom priestore, čiže de facto akémukoľvek kybernetickému útoku. Na základe systematického výkladu dotknutých ustanovení by bola Ministerstvu obrany Slovenskej republiky priznaná právomoc vykonávať štátnu správu na úseku kybernetickej bezpečnosti v čase krízovej situácie vo vzťahu k akémukoľvek bezpečnostnému incidentu. Uvedená koncepcia však narúša koncept zavedený ústavným zákonom č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení neskorších predpisov s prísnym rozlišovaním medzi prijímaním opatrení na úseku bezpečnosti štátu v čase vojny a vojnového stavu a v čase iných krízových situácií. V zmysle cit. ústavného zákona sa za krízovú situáciu nepovažuje len vojna a vojnový stav, ale aj výnimočný stav a núdzový stav, kedy pôsobnosť Ministerstva obrany Slovenskej republiky, resp. Ozbrojených síl Slovenskej republiky, zahŕňa výkon podporných činností vo vzťahu k pôsobnosti „civilných“ zložiek, tak ako to ustanovuje aj zákon č. 321/2002 Z. z. o ozbrojených silách v znení neskorších predpisov. Z uvedeného dôvodu preto navrhujeme použiť slovné spojenie „ak kybernetický bezpečnostný incident ohrozuje obranu štátu alebo obranyschopnosť štátu“. Uvedené je však prijateľné len za podmienky súčasného akceptovania pripomienky k čl. IV bod 1 písm. b). V súvislosti s ustanovením § 28 ods. 9 písm. c) poukazujeme na všeobecnosť a vágnosť dotknutého ustanovenia, ktoré rovnako umožňuje jeho nejednoznačný výklad, v dôsledku čoho bude vytvorený priestor pre vznik kompetenčných konfliktov v oblasti výkonu štátnej správy na úseku kybernetickej bezpečnosti. Slovenská informačná služba v kontexte vyššie uvedených dôvodov zastáva názor, na základe ktorého by právomoc Ministerstva obrany Slovenskej republiky, resp. Ozbrojených síl Slovenskej republiky mala zahŕňať výkon štátnej správy na uvedenom úseku v čase vojny a vojnového stavu, resp. v prípade ak kybernetický bezpečnostný incident ohrozuje obranu alebo obranyschopnosť štátu. Akýkoľvek iný koncept výkonu štátnej správy na úseku kybernetickej bezpečnosti, ktorý by priznával Ministerstvu obrany Slovenskej republiky, resp. Ozbrojeným silám Slovenskej republiky viac kompetencií v predmetnej oblasti, by predstavoval militarizáciu štátnej správy na uvedenom úseku a vymykal sa štandardom úpravy danej problematiky v členských štátoch Európskej únie a NATO. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **SIS** | **čl. IV bod 6** Z dôvodu nekonzistentnosti navrhovanej právnej úpravy Slovenská informačná služba považuje za nevyhnutnú úpravu jednotlivých ustanovení predmetného bodu, a to nasledovným spôsobom. Nakoľko ustanovenie § 7 odsek 2 vymedzuje pôsobnosť Ministerstva obrany Slovenskej republiky na úseku kybernetickej obrany je použitie slovného spojenia „v oblasti kybernetickej bezpečnosti“ v písm. b) a c) zmätočné a navodzujúce zásah do kompetencií Národného bezpečnostného úradu v zmysle § 6 návrhu zákona. Z uvedeného dôvodu je potrebné predmetné slovné spojenie zo znenia ustanovenia vypustiť. V súvislosti s navrhovanou dikciou písm. c) poukazujeme zároveň na skutočnosť, že v predchádzajúcej časti návrhu v bode 3 bol zavedený pojem „plánovanie kybernetickej obrany“, čím by dochádzalo k terminologickému nesúladu a k obsahovej neurčitosti zavádzaných pojmov. Vo vzťahu k navrhovanému odseku 4 písm. c) bod 2 uvádzame, že nemožno spochybniť úlohy Ministerstva obrany Slovenskej republiky pri plnení úloh na úseku kybernetickej obrany, toto však musí byť jednoznačne vymedzené v takom rozsahu, v akom sa predpokladá obrana kybernetického priestoru, pričom priznanie určitých kompetencií by malo byť priamo závislé od charakteru hrozby. V kontexte uvedeného je navrhované prijímanie hlásení, poskytovanie súčinnosti a koordinácia riešenia kybernetických bezpečnostných incidentov v sieťach a informačných systémoch prvkov kritickej infraštruktúry s nepriaznivým dopadom na uskutočňovanie hospodárskej a sociálnej funkcie Slovenskej republiky bez dopadu na obranu a obranyschopnosť zasahujúce do kompetencie Národného bezpečnostného úradu podľa § 6 návrhu zákona. Z uvedeného dôvodu preto navrhujeme dotknutý bod vypustiť. | Z | ČA | Text vypustený a preformulovaný celý čl. IV v zmysle doručených pripomienok, upravená legislatívna technika v zmysle LPV. |
| **SLASPO** | **K čl. I § 29 ods. 6** Ustanovenie je podľa nášho názoru formulované nejednoznačne. Z textu nie je zrejmé, u ktorých subjektov môže úrad vykonávať kontrolu vstupovaním do informačných systémov. V niektorých odstavcoch § 29 sa uvádza kontrola prevádzkovateľa základných služieb, v iných kontrola poskytovateľa digitálnych služieb. V odseku 6 je ale kontrola uvedená všeobecne, bez konkretizácie dotknutého subjektu. Je tak otázne, či takto kontrolovaným subjektom má byť akákoľvek osoba, hoci neposkytuje ani základné ani digitálne služby v zmysle definície zákona. Takto všeobecnú formuláciu v tomto prípade považujme za neprijateľnú. | O | A | Vaša pripomienka bola akceptovaná a zapracovaná. |
| **Slovensko.Digital** | **§19** V zmysle deklarovaných ambícií zákona mal zákon o kybernetickej bezpečnosti zjednotiť, resp. zastrešiť všetky povinnosti vytvárania bezpečnostnej dokumentácie a bezpečnostných opatrení, najmä podľa zákona o informačných systémoch verejnej správy, zákona o ochrane osobných údajov, zákona o kritickej infraštruktúre. Namiesto toho sa predpisujú opäť nové opatrenia, čo zásadným spôsobom zvýši administratívne zaťaženie. Žiadame tento legislatívny zámer aj v zákone realizovať. | Z | N | Na rozporovom konaní bolo vysvetlené, že úrad mal ambíciu zabezpečiť IS a dokumentácie takým spôsobom, ako uvádzate v pripomienke. V rámci rozporového konania však zazneli pochybnosti zo strany pripomienkujúcich subjektov. Budovanie IS je dohodnuté s príslušnými subjektami tak, aby sa zjednodušilo povinným osobám nahlasovanie údajov a incidentov na jednom mieste. V rámci rozporových konaní zaznela dohoda napr. s ÚOOÚ, ktorý má rovnakú ambíciu a umožní subjektom hlásiacim porušenie osobných údajov aj cez informačný systém kybernetickej bezpečnosti. Čo sa týka bezpečnostnej dokumentácie, tá v oblasti kybernetickej bezpečnosti vychádza z ISO 27002. napríklad smernica GDPR navádza bezpečnostné opatrenia ani bezpečnostnú dokumentáciu. V rámci budovania ISKB a kreovania formulárov budeme vyvíjať snahu o kooperatívny postup u zainteresovaných subjektov. Záver: Po vysvetlení rozpor odstránený. |
| **Slovensko.Digital** | **§10** Zmeniť konštrukciu §10 tak, aby bolo jednoznačné, aké evidencie/zoznamy/registre bude NBÚ viesť, aký bude ich obsah a ich prístupnosť. Odôvodnenie: Nie je jasné, čo všetko má byť obsahom neverejnej časti JISCD. Takto hrozí, že verejný záujem (na sprístupnení určitých informácií), rovnako ako aj zabezpečenie práva na informácie, nebude možné v čase schvaľovania dostatočne posúdiť. Máme za to, že zriadiť 4 nové registre nie je možné ich jednoduchým "spomenutím" ako súčasť určitého IS. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že na rozporovom konaní bolo vysvetlené, o aké zoznamy a registre ide, bolo vysvetlené fungovanie IS a jeho tvorba. Záver: Po vysvetlení rozpor odstránený. |
| **Slovensko.Digital** | **§12 ods.1** Zúžiť povinnosť mlčanlivosti iba na tie oblasti, kde je to nevyhnutné. Odôvodnenie: Povinnosť mlčanlivosti je neobvykle a neúčelne široko stanovená. Zahŕňa napr. aj požiadavku mlčanlivosti o údajoch, ktoré sú podľa §10 zverejňované. Vzhľadom na rozsah témy nie je možné v tejto pripomienke presne vymenovať potrebný rozsah mlčanlivosti, sme pripravení túto tému riešiť v rámci vysporiadania pripomienok. | Z | A | Vaša pripomienka bola akceptovaná čo do splnenia jej zamýšľaného cieľa. Bol zmenený odsek 2, v ktorom bolo vypustený účel zbavovania mlčanlivosti štatutárom, čím sa vytvoril priestor pre jednotlivé subjekty zbaviť mlčanlivosti svojich zamestnancov na úseku kybernetickej bezpečnosti z dôvodov a na účel, ktorý považujú za potrební a tak povinnosť mlčanlivosti netvorí prekážku napr. pri potrebe riešiť kybernetický bezpečnostný incident. |
| **Slovensko.Digital** | **§12 ods.7** Žiadame vypustiť tento bod Odôvodnenie: V §10 už je rozsah sprístupňovania údajov z JISCD dostatočne riešené. Nie je žiadny dôvod na výnimku z ochrany osobných údajov v zmysle príslušnej legislatívy, ktorá poskytuje dostatočné mechanizmy na umožnenie spracúvania OÚ pre JISCD potrebného. | Z | A |  |
| **Slovensko.Digital** | **§29 ods.6** Žiadame vypustiť tento odsek. Možnosť vstupovať do IS na úrovni správcu a meniť ich konfiguráciu zásadne prevyšuje možnosti potrebné na výkon kontroly a súčasne vytvára vysoké riziko narušenia činnosti a bezpečnosti týchto IS. | Z | A | Text nahradený novým textom a sporné ustanovenie odstránené bez náhrady. |
| **Slovensko.Digital** | **§29 ods.6** Žiadame vypustiť tento odsek. Možnosť vstupovať do IS na úrovni správcu a meniť ich konfiguráciu zásadne prevyšuje možnosti potrebné na výkon kontroly. | Z | A | Text nahradený novým textom a sporné ustanovenie odstránené bez náhrady. |
| **Slovensko.Digital** | **§6 ods.1 písm.m)** Žiadame vypustiť toto písmeno. Odôvodnenie: Nie je jasné, prečo má NBÚ vykonávať výskum a vývoj. Na tieto úlohy existujú iné príslušné inštitúcie - napr. akademické pracoviská na výskum. Duplicitné vykonávanie činností bude vysoko neoptimálne z hľadiska potrebných zdrojov. Znenie tejto kompetencie je nejasné a neobvykle široké. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že úrad vykonáva výskum a vývoj vo všetkých oblastiach, v ktorých vykonáva ústrednú štátnu správu. Slovo "vykonáva" bolo nahradené slovom "koordinuje" po dohode s MŠ. Záver: Po vysvetlení rozpor odstránený. |
| **SOCPOIST** | **K čl. I - k § 4**  Ak má byť ochrana kybernetického priestoru efektívna, potom jej kľúčovým prvkom je jednotné riadenie rizík a nie jeho kultúra; z uvedeného dôvodu navrhujeme zvážiť vypustenie odseku 5. Kultúra riadenia rizík nie je upravená ani v Smernici Európskeho parlamentu a Rady (EÚ) 2016/1148. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **SOCPOIST** | **K čl. I - k § 27 ods. 1** Kybernetické bezpečnostné incidenty v súčasnosti (a aj naďalej) musia riešiť predovšetkým prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb a jednotky CSIRT im v tom môžu len pomôcť. Ak nastane kybernetický bezpečnostný incident, prevádzkovateľ základnej služby ho musí riešiť bezodkladne a nemôže čakať, kým úrad uloží reaktívne opatrenie. Uvedeným postupom sa predĺži celý proces riešenia bezpečnostného incidentu, čo znamená ohrozenie informačného systému. Z uvedeného dôvodu navrhujeme znenie odseku 1 upraviť napríklad nasledovne: „(1) Riešenie bezpečnostných incidentov predstavuje najmä a) odhaľovanie kybernetických bezpečnostných incidentov, b) analyzovanie kybernetických bezpečnostných incidentov, c) implementácia nápravných bezpečnostných opatrení na odstránenie kybernetických bezpečnostných incidentov.“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že uvedený spôsob riešenia nastáva v určitých kriteriálnych rozhraniach kybernetických bezpečnostných incidentov. Samozrejme platí, že každý kybernetický bezpečnostný incident musí v prvom rade riešiť prevádzkovateľ základnej služby a jednotka CSIRT, avšak § 27 predstavuje riešenie závažných druhov kybernetických bezpečnostných incidentov, alebo riešenie incidentov, ak prevádzkovateľ základnej služby alebo jednotka CSIRT nemá schopnosť ich riešiť. |
| **SOCPOIST** | **K čl. I - k bodu § 30 ods. 2** Navrhujeme zrušiť povinnosť prevádzkovateľa zasielať úradu správu o výsledku auditu. Každý prevádzkovateľ základnej služby má svoju sektorovú vecne príslušnú autoritu, ktorá by mala mať prehľad o situácii u prevádzkovateľov v pôsobnosti svojho sektoru. Máme za to, že by išlo o neodôvodnené administratívne zaťažovanie prevádzkovateľa; ak bude úrad potrebovať výsledky auditu, môže si ich vyžiadať priamo od vecne príslušnej autority. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že kontrola a audit bezpečnostných opatrení je elementárnou súčasťou zabezpečenia kybernetickej bezpečnosti. |
| **SOCPOIST** | **K čl. I - k § 6 ods. 1** Navrhujeme zvážiť vypustenie kompetencie úradu v oblasti výskumu a vývoja, nakoľko uvedenú činnosť zabezpečujú predovšetkým výskumné ústavy a je možné využiť aj vedecké kapacity na vysokých školách. Uvedená skutočnosť vyplýva aj zo Smernice Európskeho parlamentu a Rady, podľa ktorého univerzity a výskumné centrá zohrávajú rozhodujúcu úlohu pri podnecovaní výskumu, vývoja a inovácií v týchto oblastiach. | O | A |  |
| **SOCPOIST** | **K čl. I - k § 6 ods. 2** Navrhujeme zvážiť zaradenie dohody o spolupráci uzatvorenej podľa odseku 2 medzi zmluvy ktoré sa nezverejňujú (aj zákon o kybernetickej bezpečnosti v Českej republike výslovne stanovuje povinnosť zverejnenia tejto zmluvy „Veřejnoprávní smlouva“). | O | A |  |
| **SOCPOIST** | **K čl. I - k § 18 ods. 4** Podľa návrhu zákona každý prevádzkovateľ základnej služby musí spolupracovať s konkrétnou jednotkou CSIRT. Najdôležitejšou úlohou jednotky CSIRT je pomôcť prevádzkovateľovi základnej služby s riešením kybernetického incidentu. Môže byť kontraproduktívne, ak poskytovateľ základnej služby pri riešení kybernetického incidentu musí komunikovať a plniť ďalšie povinnosti aj voči úradu, čím sa predlžuje proces riešenia incidentu; navyše za prevádzku základnej služby a za jej bezpečnosť je zodpovedný výhradne jej prevádzkovateľ. Z uvedeného dôvodu navrhujeme znenie odseku 4 upraviť napríklad nasledovne: „(4) Prevádzkovateľ základnej služby je povinný bezodkladne hlásiť kybernetický bezpečnostný incident identifikovaný podľa § 24 ods. 1 prostredníctvom jednotného informačného systému kybernetickej bezpečnosti podľa § 23, riešiť tento kybernetický bezpečnostný incident a spolupracovať s vecne príslušnou autoritou na zabezpečení kybernetickej bezpečnosti.“. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že úrad v zmysle smernice NIS plní úlohu okrem vnútroštátneho príslušného orgánu (vecne príslušný subjekt pre ochranu utajovaných skutočností) aj úlohu národného jednotného kontaktného miesta (spolupráca, cezhraničný presah incidentov) a podľa návrhu zákona je aj národnou jednotkou CSIRT. Z uvedeného nie je preto logické, aby informácie o incidentoch neboli v rámci jedného hlásenia k dispozícii orgánu, ktorý je zodpovedný za systém kybernetickej bezpečnosti na celoštátnej úrovni, čo samozrejme nevylučuje predpoklad uvedený vo Vašej pripomienke avšak bez navrhovanej legislatívnej zmeny. |
| **SOCPOIST** | **K čl. I – k § 3 písm. d)** Pojem „kybernetická bezpečnosť“ navrhujeme definovať jednoznačnejšie a vymedziť ju vo vzťahu k informačnej bezpečnosti. ISO/IEC2700 zavádza pojmy pre všetky ISO štandardy radu 27K. Informačnú bezpečnosť definuje nasledovne: Informačná bezpečnosť chráni tri hlavné vlastnosti informácií: dôvernosť, dostupnosť a integritu. S cieľom podporiť úspech biznisu, prípadne zaistiť jeho kontinuitu s minimálnymi dopadmi, aplikáciou a riadením vhodných bezpečnostných opatrení so zreteľom na širokú škálu hrozieb. Bezpečnosť informácií sa dá dosiahnuť ochranou identifikovaných aktív a to implementáciou celej rady vhodných opatrení, vybraných v procese manažmentu rizík a riadených použitím ISMS, prostredníctvom politík, procesov, procedúr, organizačných štruktúr, softvéru a hardvéru. Tieto opatrenia je potrebné vyšpecifikovať, implementovať, monitorovať, preskúmavať a zlepšovať tam, kde je to potrebné, aby sa zaistila potrebná bezpečnosť pre splnenie cieľov organizácie. ISO/IEC27001 zavádza požiadavky na vytvorenie, zavedenie, údržbu a kontinuálne zlepšovanie ISMS (systému riadenia informačnej bezpečnosti). Všetky doteraz platné legislatívne opatrenia EÚ v oblastiach ochrany informácií, sietí a komunikačných systémov dôsledne vychádzajú práve z radu ISO/IEC27K (včítane Smernice EÚ 2016/1148), preto navrhujeme kybernetickú bezpečnosť transparentne definovať a jasne vymedziť vo vzťahu k informačnej bezpečnosti. | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **SOCPOIST** | **K čl. I - k § 3 písm. c)** Poznámku pod čiarou k odkazu 3 navrhujeme upraviť, nakoľko nie je to odkaz na platnú technickú normu, ale na Nariadenie EÚ č. 1025/2012, ktorým sa stanovujú pravidlá spolupráce medzi európskymi normalizačnými organizáciami, národnými normalizačnými orgánmi, členskými štátmi a Komisiou, pravidlá tvorby európskych noriem a európskych normalizačných produktov pre výrobky a pre služby na podporu legislatívy a politík Únie, na určovanie technických špecifikácií IKT, ktoré sú oprávnené na odkazovanie, na financovanie európskej normalizácie a na účasť zainteresovaných strán na európskej normalizácii. | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **SOCPOIST** | **K čl. I - k § 12 ods. 4 a 6**  Práva a povinnosti súvisiace s ochranou osobných údajov upravené v odsekoch 4 a 6 navrhujeme rozšíriť na všetky zúčastnené subjekty, t. j. úrad, vecne príslušnú autoritu, prevádzkovateľa základnej služby a poskytovateľa digitálnej služby, nakoľko dôsledné dodržiavanie zákona č. 122/2013 Z. z. ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov je v oblasti kybernetickej bezpečnosti mimoriadne dôležité pre všetky zúčastnené strany. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že povinnosti vyplývajú každému prevádzkovateľovi osobných údajov buď priamo z nariadenia GDPR alebo z osobitných predpisov. |
| **SOCPOIST** | **K čl. I - k § 13 ods. 10**  Účelom zákona je budovať a udržiavať bezpečnosť kybernetického priestoru, preto navrhujeme zvážiť, aby akreditácia jednotky CSIRT nepodliehala povinnosti zaplatiť správny poplatok (akreditáciu jednotky CSIRT neupravuje ani Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 ani zákon o kybernetickej bezpečnosti v Českej republike). V súvislosti s uvedeným navrhujeme vypustiť aj Čl. II návrhu (novela zákona o správnych poplatkoch). | O | A |  |
| **SOCPOIST** | **K čl. I - k § 14 ods. 1** V odseku 1 navrhujeme vypustiť písmená b) až d), nakoľko ochrana kybernetického priestoru nesúvisí s ochranou utajovaných skutočností štátu, je hlavným cieľom je ochrana pred počítačovými incidentmi a to najmä pred hackerskými útokmi. V niektorých prípadoch utajovanie skutočností by práve znemožňovalo efektívnu ochranu pred novými spôsobmi hackerských útokov, ktoré by mali byť najrýchlejšie zverejňované, nie utajované. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že jednotky CSIRT v zmysle smernice NIS musia využívať infraštruktúru, ktorá je zabezpečená (príloha 1). Fyzická bezpečnosť a bezpečnosť prostredia je teda imanentnou súčasťou jednotky CSIRT, rovnako tak systém klasifikácie incidentov predpokladá existenciu utajovanej skutočnosti. Jednotka CSIRT predstavuje kanál dôvery a dôvera používateľov sa bez primeranej ochrany prostredia, v ktorom sa nachádzajú informácie nedá budovať. K druhej časti pripomienky uvádzame, že jednotka CSIRT predstavuje tím expertov, ktorý odhaľuje bezpečnostné incidenty, koordinuje a kooperuje pri ich riešení a pôsobí preventívne proti vzniku ďalších hrozieb. CSIRT je expertný orgán, ktorý poskytuje svoje služby určitej zložke alebo skupine zložiek, na ktorých ochranu je zameraný. Vymedzovanie kompetencií je preto irelevantné, jednotka CSIRT poskytuje služby a tie sú v zákone jasne definované. |
| **SOCPOIST** | **K čl. I - k Prílohe č. 1**  V prílohe sa navrhuje ako vecne príslušná autorita v sektore 8 (Verejná správa), v podsektore ISVS Národný bezpečnostný úrad. Uvedené však nie je v súlade s § 4 ods. 1 písm. f) zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy, podľa ktorého informačnú bezpečnosť informačných systémov verejnej správy riadi a koordinuje Úrad podpredsedu vlády pre investície a informatizáciu. | O | N | Určenie VPA bolo predmetom dohody NBU A ÚPVII. |
| **SOCPOIST** | **K čl. I - k § 30 ods. 1** V súvislosti s povinnosťou vykonania auditu máme za to, že by ho mala vykonať vecne príslušná autorita príslušného sektoru. Z uvedeného dôvodu navrhujeme znenie upraviť napríklad nasledovne: „(1) Prevádzkovateľ základnej služby je povinný umožniť a podrobiť sa auditu kybernetickej bezpečnosti do 24 mesiacov odo dňa zápisu prevádzkovateľa základných služieb do registra prevádzkovateľov základných služieb. Opakované audity, v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov, sa vykonávajú spôsobom podľa osobitného predpisu.32). Audity vykoná vecne príslušná autorita.“. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná - text bol preformulovaný v zmysle pripomienky. |
| **SOCPOIST** | **k čl. I - k § 3 písm. b)**  Vymedzenie pojmu „kybernetický priestor“ navrhujeme definovať spôsobom ako bolo upravené vo schválenej koncepcii kybernetickej bezpečnosti SR z roku 2015, alebo obdobne ako je v zákone o kybernetickej bezpečnosti v ČR z roku 2014; v návrhu zákona sa už v samotnom texte vymedzenia pojmu používa aj pojem kybernetický priestor, ktorý ešte nebol definovaný. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **SOCPOIST** | **K čl. I - k § 30 ods. 4**  Vzhľadom na to, že výsledky auditu sú potrebné pre externý subjekt, navrhujeme, aby náklady na audit znášala vecne príslušná autorita, nie prevádzkovateľ základných služieb. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že audit je najmä kontrolou vlastných bezpečnostných nastavení. |
| **SOCPOIST** | **K čl. I - k § 27 ods. 6 a k § 6 ods. 1**  Vzhľadom nato, že za bezpečnosť svojich systémov zodpovedá poskytovateľ základnej služby, nepovažujeme za odôvodnený postup, podľa ktorého má poskytovateľ základnej služby navrhovať úradu opatrenia na riešenie kybernetického bezpečnostného incidentu a následne čakať, kým ich úrad schváli. Navrhovaným postupom by dochádzalo aj k časovému riziku pri potrebe neodkladného riešenia kybernetického bezpečnostného incidentu. Z uvedeného dôvodu navrhujeme odsek 6 vypustiť resp. voči úradu upraviť len oznamovaciu povinnosť. V súvislosti s uvedeným navrhujeme aj v § 6 ods. 1 vypustiť písmeno k). | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že prevádzkovateľ základnej služby ako jediný subjekt v procese zabezpečenia sieti a informačných systémov má v dispozícii informačný systém, ktorý chráni a teda iba prevádzkovateľ základnej služby môže navrhnúť riešenie. Jeho schválením má zabezpečený postup administratívnej správnosti. Text bol doplnený o definovanie pojmu. |
| **ŠÚSR** | **čl. I** K §10 ods.2 písm. j) – slová „podľa §28 odsek 3“ odporúčame nahradiť slovami „podľa §28 ods. 3“. | O | A |  |
| **ŠÚSR** | **čl.I** K §10 ods.4 – slová „podľa ods. 2 písmeno j)“ odporúčame nahradiť slovami „podľa odseku 2 písm. j)“. | O | A |  |
| **ŠÚSR** | **čl. I** K §11 ods. 2 – slová „podľa ods.1 písmeno b)“ odporúčame nahradiť slovami „podľa odseku 1 písm. b)“. | O | A |  |
| **ŠÚSR** | **čl. I** K §15 ods. 5 – slová „§13 odsek 7“ odporúčame nahradiť slovami „§13 ods. 7“. | O | A |  |
| **ŠÚSR** | **čl. I** K §2 ods.2 písm. a) – slovo „utajovaných“ odporúčame nahradiť slovami „utajovaných skutočností“. | O | A |  |
| **ŠÚSR** | **čl. I** K §24 ods.4 a §25 ods.3 – slová „podľa §27 ods.1 písm. b) alebo c)“ odporúčame nahradiť slovami „podľa §27 ods.1 písm. b) alebo písm. c)“. | O | A |  |
| **ŠÚSR** | **čl. I** K §32 ods.1 – slová „§18 ods.2 a 3 a ods. 5 a 6“ odporúčame nahradiť slovami „§18 ods.2 a 3 a 5 a 6“. | O | A |  |
| **ŠÚSR** | **čl. I** K §35 ods.5 – slová „podľa odsekov 2 alebo 4“ odporúčame nahradiť slovami „podľa odseku 2 alebo odseku 4“. | O | A |  |
| **ŠÚSR** | **čl. I** K §36 a prílohe č. 3 - slová „právne záväzné právne akty“ odporúčame nahradiť slovami „právne záväzné akty“. | O | A |  |
| **ŠÚSR** | **čl.I** K §6 ods. 2 – slová „toho zákona“ odporúčame nahradiť slovami „tohto zákona“. | O | A |  |
| **ŠÚSR** | **čl. VIII** K bodom 2 a 3 – odporúčame ich spojiť do jedného bodu s touto úvodnou vetou „V §10 odseky 2 a 3 znejú:“ a v tomto zmysle upraviť aj ďalší text. Súčasne odporúčame nad slová „kybernetickej bezpečnosti“ a „ osobitného predpisu“ umiestniť správne čísla odkazov ( pravdepodobne 4a a 4b ). | O | N | Text preformulovaný. |
| **ŠÚSR** | **čl. IV** K bodu 1 - v úvodnej vete k poznámke pod čiarou odporúčame uviesť správne číslo odkazu, ktorým je odkaz 5a. | O | A |  |
| **ŠÚSR** | **čl. VIII** K bodu 1 – začiatok znenia odporúčame upraviť „V §3 písm. c) sa...“. | O | A |  |
| **ŠÚSR** | **čl. VII** K bodu 1 – začiatok znenia odporúčame upraviť „V §35 ods.2 ....“. | O | A |  |
| **ŠÚSR** | **čl. IX** K bodu 1 – začiatok znenia odporúčame upraviť „V §55 ods.6 sa...“. | O | N | Text preformulovaný. |
| **ŠÚSR** | **čl. VII** K bodu 3 – celé znenie odporúčame upraviť „V §71 ods.7 sa za slovom „vlády“ vypúšťa slovo „alebo“. | O | A |  |
| **ŠÚSR** | **čl. VII** K bodu 4 – celé znenie odporúčame upraviť „V §71 sa vypúšťa odsek 9. Doterajšie odseky 10 až 12 sa označujú ako odseky 9 až 11.“. Súčasne odporúčame zaradiť do materiálu nový bod s týmto znením „V §71 sa vypúšťajú odseky 10 a 11.“. | O | A |  |
| **ŠÚSR** | **čl. V** K bodu 4 – v §4e ods.3 odporúčame slová „podľa ods.2“ nahradiť slovami „podľa odseku 2“. | O | A |  |
| **ŠÚSR** | **čl. VII** K bodu 5 - celé znenie odporúčame upraviť „V §71a sa vypúšťa odsek 1. Doterajšie odseky 2 až 5 sa označujú ako odseky 1 až 4.“. Súčasne odporúčame zaradiť do materiálu za bod 6. nový bod s týmto znením „V §71a sa vypúšťajú odseky 3 a 4.“. | O | A |  |
| **ŠÚSR** | **čl. IV** K bodu 6 – začiatok úvodnej vety odporúčame upraviť „Doterajší text §7 sa označuje ako odsek 1 a...“. Zároveň odporúčame v texte na príslušnom mieste umiestniť aj číslo odkazu 9f, v znení poznámky pod čiarou k odkazu 9c odporúčame uviesť už iba skrátenú citáciu zákona č. 387/2002 Z. z. a v poznámke pod čiarou k odkazu 9e skrátenú citáciu zákona č. 45/2011 Z. z.. | O | N | Po dohode všetkých subjektov MOSR predloží text predmetnej novelizácie príslušného zákona. |
| **ŠÚSR** | **čl. IX** K prílohám č.1 až 3 k zákonu o kybernetickej bezpečnosti – odporúčame uviesť, že ide o prílohy k zákonu č. ..../2017 Z. z. a súčasne pri prílohách č.1 a 2 odporúčame uviesť aj ich názov. | O | A |  |
| **ŠÚSR** | **čl. II** Úvodnú vetu k čl. II odporúčame doplniť o všetky zmeny a doplnenia pôvodného právneho predpisu a v závere úvodnej vety slovo „mení“ odporúčame nahradiť slovom „dopĺňa“. | O | A |  |
| **ŠÚSR** | **čl.I** V poznámke pod čiarou k odkazu 12 odporúčame uvádzať už iba skrátenú citáciu zákona č. 319/2002 Z. z.. | O | A |  |
| **ŠÚSR** | **čl. I** V poznámke pod čiarou k odkazu 17 odporúčame uviesť celý názov zákona č. 122/2013 Z. z.. | O | A |  |
| **ŠÚSR** | **čl. I** V poznámke pod čiarou k odkazu 29 slová „321/2002 Z. z.“ odporúčame nahradiť slovami „zákon č. 321/2002 Z. z.“ | O | A |  |
| **ŠÚSR** | **čl.I** V poznámke pod čiarou k odkazu 3 odporúčame uvádzať už iba skrátené citácie zákonov č. 46/1993 Z. z. a č. 198/1994 Z. z. a v názve zákona č. 319/2002 Z. z. odporúčame za slovo „obrane“ vložiť slová „Slovenskej republiky“. | O | A |  |
| **ŠÚSR** | **čl. IX** V úvodnej vete k čl. IX odporúčame slová „zákona č. 351/2011 Z. z.“ vypustiť a slová „zákona č. 25/2016 Z. z.“ nahradiť slovami „zákona č. 125/2016 Z. z.“. | O | A |  |
| **ŠÚSR** | **čl. V** V úvodnej vete k čl. V odporúčame v závere vypustiť slová „mení a“. | O | A |  |
| **ŠÚSR** | **čl. VII** V úvodnej vete k čl. VII odporúčame pri zákone č. 215/2004 Z. z. slová „niektorých predpisov“ nahradiť slovami „niektorých zákonov“ a slová „zákona č. 392/2011 Z. z. (nepriama novela)“ vypustiť. | O | A |  |
| **ŠÚSR** | **čl. VIII** V úvodnej vete k čl. VIII odporúčame v závere vypustiť slová „a dopĺňa“. | O | N | Zmena textu. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 1. v § 2 ods. 2 písm. a) za slovo „utajovaných“ vložiť slovo „skutočností“. Odôvodnenie: legislatívno – technická pripomienka. Obyčajná pripomienka | O | A |  |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 10. v § 17 ods. 1 za slovo „prevádzkovateľ“ vložiť slovo „základnej“. Odôvodnenie: legislatívno – technická pripomienka. Obyčajná pripomienka | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že v tomto okamihu nejde o prevádzkovateľa základnej služby, ale len prevádzkovateľa služby, ktorý má povinnosť identifikovať svoju službu ako základnú. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 11. v § 17 ods. 1 za slovo „ktorým“ vložiť sloveso, napr. „je“. Odôvodnenie: legislatívno – technická pripomienka. Obyčajná pripomienka | O | A |  |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 12. podľa § 17 ods. 1 sú vyňatí správcovia informačných systémov verejnej správy. Nikde v texte návrhu zákona nie je popísaný postup ako budú títo prevádzkovatelia základnej služby registrovaní. Bez zápisu do registra prevádzkovateľov základnej služby však nebude splnená druhá podmienka podľa § 3 písm. h) návrhu zákona a nebudú môcť plniť svoje úlohy ako prevádzkovatelia základnej služby. Úrad žiada upraviť postup pre registráciu alebo iný spôsob evidovania správcov informačného systému verejnej správy ako prevádzkovateľa základnej služby. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | A | Vaša pripomienka bola akceptovaná. Bola upravená definícia prevádzkovateľ základnej služby a základná služba. Prevádzkovatelia základnej služby, ktorí prevádzkujú informačný systém verejnej správy budú do zoznamu zaradení automaticky úradom. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 13. v § 18 ods. 4 slová „podľa § 23“ nahradiť slovami „§ 10“ nakoľko ide o nesprávny odkaz. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | A |  |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 14. v § 18 ods. 7 a v § 21 ods. 5 definovať, čo sú to "tretie strany" a dokončiť vetu. Z kontextu nie je jasné, kto sú to tretie strany a zároveň ustanovenie pôsobí nedokončene. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | ČA | V návrhu zákona je legislatívna skratka "tretie strany" - "dodávateľ isvs", vysvetlené v dôvodovej správe. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 15. v § 29 ods. 6 za slová „správcu systému“ vložiť bodku a vypustiť slová „vrátane oprávnenia dočasne zmeniť hardvérovú alebo softvérovú konfiguráciu“. Odôvodnenie: vzhľadom na citlivosť údajov nachádzajúcich sa na serveroch úradu je pre úrad neprijateľné, aby v súvislosti s výkonom kontroly mali príslušníci úradu (NBÚ) možnosť a oprávnenia dočasne zmeniť hardvérovú alebo softvérovú konfiguráciu. Zásadná pripomienka | Z | A | Ustanovenie o kontrole bolo upravené. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 16. v § 29 ods. 6 za slová „oprávnení vstupovať“ vložiť slová „za prítomnosti správcu systému“. Odôvodnenie: vzhľadom na citlivosť údajov nachádzajúcich sa na serveroch úradu je pre úrad neprijateľné, aby v súvislosti s výkonom kontroly mali príslušníci úradu (NBÚ) oprávnenie vstupovať do komunikačných a informačných systémov do úrovne správcu systému bez prítomnosti správcu systému. Zásadná pripomienka | Z | A | Ustanovenie o kontrole bolo upravené. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 17. v § 30 ods. 1 prvej vete slová „do 24 mesiacov“ nahradiť slovami „do 36 mesiacov“. Odôvodnenie: úrad žiada predĺženie lehoty na podrobenie sa auditu kybernetickej bezpečnosti z 24 na 36 mesiacov z dôvodu zabezpečenia pripravenosti na audit ako i pripravenosti samotného audítora. Zásadná pripomienka | Z | A | Upravené na 24 mesiacov od zápisu do zoznamu. To ale platí pre subjekty, ktoré vzniknú po účinnosti zákona. Podľa prechodného ustanovenia bude prvý audit vykonaný do 36 mesiacov od nadobudnutia účinnosti. Účel Vašej pripomienky je teda zachovaný, ale text je upravený na mieste (prechodné ustanovenia), kam podľa legislatívnej techniky patrí. Rovnako formulovanie prechodných ustanovení je v súlade so zaužívanou legislatívnou praxou. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 18. v § 30 ods. 1 druhej vete sa upravuje realizácia opakovaných auditov bezpečnostných opatrení v rámci kybernetickej bezpečnosti vnútorným audítorom úradu (vychádzajúc z odkazu pod čiarou na zákon č. 357/2015 Z. z. o finančnej kontrole a audite). Vzhľadom na vysokú špecializáciu zamestnancov v oblasti kybernetickej bezpečnosti (dokonca im možno priznať osobitný príplatok za túto činnosť v zmysle Článku X. vlastného materiálu), úrad žiada zvážiť možnosť výkonu opakovaných auditov v dlhších časových intervaloch a v rámci možnosti buď v zmysle § 30 ods. 3 alebo zriadením centralizovanéj auditorskej jednotky pri Národnej jednotke CSIRT. Odôvodnenie: úrad upozorňuje na požiadavku vysokej špecializácie audítorov, a teda s tým spojených aplikačných problémov, ak sa predpokladá jej výkon vnútornými audítormi, čo možno predpokladať odkazom na zákon č. 357/2015 Z. z. o finančnej kontrole a audite. Rovnako tiež úrad upozorňuje, že z § 30 ods. 3 nevyplýva, že aj opakovaný audit môže byť vykonaný nezávislou, odborne spôsobilou osobou s preukázateľnou praxou v audite informačnej bezpečnosti. Zásadná pripomienka | Z | ČA | Ustanovenie o audite preformulované, uvedený odkaz odstránený. Audit budú vykonávať SNASom akreditovaní audítori z oblasti kybernetickej bezpečnosti. Záver: rozpor odstránený. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 19. v § 31 (priestupky, ktorých sa dopustí FO) úrad navrhuje vypustiť z odseku 1 písm. a) text "alebo § 18" a písmená b) až d). Úrad má zato, že ide o porušenie povinností prevádzkovateľa základnej služby (viď písm. a), b). K písm. c) má za to, že riešenie nepostupovania v súlade s prijatými opatreniami prevádzkovateľa je v kompetencii prevádzkovateľa základnej služby. Úrad upozorňuje, že môže dôjsť k rozporu so Zákonníkom práce, zákonom č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov a zákonom č. 552/2003 Z. z. o výkone práce vo verejnom záujme v znení neskorších predpisov. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | N | Vaša pripomienka nebola akceptovaná, pretože prevádzkovateľom základnej služby môže byť aj fyzická osoba. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 2. v poznámke pod čiarou k odkazu 4) vložiť text: „4) Zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov“. Odôvodnenie: podľa § 3 ods. 14 atómového zákona (s účinnosťou od 01. 08. 2017 – z. č. 96/2017 Z. z. - ide od odsek 16) „Za dokumentáciu obsahujúcu citlivé informácie sa považuje dokumentácia, ktorej zverejnenie by sa mohlo použiť na naplánovanie a vykonanie činností s cieľom spôsobiť narušenie alebo zničenie jadrového zariadenia a tým nepriaznivo ovplyvniť bezpečnosť verejnosti a spôsobiť ekologickú alebo ekonomickú škodu. Táto dokumentácia sa nezverejňuje podľa osobitného predpisu.“. Podľa § 3 ods. 15 atómového zákona (s účinnosťou od 01. 08. 2017 – z. č. 96/2017 Z. z. - ide o odsek 17) „Dokumentáciou obsahujúcou citlivé informácie sa rozumie dokumentácia uvedená v prílohe č. 1 bode A písm. c), bode B písm. a), b), i), m), bode C písm. a), d), i), j), s), w) a prílohe č. 2 bode A písm. b), bode B písm. b). Zároveň úrad zvažuje úpravu vlastnej legislatívy v tejto oblasti. Zároveň úrad podľa § 28 ods. 21 atómového zákona (s účinnosťou od 01. 08. 2017 – z. č. 96/2017 Z. z. - ide o odsek 25) disponuje údajmi potrebnými na zabezpečenie havarijnej pripravenosti, na prípravu a realizáciu cvičení, na hodnotenie nehôd alebo havárií na jadrových zariadeniach a pri preprave rádioaktívnych materiálov a na prognózu ich vývoja, ako sú technologické údaje jadrových zariadení, údaje z radiačného monitorovania, meteorologické údaje a ďalšími údajmi, ktorých ochranu je nevyhnutné zabezpečiť ako i zabezpečiť ochranu týchto údajov u držiteľa povolenia. Na základe týchto ustanovení atómového zákona úrad žiada upraviť poznámku pod čiarou k odkazu 4). Zásadná pripomienka | Z | A |  |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 20. v § 32 (pokuty voči prevádzkovateľovi základnej služby) vypustiť text "a 3" (§ 18), nakoľko v § 18 ods. 3 nie je definovaná povinnosť prevádzkovateľa základnej služby. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | A |  |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 21. k § 31 a 32 Priestupky a iné správne delikty: úrad odporúča zvážiť zníženie výšky pokút, ktoré sa javia neprimerane vysoké. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | A |  |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 22. v § 33 úrad navrhuje doplniť aj splnomocnenie na úpravu podrobností o tvorbe, obsahu a pod. politík (§ 4 ods. 3) alebo vypustiť povinnosť „rozvíjať politiky“ podľa § 4 ods. 3. Odôvodnenie: v § 33 návrhu zákona nie je upravené splnomocnenie na vydanie predmetného vykonávajúceho právneho predpisu. Obyčajná pripomienka | O | N | Vaša pripomienka nebola akceptovaná z dôvodu že ustanovenie § 4 bolo z návrhu zákona vypustené. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 23. v § 35 sú určené lehoty (6 mesiacov, resp. 18 mesiacov od účinnosti zákona), avšak plnenie povinností vyplývajúcich z tohto ustanovenia sú naviazané na vykonávajúce právne predpisy, ktoré nemajú určenú lehotu na ich zverejnenie v Zbierke zákonov Slovenskej republiky a ani ich text nebol prílohou tohto materiálu. Z uvedeného dôvodu úrad odporúča, aby text "odo dňa účinnosti tohto zákona" bol nahradený napr. textom "odo dňa nadobudnutia účinnosti príslušného vykonávacieho právneho predpisu podľa § 33". Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | A |  |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 24. v § 35 ods. 2 prvej vete za slovo „Prevádzkovateľ“ vložiť slovo „základnej“. Odôvodnenie: legislatívno – technická pripomienka. Obyčajná pripomienka | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že prevádzkovateľ služby sa stane prevádzkovateľom základnej služby až po zápise do registra. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 25. v § 35 ods. 2 sa popisuje spôsob a lehoty podania oznámenia prevádzkovateľa základnej služby, ak prevádzkovateľ zistil prekročenie prahových hodnôt kritérií. Nikde v texte návrhu zákona však nie je definované, akú má lehotu na podanie oznámenia prevádzkovateľ už existujúcej základnej služby podľa prílohy č. 1 návrhu zákona. Pokiaľ však nebudú uvedení v registri prevádzkovateľov základnej služby (druhá podmienka § 3 písm. h)), nebudú môcť byť prevádzkovateľom základnej služby. Žiadame doplniť prechodné ustanovenie pre oznámenie prevádzkovateľa základnej služby podľa prílohy č. 1. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | A |  |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 26. v § 35 ods. 5 slová „do 18 mesiacov“ nahradiť slovami „do 24 mesiacov“. Odôvodnenie: úrad požaduje predĺženie lehoty na splnenie povinnosti vyplývajúcej z predmetného ustanovenia s poukazom aj na skutočnosť, že nie je určená lehota na vydanie vykonávacích predpisov (podľa § 33), ktorých vydanie bezprostredne súvisí s plnením povinností vyplývajúcich pre prevádzkovateľa základnej služby. Zásadná pripomienka | Z | A |  |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 27. všeobecne k materiálu: úrad má za to, že súčasťou predloženého materiálu mal byť základný popis vykonávacích právnych predpisov, resp. ich znenie. Odôvodnenie: legislatívno – technická pripomienka Obyčajná pripomienka | O | A | Text preformulovaný, tézy vykonávacích predpisov budú súčasťou schvaľovania aj dôvodovej správy, do účinnosti zákona sa predpokladá prijatie vykonávacích predpisov. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 28. V Prílohe č. 1 úrad odporúča nepoužívať skratky „PZS“ a VPA“ bez zavedenia legislatívnej skratky. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | A |  |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 29. V Prílohe č. 2 úrad odporúča namiesto pojmu "CLOUD computing" zaviesť náležitý slovenský ekvivalent. Odôvodnenie: právne normy majú osobitný význam pri tvorbe terminológie. Obyčajná pripomienka | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že pojem "CLOUD computing" je nezameniteľný a zaužívaný v celej EÚ. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 3. k § 3: úrad žiada doplniť definíciu pojmu "prahové hodnoty pre identifikáciu základnej služby". Odôvodnenie: podľa § 17 ide o dôležitý údaj, podľa ktorého sa oznamujú základné služby. Nikde v celom návrhu zákona sa tento pojem nevysvetľuje, ani bližšie nedefinuje. Na základe splnomocňovacieho ustanovenia v § 33 bude vydaný všeobecne záväzný právny predpis, ktorý upraví prahové hodnoty, ale tým, že sa tento pojem používa v návrhu zákona, je žiadúce, aby pojem bol definovaný už priamo v zákone. Zásadná pripomienka | Z | N | Úrad ustupuje od zásadnej pripomienky zároveň však upozorňuje, že prahové hodnoty sú závažný pojem pre optimálne napĺňanie povinností vyplývajúcich z návrhu zákona a chýba návrh vykonávacieho predpisu, ktorý by stanovoval kritéria pre tieto prahové hodnoty a na ktoré sa odvoláva NBÚ vo svojom stanovisku. Problémom však je, že vzhľadom na uvedené nie je možné posúdiť zosúladenie požiadaviek návrhu zákona s návrhom vyhlášky, keďže táto nebola priložená v rámci medzirezortného pripomienkového konania. Záver: Po vysvetlení rozpor odstránený. |
| **ÚJDSR** | **II. K doložke vybraných vplyvov** 30. V zmysle predloženého návrhu zákona bude pravdepodobne aj úrad poskytovateľom základnej služby, ktorý ako taký bude musieť plniť celý rad úloh v súvislosti s preventívnymi činnosťami (vypracovanie bezpečnostnej dokumentácie, jej aktualizácia, vykonávanie auditu /§ 30 ods. 1 a 4/, aplikácia bezpečnostných opatrení a štandardov), reaktívnymi činnosťami, notifikačnými povinnosťami, vzdelávaním a pod. Realizácia týchto činností si vyžiada aktívne technické, organizačné i personálne opatrenia, ktoré v návrhu nie sú vyčíslené a nie je zabezpečené ich financovanie. Tieto činnosti nebudú mať charakter dobrovoľnosti, ale povinností. V tomto momente ich rozsah ani nie je možné stanoviť detailnejšie, keďže nie je známy návrh vyhlášky k prahovým hodnotám kritérií. V tejto súvislosti úrad na rok 2017 síce získal zvýšenie limitu zamestnancov o 2 osoby, ktorí sú určení na riešenie úloh v oblasti kybernetickej bezpečnosti, ale v rámci rozpočtu na roky 2018-2020 nie je návrhom zákona zabezpečené financovanie technických, organizačných i personálnych nárokov na implementáciu povinností v zmysle predloženého návrhu zákona (a to ani limit počtu zamestnancov zvýšený o dve osoby). Predkladacia správa síce uvádza, že "návrh zákona komplexným spôsobom poníma problematiku riešenia a zabezpečovania kybernetickej bezpečnosti. Vytvára konkurenčné prostredie v oblasti zamestnávania kvalifikovaných pracovníkov na strane štátu....", o čom svedčí snaha novelizovať zákon o štátnej službe s možnosťou poskytovania osobitného príplatku, avšak v rozpore s tým je doložka vybraných vplyvov v ktorej sa uvádza, že financovanie návrhu je zabezpečené v rámci limitov rozpočtu na jednotlivé roky s tým, že nie je možné identifikovať subjekty verejnej správy, o ktoré ide. Pripomienkou úradu je: Ak nie je možné kvantifikovať finančný dopad na subjekty verejnej správy, je potrebné aspoň identifikovať o aké subjekty ide a z akých zdrojov finančný dopad bude krytý v ich rozpočtoch, t. j. či pôjde o financovanie z medzirezortného programu, vyčlenenie prostriedkov v rozpočte v zvlášť vykazovanej položke v rozpočte subjektu a pod. Dopady návrhu predloženého zákona pre subjekty verejnej správy je možné kvantifikovať personálne, ale aj cez potrebu technických prostriedkov realizácie opatrení, ako aj cez náklady na organizačné opatrenia. Sú to náklady, ktoré napríklad úrad nie je schopný kryť v rámci existujúcich zdrojov bez navýšenia rozpočtu. Nehovoriac o tom, že neplnenie povinnosti v zmysle návrhu zákona je sankcionované pokutou až do výšky 30.000,- eur. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Zásadná pripomienka | Z | A |  |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 4. k § 10 ods. 2: úrad odporúča zvážiť zverejňovanie jednotlivých položiek definovaných v písmenách a) až j) z dôvodu, aby zbytočne neboli zverejnené jednotlivé registre, resp. metodiky, usmernenia a informácie (napr. ide o písmená b), c) h) i)) z dôvodu možného zneužitia. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že úrad po zvážení pripomienky trvá na predmetnom ustanovení v navrhovanej podobe. Obava zo zneužitia je neopodstatnená, keďže vo verejnej časti nebudú zverejnené žiadne utajované skutočnosti ani osobné údaje, či iné citlivé informácie. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 5. k § 10 ods. 5: úrad odporúča zvážiť definovanie (v obsahových črtách), čo tvorí neverejnú časť jednotného informačného systému kybernetickej bezpečnosti, nakoľko to nie je vôbec v návrhu zákona upravené. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že úrad po zvážení pripomienky trvá na predmetnom ustanovení v navrhovanej podobe. Obava zo zneužitia je neopodstatnená, keďže vo verejnej časti nebudú zverejnené žiadne utajované skutočnosti ani osobné údaje. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 6. k § 10 ods. 5: úrad odporúča zvážiť bližšie konkretizovanie pojmu „partneri Národnej jednotky CSIRT“. Ak ide o partnerov na základe dohody o spolupráci (§ 7 ods. 2), bolo by žiadúce doplniť odkaz pod čiarou na uvedenú dohodu. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že partneri Národnej jednotky CSIRT boli z textu vypustení. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 7. k § 12: úrad odporúča zvážiť, či § 12 ods. 3 nie je v rozpore s § 12 ods. 1, resp. 2 a aj vo vzťahu k zamestnancovi prevádzkovateľa základnej služby. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | A |  |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 8. k § 12 ods. 7: úrad odporúča riešiť aj otázky ochrany osobných údajov v jednotnom informačnom systéme a ich podmienky, ktoré je potrebné subjektom s prístupom k týmto údajom poskytnúť, keďže v zmysle zákona č. 122/2013 Z. z. o ochrane osobných údajov v znení neskorších predpisov nie je v predloženom návrhu zákona riešená otázka poskytovania osobných údajov (napr. úrad ako prípadný prevádzkovateľ základnej služby s prístupom do JIS kybernetickej bezpečnosti, ktorý je v zmysle zákona č. 122/2013 Z. z. automaticky "prevádzkovateľom informačného systému" obsahujúceho osobné údaje). Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Obyčajná pripomienka | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ochranu osobných údajov prostredníctvom nástrojov zabezpečujúcich údaje v jednotnom informačnom systéme kybernetickej bezpečnosti je na vyššej bezpečnostnej úrovni ako to definuje GDPR, teda práve naopak GDPR neposkytuje takú vysokú mieru ochrany. To samozrejme nevylučuje, že na ostatné subjekty v rámci systému ochrany osobných údajov sa GDPR nevzťahuje. |
| **ÚJDSR** | **I. K vlastnému materiálu Čl. I.** 9. vypustiť § 15 ods. 5. Odôvodnenie: úrad požaduje vypustenie predmetného ustanovenia z dôvodu, že ponechaním uvedeného ustanovenia by jednotka CSIRT akreditovaná podľa § 13 ods. 7 nemala žiadne oprávnenia podľa predloženého materiálu. Zásadná pripomienka | Z | A |  |
| **ÚNMSSR** | **celému materiálu** bez pripomienok | O |  |  |
| **UOOU SR** | **K čl. I ako celku** K čl. I ako celku Požadujeme vysvetlenie úmyslu oznamovať porušenia ochrany osobných údajov cez JISKB, tak ako to je nepriamo spomenuté v návrhu zákona a priamo v dôvodovej správe k návrhu zákona(str. 5 dole, alebo k § 12 dôvodová správa osobitná časť). Táto pripomienka je zásadná Odôvodnenie: Návrh zákona vo svojom texte iba nepriamo a pomerne nejasne naznačuje, že aj hlásenia prevádzkovateľa o porušení ochrany osobných údajov podľa čl. 33 nariadenie EU 2016/679 by mohli byť vykonávané cez JISKB. Priamo návrh je obsiahnutý iba v osobitnej časti dôvodovej správy k zákonu. Požadujeme vyjasnenie a celkové spresnenie vykonávania týchto oznámení cez JISKB v prípade, ak by boli vykonávané prostredníctvom JISKB. | Z | A | Návrh zákona o KB určuje minimálne bezpečnostné štandardy zabezpečenia kvality sietí a informačných systémov v pôsobnosti subjektu, ktorý je pomocou určených kritérií určený ako "kritický" vo vzťahu k zabezpečeniu a udržaniu úloh štátu. Hlásenie KBI je jedným zo základných nástrojov zabezpečovania monitorovania a riešenia narušenia sietí a informačných systémov. Toto hlásenie sa realizuje prostredníctvom informačného systému, ktorý vybuduje úrad. Informačný systém bude obsahovať moduly a funkcionality uvedené v zákone. V zákone nemožno uviesť, ako technicky bude systém vyzerať, ide o konštrukčnú záležitosť na úrovni IT, avšak spôsobilosť informačného systému tak, ako je uvedené v zákone, bude zabezpečená. Verejnosť od začiatku polemík o zákone o KB apelovala na zjednodušenie prístupu povinných subjektov k naplneniu ich povinností vyplývajúcich z rôznych zákonov (nielen zákon o OOU, ale aj zákon o kritickej infraštruktúre, telekomunikačný zákon, zákon o bankách), čím sa zníži administratívna zaťaženosť subjektov a zvýši sa ich ochota hlásiť incidenty. Preto je vybudovanie jedného "kanálu" pre hlásenie incidentov pochádzajúcich z porušenie rôznych zákonov legitímnou požiadavkou. Treba si uvedomiť, že ide o vybudovanie jedného kanálu, nie o vybudovanie jednej databázy. Hlásenie skončí vždy u subjektu, ktorý je povinný ho spracovávať a riešiť. Uvedené bolo vysvetlené aj na rozporovom konaní k novému zákonu o OOU, s čím úrad vyslovil súhlas a nemal námietky, aby jeden zo spôsobov hlásenia incidentov na úseku OOU bol aj informačný systém zo zákona o KB. Na tejto báze je teda postavený aj prístup k neverejnej časti - teda prístup i nahlásených informáciám týkajúcich sa konkrétneho subjektu. Poskytovanie údajov z tejto neverejnej časti môže úrad "otvoriť" len v prípade verejného záujmu. V snahe predísť obštrukciám pri riešení závažných otázok týkajúcich sa zabezpečenia základných úloh štátu je potrebné uviesť takúto úpravu priamo do zákona. V uvedení súvislosti úrad na ochranu osobných údajov v súlade s nariadením o GDPR, kedy je možné v záujme bezpečnosti uplatniť podmienky obmedzenia. To iste nevylučuje, že úrad bude chrániť osobné údaje spôsobom akým mu to nariadenie určuje. Tu treba uviesť, že všetky údaje v JISKB budú užívať ochranu vyššou mierou bezpečnosti nástrojov, ako ustanovuje dokonca samotné GDPR, keďže systém bude utajovaný (rovnaký princíp je uplatnený aj v rámci spracovania osobných údajov v zmysle zákona č. 215/2004 Z. z., kde sú osobné údaje chránené v systéme, ktorý je utajovaný, čo bolo rovnako vysvetlené a akceptované UOOU na rozporovom konaní k zákonu o OOU). |
| **UOOU SR** | **K Čl. I k § 10 ods. 2** K Čl. I k § 10 ods. 2 Požadujeme spresnenie a vymedzenie fungovania jednotného informačného systému kybernetickej bezpečnosti s ohľadom na to, ktoré hlásenia majú byť vykonávané prostredníctvom tohto systému. Táto pripomienka je zásadná. Odôvodnenie: Jednotný informačný systém kybernetickej bezpečnosti (ďalej len „JISKB“) obsahuje komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania. Z navrhovaného znenia nie je zrejmé, či súčasťou tohto systému nahlasovania kybernetických incidentov má byť aj nahlásenie podľa čl. 33 nariadenia EU 2016/679 (ďalej len „nariadenie“), ktoré je povinný vykonať prevádzkovateľ Úradu na ochranu osobných údajov SR (ďalej len „UOOU“). Z navrhovaného znenia tiež nie je zrejmé, či súčasťou tohto systému nahlasovania kybernetických incidentov má byť aj nahlásenie podľa navrhovaného znenia zákona o ochrane osobných údajov (toho času v PPK), ktoré bude povinný vykonať prevádzkovateľ UOOU. V prípade, ak tomu tak je, tak na základe nariadenia, a ani na základe návrhu zákona o ochrane osobných údajov nie je stanovená povinnosť zverejňovania konkrétneho „kybernetického bezpečnostného incidentu“, teda automatická zverejňovanie porušenia ochrany osobných údajov, ak sa bude nahlasovať do JISKB, namietame. Zo znenia navrhovaného ustanovenia nevyplýva, že by sa zverejňovanie kybernetických útokov malo nejak členiť, teda ak by dochádzalo na základe nahlásenia porušenia ochrany osobných údajov úradu (podľa čl. 33 nariadenia, alebo zákona o ochrane osobných údajov) k zverejneniu prevádzkovateľa automaticky považujeme takéto zverejnenie nesúladné s nariadením aj so zákonom o ochrane osobných údajov. | Z | N | Bezpečnostné štandardy zabezpečenia kvality sietí a informačných systémov v pôsobnosti subjektu, ktorý je pomocou určených kritérií určený ako "kritický" vo vzťahu k zabezpečeniu a udržaniu úloh štátu. Hlásenie KBI je jedným zo základných nástrojov zabezpečovania monitorovania a riešenia narušenia sietí a informačných systémov. Toto hlásenie sa realizuje prostredníctvom informačného systému, ktorý vybuduje úrad. Informačný systém bude obsahovať moduly a funkcionality uvedené v zákone. V zákone nemožno uviesť, ako technicky bude systém vyzerať, ide o konštrukčnú záležitosť na úrovni IT, avšak spôsobilosť informačného systému tak, ako je uvedené v zákone, bude zabezpečená. Verejnosť od začiatku polemík o zákone o KB apelovala na zjednodušenie prístupu povinných subjektov k naplneniu ich povinností vyplývajúcich z rôznych zákonov (nielen zákon o OOU, ale aj zákon o kritickej infraštruktúre, telekomunikačný zákon, zákon o bankách), čím sa zníži administratívna zaťaženosť subjektov a zvýši sa ich ochota hlásiť incidenty. Preto je vybudovanie jedného "kanálu" pre hlásenie incidentov pochádzajúcich z porušenie rôznych zákonov legitímnou požiadavkou. Treba si uvedomiť, že ide o vybudovanie jedného kanálu, nie o vybudovanie jednej databázy. Hlásenie skončí vždy u subjektu, ktorý je povinný ho spracovávať a riešiť. Uvedené bolo vysvetlené aj na rozporovom konaní k novému zákonu o OOU, s čím úrad vyslovil súhlas a nemal námietky, aby jeden zo spôsobov hlásenia incidentov na úseku OOU bol aj informačný systém zo zákona o KB. Na tejto báze je teda postavený aj prístup k neverejnej časti - teda prístup i nahlásených informáciám týkajúcich sa konkrétneho subjektu. Poskytovanie údajov z tejto neverejnej časti môže úrad "otvoriť" len v prípade verejného záujmu. V snahe predísť obštrukciám pri riešení závažných otázok týkajúcich sa zabezpečenia základných úloh štátu je potrebné uviesť takúto úpravu priamo do zákona. V uvedení súvislosti úrad na ochranu osobných údajov v súlade s nariadením o GDPR, kedy je možné v záujme bezpečnosti uplatniť podmienky obmedzenia. To iste nevylučuje, že úrad bude chrániť osobné údaje spôsobom akým mu to nariadenie určuje. Tu treba uviesť, že všetky údaje v JISKB budú užívať ochranu vyššou mierou bezpečnosti nástrojov, ako ustanovuje dokonca samotné GDPR, keďže systém bude utajovaný (rovnaký princíp je uplatnený aj v rámci spracovania osobných údajov v zmysle zákona č. 215/2004 Z. z., kde sú osobné údaje chránené v systéme, ktorý je utajovaný, čo bolo rovnako vysvetlené a akceptované UOOU na rozporovom konaní k zákonu o OOU). Rozpor bol odstránený. |
| **UOOU SR** | **K Čl. I k § 10 ods. 5** K Čl. I k § 10 ods. 5 Požadujeme objasnenie toho, ktorý subjekt a v akom rozsahu má mať prístup do neverejnej časti JISKB. Táto pripomienka je zásadná. Odôvodnenie: V návrhu zákona je prístup subjektov v odseku 5 limitovaný vecnou pôsobnosťou a tým, ako prístup do systému bude určovať úrad. Namietame také určovanie prístupu subjektov podľa ods. 5, kedy by k hláseniam úradu podľa čl. 33 nariadenia a podľa návrhu zákona o ochrane osobných údajov mal mať prístup bez vedomia úradu iný subjekt. Nakoľko sa oznámenie porušenia ochrany osobných údajov podľa čl. 33 nariadenia a podľa navrhovaného zákona o ochrane osobných údajov oznamuje úradu, v prípadoch, keď to nie je nevyhnutné nevidíme dôvod, aby do systému hlásení podľa ustanovení vyššie uvedených mal mať prístup iný subjekt. Taktiež vymedzenie a ustanovenie prístupu do JISKB na základe „v rozsahu určenom úradom“ nie je pojem a určovanie mechanizmu prístupu úradom jasné, požadujeme preto jeho vysvetlenie/spresnenie. | Z | N | Návrh zákona o KB určuje minimálne bezpečnostné štandardy zabezpečenia kvality sietí a informačných systémov v pôsobnosti subjektu, ktorý je pomocou určených kritérií určený ako "kritický" vo vzťahu k zabezpečeniu a udržaniu úloh štátu. Hlásenie KBI je jedným zo základných nástrojov zabezpečovania monitorovania a riešenia narušenia sietí a informačných systémov. Toto hlásenie sa realizuje prostredníctvom informačného systému, ktorý vybuduje úrad. Informačný systém bude obsahovať moduly a funkcionality uvedené v zákone. V zákone nemožno uviesť, ako technicky bude systém vyzerať, ide o konštrukčnú záležitosť na úrovni IT, avšak spôsobilosť informačného systému tak, ako je uvedené v zákone, bude zabezpečená. Verejnosť od začiatku polemík o zákone o KB apelovala na zjednodušenie prístupu povinných subjektov k naplneniu ich povinností vyplývajúcich z rôznych zákonov (nielen zákon o OOU, ale aj zákon o kritickej infraštruktúre, telekomunikačný zákon, zákon o bankách), čím sa zníži administratívna zaťaženosť subjektov a zvýši sa ich ochota hlásiť incidenty. Preto je vybudovanie jedného "kanálu" pre hlásenie incidentov pochádzajúcich z porušenie rôznych zákonov legitímnou požiadavkou. Treba si uvedomiť, že ide o vybudovanie jedného kanálu, nie o vybudovanie jednej databázy. Hlásenie skončí vždy u subjektu, ktorý je povinný ho spracovávať a riešiť. Uvedené bolo vysvetlené aj na rozporovom konaní k novému zákonu o OOU, s čím úrad vyslovil súhlas a nemal námietky, aby jeden zo spôsobov hlásenia incidentov na úseku OOU bol aj informačný systém zo zákona o KB. Na tejto báze je teda postavený aj prístup k neverejnej časti - teda prístup i nahlásených informáciám týkajúcich sa konkrétneho subjektu. Poskytovanie údajov z tejto neverejnej časti môže úrad "otvoriť" len v prípade verejného záujmu. V snahe predísť obštrukciám pri riešení závažných otázok týkajúcich sa zabezpečenia základných úloh štátu je potrebné uviesť takúto úpravu priamo do zákona. V uvedení súvislosti úrad na ochranu osobných údajov v súlade s nariadením o GDPR, kedy je možné v záujme bezpečnosti uplatniť podmienky obmedzenia. To iste nevylučuje, že úrad bude chrániť osobné údaje spôsobom akým mu to nariadenie určuje. Tu treba uviesť, že všetky údaje v JISKB budú užívať ochranu vyššou mierou bezpečnosti nástrojov, ako ustanovuje dokonca samotné GDPR, keďže systém bude utajovaný (rovnaký princíp je uplatnený aj v rámci spracovania osobných údajov v zmysle zákona č. 215/2004 Z. z., kde sú osobné údaje chránené v systéme, ktorý je utajovaný, čo bolo rovnako vysvetlené a akceptované UOOU na rozporovom konaní k zákonu o OOU). Rozpor bol odstránený. |
| **UOOU SR** | **K Čl. I k § 10 ods. 7** K Čl. I k § 10 ods. 7 Požadujeme odstránenie podmienky na informovanie o údajoch a informáciách, o ktorých sa subjekt v odseku 5 dozvedel v rámci neverejnej časti, aby ich mohol poskytovať alebo zverejňovať iba so súhlasom úradu. Požadujeme vypustenie práva úradu, aby mohol informácie získané z neverejnej časti JISKB , týkajúce sa povinnosti nahlasovať porušenie ochrany osobných údajov UOOU zverejniť, a to bez jeho informovania alebo súhlasu. Táto pripomienka je zásadná. Odôvodnenie: Ustanovený návrh zákazu poskytovania alebo informovania o informáciách, o ktorých sa subjekt dozvedel, iba so súhlasom úradu je pre UOOU neprijateľný, nakoľko je v rozpore s čl. 58 ods. 2 písm. e) nariadenia a s navrhovaným znením návrhu zákona o ochrane osobných údajov v príslušnom ustanovení. Na základe čl. 58 ods. 2 písm. e) nariadenia a na základe navrhovaného znenia návrhu zákona o ochrane osobných údajov UOOU, ako dozorný orgán v oblasti ochrany osobných údajov, má právomoc nariadiť prevádzkovateľovi, aby porušenie ochrany osobných údajov, oznámené úradu, oznámil dotknutej osobe. Táto právomoc podľa nariadenia, ktorú UOOU má, je podľa navrhovaného znenia zákona v priamom rozpore s tým, aby iba na základe rozhodnutia úradu mohol UOOU informáciu, ktorú mu nahlásil prevádzkovateľ, použiť na ochranu dotknutých osôb iba v tom prípade, ak bude mať povolenie úradu. Tiež je potrebné vziať do úvahy povinnosť samotného prevádzkovateľa, ktorý na základe čl. 34 naradenia a na základe ustanovenia návrhu zákona o ochrane osobných údajov, o porušení ochrany osobných údajov, ak to je potrebné, informoval nielen UOOU, ale aj samotnú dotknutú osobu. Pokiaľ ide o právo úradu na zverejnenie informácií získaných z neverejnej časti JISKB, ktoré môže vo verejnom záujme, ak uzná za vhodné zverejniť, nie sme toho názoru, že by tak mal úrad právo robiť iba na základe svojho uváženia podľa navrhovaného zákona, nakoľko podľa čl. 34 ods. 4 nariadenia UOOU, ak sú splnené podmienky, môže informovanie dotknutých osôb o porušení ochrany osobných údajov od prevádzkovateľa požadovať; ide však o požadovanie/nariadenie UOOU prevádzkovateľovi, aby informoval dotknutú osobu, nie porušenie ochrany osobných údajov aj zverejnil (aj keď v krajných prípadoch nie je ani informovanie formou verejných komunikačných prostriedkov vylúčené); no mal by o ňom rozhodovať UOOU, nie úrad. | Z | N | Návrh zákona o KB určuje minimálne bezpečnostné štandardy zabezpečenia kvality sietí a informačných systémov v pôsobnosti subjektu, ktorý je pomocou určených kritérií určený ako "kritický" vo vzťahu k zabezpečeniu a udržaniu úloh štátu. Hlásenie KBI je jedným zo základných nástrojov zabezpečovania monitorovania a riešenia narušenia sietí a informačných systémov. Toto hlásenie sa realizuje prostredníctvom informačného systému, ktorý vybuduje úrad. Informačný systém bude obsahovať moduly a funkcionality uvedené v zákone. V zákone nemožno uviesť, ako technicky bude systém vyzerať, ide o konštrukčnú záležitosť na úrovni IT, avšak spôsobilosť informačného systému tak, ako je uvedené v zákone, bude zabezpečená. Verejnosť od začiatku polemík o zákone o KB apelovala na zjednodušenie prístupu povinných subjektov k naplneniu ich povinností vyplývajúcich z rôznych zákonov (nielen zákon o OOU, ale aj zákon o kritickej infraštruktúre, telekomunikačný zákon, zákon o bankách), čím sa zníži administratívna zaťaženosť subjektov a zvýši sa ich ochota hlásiť incidenty. Preto je vybudovanie jedného "kanálu" pre hlásenie incidentov pochádzajúcich z porušenie rôznych zákonov legitímnou požiadavkou. Treba si uvedomiť, že ide o vybudovanie jedného kanálu, nie o vybudovanie jednej databázy. Hlásenie skončí vždy u subjektu, ktorý je povinný ho spracovávať a riešiť. Uvedené bolo vysvetlené aj na rozporovom konaní k novému zákonu o OOU, s čím úrad vyslovil súhlas a nemal námietky, aby jeden zo spôsobov hlásenia incidentov na úseku OOU bol aj informačný systém zo zákona o KB. Na tejto báze je teda postavený aj prístup k neverejnej časti - teda prístup i nahlásených informáciám týkajúcich sa konkrétneho subjektu. Poskytovanie údajov z tejto neverejnej časti môže úrad "otvoriť" len v prípade verejného záujmu. V snahe predísť obštrukciám pri riešení závažných otázok týkajúcich sa zabezpečenia základných úloh štátu je potrebné uviesť takúto úpravu priamo do zákona. V uvedení súvislosti úrad na ochranu osobných údajov v súlade s nariadením o GDPR, kedy je možné v záujme bezpečnosti uplatniť podmienky obmedzenia. To iste nevylučuje, že úrad bude chrániť osobné údaje spôsobom akým mu to nariadenie určuje. Tu treba uviesť, že všetky údaje v JISKB budú užívať ochranu vyššou mierou bezpečnosti nástrojov, ako ustanovuje dokonca samotné GDPR, keďže systém bude utajovaný (rovnaký princíp je uplatnený aj v rámci spracovania osobných údajov v zmysle zákona č. 215/2004 Z. z., kde sú osobné údaje chránené v systéme, ktorý je utajovaný, čo bolo rovnako vysvetlené a akceptované UOOU na rozporovom konaní k zákonu o OOU).Rozpor bol odstránený. |
| **UOOU SR** | **K Čl. I k § 12 ods. 7** K Čl. I k § 12 ods. 7 Požadujeme zahrnutie spracovateľských operácií s osobnými údajmi vrátanie sprístupňovania osobných údajov v JISKB pod zákon o ochrane osobných údajov. Táto pripomienka je zásadná. Odôvodnenie: Požadujeme ozrejmenie dôvodov, pre ktoré spracúvanie a sprístupňovanie osobných údajov v JISKB nebude podliehať zákonu o ochrane osobných údajov. | Z | N | Návrh zákona o KB určuje minimálne bezpečnostné štandardy zabezpečenia kvality sietí a informačných systémov v pôsobnosti subjektu, ktorý je pomocou určených kritérií určený ako "kritický" vo vzťahu k zabezpečeniu a udržaniu úloh štátu. Hlásenie KBI je jedným zo základných nástrojov zabezpečovania monitorovania a riešenia narušenia sietí a informačných systémov. Toto hlásenie sa realizuje prostredníctvom informačného systému, ktorý vybuduje úrad. Informačný systém bude obsahovať moduly a funkcionality uvedené v zákone. V zákone nemožno uviesť, ako technicky bude systém vyzerať, ide o konštrukčnú záležitosť na úrovni IT, avšak spôsobilosť informačného systému tak, ako je uvedené v zákone, bude zabezpečená. Verejnosť od začiatku polemík o zákone o KB apelovala na zjednodušenie prístupu povinných subjektov k naplneniu ich povinností vyplývajúcich z rôznych zákonov (nielen zákon o OOU, ale aj zákon o kritickej infraštruktúre, telekomunikačný zákon, zákon o bankách), čím sa zníži administratívna zaťaženosť subjektov a zvýši sa ich ochota hlásiť incidenty. Preto je vybudovanie jedného "kanálu" pre hlásenie incidentov pochádzajúcich z porušenie rôznych zákonov legitímnou požiadavkou. Treba si uvedomiť, že ide o vybudovanie jedného kanálu, nie o vybudovanie jednej databázy. Hlásenie skončí vždy u subjektu, ktorý je povinný ho spracovávať a riešiť. Uvedené bolo vysvetlené aj na rozporovom konaní k novému zákonu o OOU, s čím úrad vyslovil súhlas a nemal námietky, aby jeden zo spôsobov hlásenia incidentov na úseku OOU bol aj informačný systém zo zákona o KB. Na tejto báze je teda postavený aj prístup k neverejnej časti - teda prístup i nahlásených informáciám týkajúcich sa konkrétneho subjektu. Poskytovanie údajov z tejto neverejnej časti môže úrad "otvoriť" len v prípade verejného záujmu. V snahe predísť obštrukciám pri riešení závažných otázok týkajúcich sa zabezpečenia základných úloh štátu je potrebné uviesť takúto úpravu priamo do zákona. V uvedení súvislosti úrad na ochranu osobných údajov v súlade s nariadením o GDPR, kedy je možné v záujme bezpečnosti uplatniť podmienky obmedzenia. To iste nevylučuje, že úrad bude chrániť osobné údaje spôsobom akým mu to nariadenie určuje. Tu treba uviesť, že všetky údaje v JISKB budú užívať ochranu vyššou mierou bezpečnosti nástrojov, ako ustanovuje dokonca samotné GDPR, keďže systém bude utajovaný (rovnaký princíp je uplatnený aj v rámci spracovania osobných údajov v zmysle zákona č. 215/2004 Z. z., kde sú osobné údaje chránené v systéme, ktorý je utajovaný, čo bolo rovnako vysvetlené a akceptované UOOU na rozporovom konaní k zákonu o OOU). Rozpor bol odstránený. |
| **UOOU SR** | **K Čl. I k § 2 ods. 2 písm. a)** K Čl. I k § 2 ods. 2 písm. a) Navrhujeme doplniť na záver písm. a) slovo „skutočností“. Odôvodnenie: Legislatívno – technická pripomienka. | O | A |  |
| **UOOU SR** | **K čl. I k § 33 písm. h)** K čl. I k § 33 písm. h) Požadujeme vypustenie písmena h) z § 33 nakoľko práva a povinnosti subjektov, pokiaľ ide o ochranu osobných údajov, je možné ukladať iba zákonom, nie vykonávacím predpisom, navyše odkaz na § 6 ods. 1 písm. d)zákona je nesprávny nakoľko tento pojednáva o inom, ako o výmene informácií. Táto pripomienka je zásadná. Odôvodnenie: Spracúvanie a ochrana osobných údajov sa toho času riadi zákonom č. 122/2013 Z. z. o ochrane osobných údajov. Avšak od 25.5.2018 bude platný a účinný nový zákon o ochrane osobných údajov, ktorý je toho času v PPK, tiež sa od tohto dátumu začne vykonávať a uplatňovať v praxi nariadenie EU 2016/679. Pokiaľ na účely podľa tohto zákona má byť výmena a spracúvanie osobných údajov upravené iným režimom, je potrebné, aby tento nekolidoval s nariadením a zákonom a tiež je potrebné, aby práva a povinnosti jednotlivých subjektov, pokiaľ ide o základné ľudské práva a slobody a ochranu súkromia upravoval a stanovoval zákon, nie vyhláška. | Z | N | Návrh zákona o KB určuje minimálne bezpečnostné štandardy zabezpečenia kvality sietí a informačných systémov v pôsobnosti subjektu, ktorý je pomocou určených kritérií určený ako "kritický" vo vzťahu k zabezpečeniu a udržaniu úloh štátu. Hlásenie KBI je jedným zo základných nástrojov zabezpečovania monitorovania a riešenia narušenia sietí a informačných systémov. Toto hlásenie sa realizuje prostredníctvom informačného systému, ktorý vybuduje úrad. Informačný systém bude obsahovať moduly a funkcionality uvedené v zákone. V zákone nemožno uviesť, ako technicky bude systém vyzerať, ide o konštrukčnú záležitosť na úrovni IT, avšak spôsobilosť informačného systému tak, ako je uvedené v zákone, bude zabezpečená. Verejnosť od začiatku polemík o zákone o KB apelovala na zjednodušenie prístupu povinných subjektov k naplneniu ich povinností vyplývajúcich z rôznych zákonov (nielen zákon o OOU, ale aj zákon o kritickej infraštruktúre, telekomunikačný zákon, zákon o bankách), čím sa zníži administratívna zaťaženosť subjektov a zvýši sa ich ochota hlásiť incidenty. Preto je vybudovanie jedného "kanálu" pre hlásenie incidentov pochádzajúcich z porušenie rôznych zákonov legitímnou požiadavkou. Treba si uvedomiť, že ide o vybudovanie jedného kanálu, nie o vybudovanie jednej databázy. Hlásenie skončí vždy u subjektu, ktorý je povinný ho spracovávať a riešiť. Uvedené bolo vysvetlené aj na rozporovom konaní k novému zákonu o OOU, s čím úrad vyslovil súhlas a nemal námietky, aby jeden zo spôsobov hlásenia incidentov na úseku OOU bol aj informačný systém zo zákona o KB. Na tejto báze je teda postavený aj prístup k neverejnej časti - teda prístup i nahlásených informáciám týkajúcich sa konkrétneho subjektu. Poskytovanie údajov z tejto neverejnej časti môže úrad "otvoriť" len v prípade verejného záujmu. V snahe predísť obštrukciám pri riešení závažných otázok týkajúcich sa zabezpečenia základných úloh štátu je potrebné uviesť takúto úpravu priamo do zákona. V uvedení súvislosti úrad na ochranu osobných údajov v súlade s nariadením o GDPR, kedy je možné v záujme bezpečnosti uplatniť podmienky obmedzenia. To iste nevylučuje, že úrad bude chrániť osobné údaje spôsobom akým mu to nariadenie určuje. Tu treba uviesť, že všetky údaje v JISKB budú užívať ochranu vyššou mierou bezpečnosti nástrojov, ako ustanovuje dokonca samotné GDPR, keďže systém bude utajovaný (rovnaký princíp je uplatnený aj v rámci spracovania osobných údajov v zmysle zákona č. 215/2004 Z. z., kde sú osobné údaje chránené v systéme, ktorý je utajovaný, čo bolo rovnako vysvetlené a akceptované UOOU na rozporovom konaní k zákonu o OOU). Rozpor bol odstránený. |
| **UOOU SR** | **K čl. I k § 35 ods. 1 a 2 Požadujeme spresnenie pojmu sprístupní a tiež požadujeme, aby narušenie ochrany osobných údajov bolo vykonávané v súlade s nariadením, a to aj pokiaľ ide o začiatok plnenia si tejto povinnosti, pokiaľ má byť táto plnená iba cez JISKB.** K čl. I k § 35 ods. 1 a 2 Požadujeme spresnenie pojmu sprístupní a tiež požadujeme, aby narušenie ochrany osobných údajov bolo vykonávané v súlade s nariadením, a to aj pokiaľ ide o začiatok plnenia si tejto povinnosti, pokiaľ má byť táto plnená iba cez JISKB. Odôvodnenie: Na základe navrhovaného ustanovenia § 35 ods. 1 zákona sa má JISKB sprístupniť do 18 mesiacov od nadobudnutia účinnosti zákona, teda najneskôr do júna 2019. Nakoľko nariadenie a navrhovaný zákon o ochrane osobných údajov ustanovujú povinnosť hlásiť porušenie ochrany osobných údajov odo dňa uplatňovania nariadenia, teda odo dňa 25.5.2018 nie je možné, aby tieto boli vykonávané iba v rámci JISKB, ako je predbežne navrhované, nakoľko by tým Slovenská republika neplnila záväzky z nariadenia EU 2016/679 a tiež zo zákona o ochrane osobných údajov, ktorý je v štádiu schvaľovania. V zmysle vyššie uvedeného požadujeme vysvetliť celkové fungovanie JISKB, termín jeho spustenia do prevádzky a uvedenie typov hlásení, ktoré by mali byť jeho obsahom. | O | N | Návrh zákona o KB určuje minimálne bezpečnostné štandardy zabezpečenia kvality sietí a informačných systémov v pôsobnosti subjektu, ktorý je pomocou určených kritérií určený ako "kritický" vo vzťahu k zabezpečeniu a udržaniu úloh štátu. Hlásenie KBI je jedným zo základných nástrojov zabezpečovania monitorovania a riešenia narušenia sietí a informačných systémov. Toto hlásenie sa realizuje prostredníctvom informačného systému, ktorý vybuduje úrad. Informačný systém bude obsahovať moduly a funkcionality uvedené v zákone. V zákone nemožno uviesť, ako technicky bude systém vyzerať, ide o konštrukčnú záležitosť na úrovni IT, avšak spôsobilosť informačného systému tak, ako je uvedené v zákone, bude zabezpečená. Verejnosť od začiatku polemík o zákone o KB apelovala na zjednodušenie prístupu povinných subjektov k naplneniu ich povinností vyplývajúcich z rôznych zákonov (nielen zákon o OOU, ale aj zákon o kritickej infraštruktúre, telekomunikačný zákon, zákon o bankách), čím sa zníži administratívna zaťaženosť subjektov a zvýši sa ich ochota hlásiť incidenty. Preto je vybudovanie jedného "kanálu" pre hlásenie incidentov pochádzajúcich z porušenie rôznych zákonov legitímnou požiadavkou. Treba si uvedomiť, že ide o vybudovanie jedného kanálu, nie o vybudovanie jednej databázy. Hlásenie skončí vždy u subjektu, ktorý je povinný ho spracovávať a riešiť. Uvedené bolo vysvetlené aj na rozporovom konaní k novému zákonu o OOU, s čím úrad vyslovil súhlas a nemal námietky, aby jeden zo spôsobov hlásenia incidentov na úseku OOU bol aj informačný systém zo zákona o KB. Na tejto báze je teda postavený aj prístup k neverejnej časti - teda prístup i nahlásených informáciám týkajúcich sa konkrétneho subjektu. Poskytovanie údajov z tejto neverejnej časti môže úrad "otvoriť" len v prípade verejného záujmu. V snahe predísť obštrukciám pri riešení závažných otázok týkajúcich sa zabezpečenia základných úloh štátu je potrebné uviesť takúto úpravu priamo do zákona. V uvedení súvislosti úrad na ochranu osobných údajov v súlade s nariadením o GDPR, kedy je možné v záujme bezpečnosti uplatniť podmienky obmedzenia. To iste nevylučuje, že úrad bude chrániť osobné údaje spôsobom akým mu to nariadenie určuje. Tu treba uviesť, že všetky údaje v JISKB budú užívať ochranu vyššou mierou bezpečnosti nástrojov, ako ustanovuje dokonca samotné GDPR, keďže systém bude utajovaný (rovnaký princíp je uplatnený aj v rámci spracovania osobných údajov v zmysle zákona č. 215/2004 Z. z., kde sú osobné údaje chránené v systéme, ktorý je utajovaný, čo bolo rovnako vysvetlené a akceptované UOOU na rozporovom konaní k zákonu o OOU). |
| **ÚPPVII** | **Čl. I § 6 ods. 1** Dávame na zváženie vypustenie písm. a) z dôvodu čiastočnej duplicity ustanovenia s § 34 zákona č. 575/2001 Z. z. Legislatívno technická pripomienka | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že úrad vystupuje aj ako vecne príslušný subjekt aj ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť a na základe toho má teda dve oddelené úlohy. |
| **ÚPPVII** | **Čl. I § 32** Maximálna výška pokuty v prípade porušenia ustanovení zákona je neprimerane vysoká bez zohľadnenia závažnosti porušenia. Odporúčame zvážiť doplnenie možnosti upustenia od potrestania v závislosti od rozsahu protiprávneho konania a spôsobenej škody. | O | A | Vaša pripomienka bola akceptovaná a zapracovaná. |
| **ÚPPVII** | **Čl. I § 10 ods. 7** Na koniec prvej vety navrhujeme doplniť slová „ak osobitný predpis neustanovuje inak“ s odkazom napríklad na § 7 ods. 2 písm. g) zákona č. 319/2002 Z.z. v znení neskorších predpisov. Odôvodnenie: Spresňujúca úprava, ktorá zosúlaďuje rozsah prístupu podľa § 10 ods. 5 a podľa navrhovaného § 7 ods. 2 písm. g) zákona o obrane. | Z | A | Vaša pripomienka nebola akceptovaná. Text preformulovaný aj po zvážení a zapracovaní odôvodnených pripomienok iných subjektov. |
| **ÚPPVII** | **Čl. I § 17** Navrhujeme do § 17 doplniť aj mechanizmus oznamovania zaradenia do zoznamu a do registra, napríklad doručením písomného oznámenia. Odôvodnenie: Keďže na zaradenie do zoznamu a registra sú naviazané povinnosti podľa tohto zákona, je vhodné, aby o dni zaradenia bola osoba informovaná. | O | A | Vaša pripomienka bola akceptovaná a textácia bola preformulovaná. |
| **ÚPPVII** | **Čl. I § 5 písm. c) deviaty bod** Navrhujeme doplniť do deviateho bodu aj „Vojenské spravodajstvo“, alebo znenie deviateho bodu uvádzať ako „spravodajské služby“. Odôvodnenie: Keďže v prílohe č. 1 v sektore „Verejná správa“, podsektore „Spravodajské služby“ sa ako VPA uvádza aj Vojenské spravodajstvo, je potrebné to zohľadniť aj v § 5. | Z | ČA | Vaša pripomienka bola čiastočne akceptovaná a upravená v zmysle nového písmena e). Po úprave prílohy č. 1 a zmene § 5 bol rozpor za odstránený. |
| **ÚPPVII** | **Čl. I § 18 ods. 1** Navrhujeme slová „od okamihu zaradenia“ nahradiť slovami „odo dňa doručenia oznámenia o zaradení“. Odôvodnenie: Moment zaradenia do registra je zásadný z pohľadu povinnosti prijať a plniť bezpečnostné opatrenia. Preto jeho vznik je potrebné viazať na konkrétny akt, ktorý je osobe známy – a tým by malo byť doručenie informácie o zaradení. | Z | A |  |
| **ÚPPVII** | **Čl. I § 16 ods. 1** Navrhujeme slovo „Jednotka“ nahradiť slovami „Prevádzkovateľ jednotky“. Odôvodnenie: Keďže jednotka CSIRT nemá právnu subjektivitu, nemôže byť nositeľom povinností a ani subjektom zodpovednosti za ich plnenie. | Z | A |  |
| **ÚPPVII** | **Čl. I § 15 ods. 1 písm. e)** Navrhujeme v zákone ustanoviť, kto vydáva, alebo ako sú definované spoločné mechanizmy spolupráce jednotiek CSIRT, pričom ak sa nimi ukladajú povinnosti, je ich potrebné ustanoviť v zákone aspoň druhovo a následne upraviť vo vykonávacom predpise. Ak v zákone ustanovené nebudú, je § 15 ods. 1 písm. e) nevyhnutné vypustiť. Odôvodnenie: Ustanovenie odkazuje na neexistujúce podmienky, mechanizmus spolupráce. Z tohto dôvodu je ho potrebné definovať, alebo ustanovenie vypustiť. | Z | A |  |
| **ÚPPVII** | **Čl. I § 3 písm. j)** Navrhujeme zladiť definíciu poskytovateľa digitálnej služby s definíciou digitálnej služby. Podmienka 50 zamestnancov a obratu, resp. bilancie sa totiž viaže len na poskytovateľa a nie je previazaná na službu. Návrh je teda nastavený tak, že môže dôjsť k zápisu služby ale už nie poskytovateľa, ak ten nespĺňa podmienku počtu zamestnancov, resp. obratu, alebo bilancie. Navrhujeme teda podmienky počtu zamestnancov, resp. obratu, alebo bilancie viazať na službu a nie poskytovateľa. | Z | A | Vaša pripomienka bola akceptovaná a text bol preformulovaný, nové pojmy v súlade s nariadením NIS po zapracovaní pripomienok iných subjektov. |
| **ÚPPVII** | **Čl. I § 6 ods. 1 písm. b)** Nie je zrejmé, čo predkladateľ myslí pod pojmom "politika správania sa v kybernetickom priestore“, odporúčame v zákone spresniť. | O | A | Vaša pripomienka bola akceptovaná a vysvetlená v dôvodovej správe. |
| **ÚPPVII** | **Čl. I § 11 ods. 1 písm. f)** Odporúčame časť vety za bodkočiarkou upraviť ako osobitnú povinnosť, ideálne aj s lehotami na doplnenie, a to buď tak, že namiesto bodkočiarky sa táto povinnosť uvedie slovami „a predkladá ich zoznam úradu v najneskôr do ...“ alebo sa uvedie v osobitnom odseku. Legislatívno-technická pripomienka | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že lehoty sú uvedené v prechodných ustanoveniach. |
| **ÚPPVII** | **Čl. I § 12 ods. 2** Odporúčame doplniť oprávnenú osobu na zbavenie mlčanlivosti aj vo vzťahu k ostatným osobám, napríklad „súkromné“ jednotky CSIRT, ako aj prevádzkovatelia základnej služby a poskytovatelia digitálnej služby, ako aj iné orgány verejnej moci, ktoré nie sú NBÚ a ani VPA. Odôvodnenie: Povinnosť mlčanlivosti sa vzťahuje na väčší okruh subjektov, než len NBÚ a vecne príslušná autorita. Preto je potrebné aj pre tieto subjekty ustanoviť osobu, ktorá je oprávnená ich zbaviť mlčanlivosti, alebo na nich vztiahnuť režim odseku 3. | O | A | Vaša pripomienka bola akceptovaná a zapracovaná. |
| **ÚPPVII** | **Čl I § 2 ods. 2 písm. c)** Odporúčame na konci doplniť slová „o trestnoprávnej zodpovednosti“. Na účely odstránenia výkladových sporov odporúčame aspoň druhovo špecifikovať o aké osobitné predpisy ide. | O | A | Text preformulovaný a upravený v zmysle pripomienok. |
| **ÚPPVII** | **Čl. I § 18 ods. 7** Odporúčame nahradiť slová „si to osobitné záujmy vyžadujú“ slovami „ide najmenej o závažný kybernetický bezpečnostný incident“. Rovnakú úpravu navrhujeme vykonať aj v § 21 ods. 5. Odôvodnenie: Považujeme za vhodné pri formulovaní povinnosti uviesť objektívne kritériá, kedy má prevádzkovateľ informovať aj tretie strany (napríklad dodávateľa systému). Za takéto kritériá navrhujeme napríklad závažnosť kybernetického incidentu. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a znenie bolo preformulované. |
| **ÚPPVII** | **Čl. I § 3 písm. g) a i)** Odporúčame pojmy „základná služba“ a „digitálna služba“ definovať len tým, že ide o služby zapísané v zozname. Podmienky závislosti od sietí a systémov a činnosti podľa príloh odporúčame uvádzať až ako podmienky zaradenia do jednotlivých zoznamov. Odporúčanou úpravou dôjde k zosúladeniu s navrhovaným postupom, kedy pre samotné služby je podstatné až zaradenie do zoznamu. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že bol upravený celý § 3 a boli zavedené nové pojmy. |
| **ÚPPVII** | **Čl. I § 27 ods. 4** Odporúčame prehodnotiť obmedzenie možnosti uloženia povinnosti len v núdzovom stave. Z textu vyplýva, že v závažnejších krízových situáciách povinnosť nebude možné uložiť, čo pôsobí nelogicky. Zároveň odporúčame doplniť aj možnosť uloženia opatrení v čase stavu kybernetického ohrozenia – § 28 ods. 5. | O | A | Pripomienka bola akceptovaná, text ustanovenia bol preformulovaný. |
| **ÚPPVII** | **Príloha č. 1** Odporúčame rozpísať v plnom znení skratky „PZS“ a „VPA“. Odôvodnenie: Skratky sa v právnych predpisoch nezvyknú používať a keďže v danom prípade ide o pojmy, ktoré sú v zákone definované, je vhodné ich uvádzať v plnom znení. | O | A |  |
| **ÚPPVII** | **Čl. I § 17 ods. 1** Odporúčame slová „ktorým správca“ nahradiť slovami „ktorým je správca“. Rovnako odporúčame doplniť nový odsek v znení „Základnú službu, ktorou je informačný systém verejnej správy a prevádzkovateľa základnej služby, ktorým je správca informačného systému verejnej správy zaradí úrad do zoznamu základných služieb a do registra prevádzkovateľov základných služieb z vlastnej iniciatívy bezodkladne po tom, ako sa o ich vzniku dozvie.“. Legislatívno-technická pripomienka | O | A | Vaša pripomienka bola akceptovaná a upravená v rámci nového ustanovenia. |
| **ÚPPVII** | **Čl. I § 7 ods. 1** Odporúčame slová „prostredníctvom ktorej zabezpečuje“ nahradiť slovami „a plní“. Okrem gramatickej úpravy ide aj o explicitné vyjadrenie toho, že NBÚ musí plniť úlohy jednotky CSIRT vlastnými kapacitami a preto je vhodné použiť slovo „plní“, a nie zabezpečuje. | O | A | Vaša pripomienka bola akceptovaná a zapracovaná. |
| **ÚPPVII** | **Čl. I § 23** Odporúčame ustanovenie rozdeliť a jednotlivé kategórie incidentov uvádzať kvôli prehľadnosti v písmenách a) až c). Legislatívno-technická pripomienka | Z | ČA | Vaša pripomienka bola čiastočne akceptovaná, konkrétne znenie bolo vypustené. Právna úprava bola premietnutá v preformulovanej podobe s obsahom aj jednotlivých kriteriálnych parametrov v rámci § o hlásení kybernetických bezpečnostných incidentov. Parametre sú v súlade so smernicou NIS na určenie závažného kybernetického bezpečnostného incidentu. Jednotlivé kategórie sú odstupňované od závažnosti od 1 po 3, v záujme flexibilného reagovania na bezpečnostné prostredie je nevyhnutné špecifikáciu prenechať do vykonávacieho predpisu. Po vysvetlení bol rozpor odstránený. |
| **ÚPPVII** | **Čl. I § 11 ods. 1 písm. a)** Odporúčame vypustiť písmeno a). Odôvodnenie: Keďže VPA nemá nad rámec písmen b) až g) v zákone ustanovené úlohy, odporúčame písmeno a) ako nadbytočné vypustiť. | O | A | Vaša pripomienka bola akceptovaná a zapracovaná. |
| **ÚPPVII** | **Čl. I § 3 písm. h)** Odporúčame vypustiť slová „a sú zároveň zaradení do registra prevádzkovateľov základných služieb“. Samotné zaradenie do registra je na účely určenia prevádzkovateľa irelevantné. Akonáhle je služba základnou službou, vždy musí mať na účely zákona prevádzkovateľa, ktorý sa zapisuje do registra. Na účely definície pojmu je preto podstatné statusové vymedzenie tejto osoby (prevádzkovateľ/správca ISVS). | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že bol upravený celý § 3 a boli zavedené nové pojmy. |
| **ÚPPVII** | **Čl. I § 11 ods. 1 písm. g)** Odporúčame vypustiť slovo „vykonávanie“, alebo upraviť skloňovanie slov „klasifikácia“ a „kategorizácia“. Legislatívno technická pripomienka. | O | A | Vaša pripomienka bola akceptovaná a zapracovaná. |
| **ÚPPVII** | **Čl I § 29 ods. 7** Odporúčame za slovné spojenie "sú povinné spolupracovať" doplniť slovné spojenie "v primeranej miere. Zároveň za slová „Orgány verejnej moci“ odporúčame doplniť slová „, ktoré nie sú kontrolovaným subjektom“. Odôvodnenie: Odstránenie konfliktu s § 29 ods. 8, keďže úprava navodzuje dojem, že orgán verejnej moci má iný rozsah povinností pri kontrole, než iný subjekt. | O | A | Text nahradený novým znením a preformulovaný aj vzhľadom na pripomienky ostatných subjektov. |
| **ÚPPVII** | **Prílohám** Označenie príloh k zákonu je potrebné upraviť podľa Legislatívnych pravidiel vlády SR (príloha č. 1 bod 15). Legislatívno-technická pripomienka | O | A |  |
| **ÚPPVII** | **Čl. I § 6 ods. 2** Poslednú vetu odporúčame vypustiť a doplniť do § 5a ods. 5 infozákona tento typ zmluvy, ak nebude spadať pod žiaden z tam už uvedených typov zmlúv. Odôvodnenie: Povinne zverejňované zmluvy sú definované v infozákone na účely celého právneho poriadku, bez možnosti negatívneho vymedzenia v osobitnom zákone. Z tohto dôvodu nie je možné úpravu vykonať tak, ako to navrhuje predkladateľ, keďže by to znamenalo nepriamu novelizáciu infozákona. Ak je zmluva podľa § 6 ods. 2 návrhu zákona iným typom zmluvy, než sú zmluvy podľa § 5a ods. 5 infozákona, je ju potrebné explicitne doplniť do § 5a ods. 5 infozákona. | Z | A |  |
| **ÚPPVII** | **Čl. I § 2** Požadujeme doplniť § 2 novým odsekom, ktorý explicitne vyjadrí princíp, že orgány verejnej moci nemôžu vykonávať preventívne a reaktívne služby, resp. ochranné a reaktívne opatrenia priamo a „bez súhlasu“ prevádzkovateľa základnej služby, resp. poskytovateľa digitálnej služby, ale môžu „len“ nariadiť ich vykonanie. V tomto kontexte navrhujeme napríklad nasledovné znenie nového odseku 3: „(3) Tento zákon nie je možné vykladať tak, že zakladá oprávnenie orgánov verejnej moci v oblasti kybernetickej bezpečnosti na priame vykonávanie služieb a opatrení podľa tohto zákona u prevádzkovateľa základnej služby alebo poskytovateľa digitálnej služby.“. alebo „(3) Tento zákon neoprávňuje orgány verejnej moci v oblasti kybernetickej bezpečnosti na priame vykonávanie služieb a opatrení podľa tohto zákona u prevádzkovateľa základnej služby alebo poskytovateľa digitálnej služby.“. | Z | ČA | Po doplnení § 15 novým odsekom 4 považujeme rozpor za odstránený. |
| **ÚPPVII** | **Čl. I § 5 písm. c)** Požadujeme medzi vecne príslušné autority zaradiť aj ministerstvá a ostatné ústredné orgány štátnej správy, a to pre podsektor „Informačné systémy verejnej správy“, buď tak, že budú VPA pre také systémy, ktorých sú správcom, alebo ktorých správcom sú organizácie v ich pôsobnosti, alebo tak, že v týchto prípadoch bude postavenie a úlohy vykonávať NBÚ v spolupráci s týmito ministerstvami a ostatnými ústrednými orgánmi verejnej správy. Následne je túto zmenu potrebné zohľadniť aj v Prílohe č. 1. Odôvodnenie: Informačné systémy verejnej správy sú zo „sektorového hľadiska“ prierezové a môžu mať diametrálne odlišné nároky od „rezortu k rezortu“. Navyše, množstvo týchto systémov de facto vylučuje, aby ich z pohľadu VPA zastrešoval jeden orgán, bez ohľadu na to, ktorý by to bol. Navrhujeme preto úpravu, ktorá umožní ústredným orgánom štátnej správy pre danú oblasť vykonávať povinnosti VPA vo vzťahu k systémom, ktoré sú v „ich rezorte“ prevádzkované. | Z | ČA | Po úprave prílohy č. 1 a zmene § 5 považujeme rozpor za odstránený. |
| **ÚPPVII** | **Čl. I § 15 ods. 5** Požadujeme slová „sa nevzťahujú žiadne práva vyplývajúce z tohto zákona“ nahradiť buď negatívnym vymedzením ustanovení zákona, ktoré sa na „súkromné CSIRTy“ neuplatnia, alebo naopak pozitívnym vymedzením ustanovení, ktoré jediné sa uplatnia. Odôvodnenie: Návrh zákona neobsahuje úpravu „práv jednotiek CSIRT“ a preto navrhovaný spôsob regulácie vytvára stav právnej neistoty, kedy nie je zrejmé, v čom sú jednotky CSIRT, ktoré neprevádzkuje VPA, obmedzené oproti iným jednotkám CSIRT. Keďže ide o úpravu práv subjektov súkromného práva, je nevyhnutné, aby táto úprava bola jasná a neumožňovala dvojaký, resp. arbitrárny výklad. | Z | N | Z textu vyplýva, že každá jednotka CSIRT musí byť akreditovaná a spĺňať podmienky podľa tohto zákona bez rozdielu „vlastníctva“ alebo pôvodu. Úrad vypustil ustanovenie týkajúce sa právneho obmedzenia „súkromných“ CSIRTov bez náhrady a text návrhu zákona nerozlišuje jednotky CSIRT. Na základe uvedeného považujeme rozpor za odstránený. Po posúdení textu ÚPVII rozpor za odstránený. |
| **ÚPPVII** | **Čl. I § 28 ods. 5** Požadujeme zjednotiť režimy ukladania opatrení podľa § 27 a podľa § 28 ods. 8. Z návrhu vyplýva, že v stave kybernetického ohrozenia môže NBÚ ukladať povinnosť vykonať všetky opatrenia podľa § 27 (teda aj varovania) všetkým vymenovaným subjektom. Navyše, vo vzťahu k prevádzkovateľovi základnej služby to pôsobí zmätočne, keďže sa vytvára dojem dvojakého režimu prístupu – mimo stavu ohrozenia a v stave ohrozenia, avšak z vecného hľadiska ide vždy len o jeden typ rozhodnutí. Preto navrhujeme § 28 ods. 5 upraviť tak, aby bol odstránený rozpor, resp. duplicita s § 27, najmä § 27 ods. 4, a to napríklad takto: „(5) V čase stavu kybernetického ohrozenia môže úrad uložiť rozhodnutím povinnosť vykonať opatrenia podľa § 27 ods. 1 písm. b) alebo c) aj vecne príslušnej autorite, prevádzkovateľovi jednotky CSIRT a poskytovateľovi digitálnej služby.“. Odôvodnenie: Odstránenie výkladových problémov. | Z | ČA | Vaša pripomienka bola čiastočne akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. Úlohy MOSR v oblasti kybernetickej obrany presunuté do zákona o obrane, kde vytvárajú ucelenú štruktúru pri zabezpečovaní obrany štátu v čase, kedy to zákon o obrane predpokladá. Zákon o KB je tak zákonom upravujúcim kybernetickú bezpečnosť a minimálne bezpečnostné atribúty na dosiahnutie tejto bezpečnosti v čase mieru. Po vysvetlení bol rozpor odstránený. |
| **ÚPPVII** | **Čl. I § 13 ods. 5** Rozhodnutie o akreditácii by malo byť vydané na dobu neurčitú, najmä pre orgány verejnej moci z dôvodu zníženia administratívnej záťaže na opätovnú akreditáciu. Neexistuje dôvod v prípade fungujúcich jednotiek ich opätovne akreditovať. Nefunkčnosť jednotiek je už týmto zákonom riešená v §15 (4). | O | N | Vaša pripomienka nebola akceptovaná. Akreditácia nepredstavuje administratívnu záťaž, ale nevyhnutnú úlohu v systéme riadneho zabezpečenia kybernetickej bezpečnosti. Uvedený systém časovo limitovaného udelenia akreditácie je štandardný nástroj zabezpečovania bezpečnosti IT. |
| **ÚPPVII** | **Čl. I § 16 ods. 1** Slová "reaktívne a preventívne služby" odporúčame nahradiť slovami "preventívne služby a reaktívne služby" z dôvodu systematiky § 16 v odsekoch 2 a 3. Zároveň sa upravuje znenie ustanovenia podľa čl. 6 ods. 3 Legislatívnych pravidiel vlády SR. legislatívno-technická pripomienka | O | A |  |
| **ÚPPVII** | **Čl. I § 9 ods. 2 písm. i)** Slová "rôznych aktérov" odporúčame nahradiť slovom "subjektov". | O | A |  |
| **ÚPPVII** | **Čl. I § 28 ods. 9** Slová "štátnu správu" odporúčame nahradiť slovom "opatrenia" za účelom zosúladenia terminológie v rámci predpisu podľa čl. 6 ods. 2 Legislatívnych pravidiel vlády SR. legislatívno-technická pripomienka | O | A |  |
| **ÚPPVII** | **Čl. I § 30 ods. 1** Slová „umožniť a“ navrhujeme vypustiť ako nadbytočné. V záujme jednoznačnosti výkladu navrhujeme jasne definovať pojem "interný audit" a "externý audit", spolu s požiadavkami na audítora a rozsah auditu na účely tohto zákona. Následne navrhujeme druhú vetu preformulovať napríklad takto: „Prevádzkovateľ základnej služby je povinný podrobiť sa opakovanému auditu v časových intervaloch podľa všeobecne záväzného právneho predpisu, a to v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov.“. Odporúčame tiež vypustiť odkaz na poznámku pod čiarou 32). Legislatívno-technická pripomienka | O | A | Vaša pripomienka bola akceptovaná a zapracovaná. |
| **ÚPPVII** | **Čl. I § 22 ods. 3** Slovo "dotknutého" odporúčame vypustiť ako nadbytočné. | O | A |  |
| **ÚPPVII** | **Čl. I § 10 ods. 4** Slovo "ods." je potrebné nahradiť slovom "odsek" v súlade s bodom 22.7. prílohy č. 1 Legislatívnych pravidiel vlády SR. Legislatívnom technická pripomienka | O | A |  |
| **ÚPPVII** | **Čl. I § 2 ods. 2 písm. a)** Slovo "osobitného" navrhujeme nahradiť slovom "všeobecného" z dôvodu všeobecného charakteru predpisu podľa jeho § 1 ods. 3. Za slovo "utajovaných" je potrebné vložiť slovo "skutočností". Odkaz 2) vrátane poznámky pod čiarou k odkazu 2) odporúčame vypustiť ako nadbytočné. | O | A |  |
| **ÚPPVII** | **Čl. I § 17 ods. 1** Upozorňujeme na skutočnosť, že v ustanovení sa uvádza všeobecne záväzný právny predpis, na ktorý sa neodkazuje. | O | A |  |
| **ÚPPVII** | **Čl. I § 31 ods. 2** Upozorňujeme predkladateľa na potrebu doplniť ustanovenie o subjekt, ktorý pokutu ukladá. | O | A |  |
| **ÚPPVII** | **Čl. I § 19 ods. 6** Ustanovenie nejednoznačne identifikuje spôsob preverenia účinnosti opatrení. Žiadame doplniť spôsob preverenia , a to buď v dôvodovej správe alebo priamo v zákone, napr. vykonaním bezpečnostného auditu, penetračného testu a ohodnotenia zraniteľností. | Z | A | Vaša pripomienka bola akceptovaná a ustanovenie bolo preformulované v zmysle pripomienky, doplnená bola aj dôvodová správa. |
| **ÚPPVII** | **Čl. I § 12 ods. 10** Ustanovenie o povinnosti zachovania mlčanlivosti podľa osobitných predpisov odporúčame uvádzať na konci odseku 1 a odsek 10 odporúčame vypustiť. | O | A |  |
| **ÚPPVII** | **Čl. I § 12 ods. 7** Ustanovenie žiadame vypustiť z dôvodu, že nie je vhodné, potrebné ani účelné, aby sa pri spracúvaní osobných údajov úrad vyňal z pôsobnosti zákona o ochrane osobných údajov. | Z | A | Vaša pripomienka nebola akceptovaná z dôvodu, že pripomienka je neodôvodnená. Vhodnosť a účelnosť samostatnej ochrany je dostatočne vyplývajúca už zo samotnej problematiky, nemáme vedomosť o akú účelnosť má v tomto prípade ísť. Ochrana osobných údajov je zabezpečená na vyššej úrovni, GDPR neposkytuje bezpečnostné opatrenia vyššieho charakteru a keďže osobné údaje v rámci informačného systému budú súčasťou informácií klasifikovaných ako V, nie je možné abstrahovať osobné údaje od iných údajov a poskytnúť im tak nižší stupeň ochrany. Úprava ochrany osobných údajov bola preformulovaná v zmysle smernice NIS a Nariadenia GDPR. Po vysvetlení bol rozpor odstránený. |
| **ÚPPVII** | **Čl. I § 33** Úvodnú vetu § 33 odporúčame upraviť napríklad nasledovne: "Úrad vydá všeobecne záväzný právny predpis, ktorým ustanoví". gramatická pripomienka | O | A |  |
| **ÚPPVII** | **Čl. III bod 2** V § 101a ods. 1 slová "na ktorej sa podľa opisu funkčnej nápne vyžaduje vykonávania" odporúčame nahradiť slovami "ktorá podľa opisu funkčnej náplne vyžaduje vykonávanie". gramatická úprava | O | N | Text bol preformulovaný. |
| **ÚPPVII** | **Čl. I § 11 ods. 1** V § 11 ods. 1 odporúčame doplniť nové písm. h) s cieľom určiť povinnosť poskytovateľa základnej služby za zabezpečenie ochrany IS vo svojej pôsobnosti, ktoré znie: "h) zabezpečuje primeranú úroveň ochrany informačného systému organizácií vo svojej pôsobnosti". | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že úlohy prevádzkovateľa základných služieb sú v osobitnom ustanovení. |
| **ÚPPVII** | **Všeobecne k vlastnému materiálu** V súlade s čl. 6 Legislatívnych pravidiel vlády SR je potrebné zvážiť používanie niektorých pojmov v návrhu zákona, napr. "autorita", "reporting". | O | A | Upravené v zmysle Legislatívnych pravidiel vlády SR. |
| **ÚPPVII** | **Čl. I § 28 ods. 9** V uvádzacej vete navrhujeme „vykonáva v potrebnom rozsahu štátnu správu“ nahradiť slovami „plní v potrebnom rozsahu úlohy úradu“ a toto znenie premietnuť aj do čl. V bod 6 § 7 ods. 2 písm. d). Následne tiež navrhujeme v písmene b) za slovo „situácie“ vložiť spojku „alebo“ a v písmene c) za slovo „útoku“ doplniť slová „alebo môže spôsobiť ohrozenie života, zdravia alebo bezpečnosti“. Odôvodnenie: Na odstránenie výkladových sporov navrhujeme pojem „štátna správa“ nahradiť pojmom „úlohy úradu“, aby bolo zrejmé, že v danom prípade ide o zmenu v kompetenciách vo vzťahu k úlohám podľa tohto zákona. Doplnenia písmena b) sa navrhuje z dôvodu pokrytia situácií, kedy dochádza k ohrozeniu obrany štátu, bez ohľadu na to, či je to v čase krízovej situácie alebo nie. Doplnenie písmena c) smeruje k ošetreniu situácií, kedy nejde o teroristický útok, ale hrozí ohrozenie života alebo bezpečnosti štátu. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. Úlohy MOSR v oblasti kybernetickej obrany presunuté do zákona o obrane, kde vytvárajú ucelenú štruktúru pri zabezpečovaní obrany štátu v čase, kedy to zákon o obrane predpokladá. Zákon o KB je tak zákonom upravujúcim kybernetiockú bezpečnosť a minimálne bezpečnostné atribúty na dosiahnutie tejto bezpečnosti v čase mieru. Po vysvetlení bol rozpor odstránený. |
| **ÚPPVII** | **Čl. I § 10 ods. 5** V uvádzacej vete navrhujeme za slová „určenom úradom“ doplniť slová „alebo osobitným predpisom“ s odkazom napríklad na § 7 ods. 6 zákona č. 319/2002 Z.z. v znení neskorších predpisov. Odôvodnenie: Spresňujúca úprava, ktorá zosúlaďuje rozsah prístupu podľa § 10 ods. 5 a podľa navrhovaného § 7 ods. 6 zákona o obrane. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že partneri Národnej jednotky CSIRT boli z textu vypustení. Rozpor bol odstránený. |
| **ÚPPVII** | **Čl. I § 6 ods. 1** z ustanovenia písm. r) nie je zrejmé komu úrad zasiela varovania a čoho sa tieto varovania týkajú. | O | A | Upravené v § 8 ods. 4. |
| **ÚPPVII** | **Čl I § 3 písm. d)** Za slovo „odolávať“ odporúčame doplniť slová „rizikám a“. Zastávame názor, že ide o spresnenie pojmu, kedy bezpečnosťou je stav, pri ktorom systémy odolávajú nielen incidentom, ale aj eliminujú riziká ich vzniku. | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **ÚPPVII** | **Čl I § 10 ods. 5 písm. h)** Žiadame jasne definovať partnerov Národnej jednotky CSIRT, resp. presný spôsob ich určenia, výberu. | Z | N | Na základe rozporového konania s MO SR, ako vecne príslušným subjektom pre oblasť obrany SR, boli vypustené z čl. I všetky ustanovenia, ktoré sa týkali zabezpečovania obrany. Ustanovenie § 28 bolo vo veciach obrany vypustené bez náhrady a zvyšné ustanovenia boli obsiahnuté v upravenom § 27 (viď vyššie). MO SR súhlasilo s vypracovaním vlastných novelizačných článkov zákona o obrane a zákona o ozbrojených silách tak, aby tie zákony tvorili spolu jeden systém zabezpečovania kybernetickej bezpečnosti. Články, ktoré MO SR navrhne, Vám doručíme hneď po ich obdržaní. Z dôvodu vysporiadania rozporných ustanovení s MO SR a úpravy samostatných ustanovení novelizačných bodov MO SR považujeme pripomienky k čl. I za bezpredmetné. Po doručení textácie z MO SR Vám táto bude preposlaná a v prípade kolízie Vám môžeme zorganizovať stretnutie s MO SR. Po posúdení upraveného textu považuje ÚPVII rozpor za odstránený. |
| **ÚPPVII** | **Čl. I § 29 ods. 6** Žiadame na koniec vety odseku 6 za slovo „konfiguráciu“ doplniť text „pod dohľadom zástupcu kontrolovaného subjektu. Úrad zodpovedá aj za škodu spôsobenú príslušníkmi úradu pri výkone kontroly v dôsledku dočasných zmien hardvérovej alebo softvérovej konfigurácie.“. Odôvodnenie: Uvedené ustanovenie dáva úradu neprimerané kompetencie, znižuje bezpečnosť kontrolovaných IS vzhľadom na kompromitáciu administratívnych účtov. Zmenou konfigurácie môže dôjsť k zníženiu bezpečnosti alebo ohrozeniu funkčnosti IS. Rovnako nie je jasné kto preberá za vzniknuté škody zodpovednosť. Žiadame do ustanovenia doplniť, že prípadné zmeny konfigurácie sa môžu vykonávať len pod dohľadom zástupcu kontrolovaného subjektu a rovnako, že úrad zodpovedá za škodu vzniknutú v dôsledku týchto zmien pri výkone kontroly. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že rozporný text bol vypustený a nahradený novým znením ku ktorému neboli vznesené výhrady zo stranu ÚPVII. Rozpor bol odstránený. |
| **ÚPPVII** | **Čl. I § 10 ods. 1** Žiadame nahradiť slovné spojenie "efektívne riadenie, evidenciu" za slovné spojenie "efektívne riadenie, koordináciu, evidenciu". Je potrebné na národnej úrovni zabezpečiť najmä koordináciu. | Z | A |  |
| **ÚPPVII** | **Čl. I § 29 ods. 9** Žiadame slová „zamestnancom kontrolovaného subjektu a vedúcemu kontrolovaného subjektu“ nahradiť slovami „kontrolovanému subjektu“. Odôvodnenie: Podľa zákona NR SR č. 10/1996 Z.z. sa pokuta ukladá kontrolovanému subjektu a nie jeho zamestnancom. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. Úlohy MOSR v oblasti kybernetickej obrany presunuté do zákona o obrane, kde vytvárajú ucelenú štruktúru pri zabezpečovaní obrany štátu v čase, kedy to zákon o obrane predpokladá. Zákon o KB je tak zákonom upravujúcim kybernetickú bezpečnosť a minimálne bezpečnostné atribúty na dosiahnutie tejto bezpečnosti v čase mieru. Po vysvetlení bol rozpor odstránený. |
| **ÚPPVII** | **Čl. I § 9 ods. 3** Žiadame slovné spojenie "informácie v požadovanom rozsahu" nahradiť slovným spojením "informácie v primeranom rozsahu". Pôvodná forma znamená riziko svojvoľného určenia rozsahu informácie nad rámec nevyhnutnosti a z dôvodu vysokého stupňa centralizácie citlivých informácií, čo predstavuje zbytočné bezpečnostné riziko. | Z | ČA | Vaša pripomienka bola čiastočne akceptovaná a upravená v zmysle pripomienky MVSR a nahradená slovom "potrebnom". Rozpor bol odstránený. |
| **ÚPPVII** | **Čl. I § 13 ods. 8** Žiadame slovné spojenie "môže na základe žiadosti uznať" nahradiť slovným spojením "na základe žiadosti uzná". | Z | A |  |
| **UpREKaPŠ** | **Čl. 1 - § 34 ods. 1** Odporúčame zvážiť predmetnú úpravu. Odôvodnenie: V prípade ak predkladateľ návrhu zákona vylúči všeobecný predpis o správnom konaní, je potrebné ku každému takémuto konaniu dopracovať procesné inštitúty (ako napr. doručovanie, odvolanie atď.) | O | A |  |
| **UpREKaPŠ** | **Čl. I - § 28 ods. 1** Predmetné ustanovenie odporúčame zosúladiť požiadavkami kladenými na zákon podľa Čl. 6 Legislatívnych pravidiel vlády. Odôvodnenie: Predmetné ustanovenie z pohľadu Úradu pre reguláciu elektronických komunikácií a poštových služieb nespĺňa tak požiadavku zrozumiteľnosti ako aj normatívnosti (slová „ak by v jeho dôsledku mohlo dôjsť“). | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **UpREKaPŠ** | **Čl. 1 - § 29 ods. 6** Predmetné ustanovenie požadujeme vypustiť Odôvodnenie: Úrad pre reguláciu elektronických komunikácií a poštových služieb upozorňuje, že vstup do komunikačných a informačných systémov do úrovne správcu systému, vrátane oprávnenia dočasne zmeniť hardvérovú alebo softvérovú konfiguráciu bez dôkladnej znalosti uvedených systémov a bez povolenia podniku by mohol spôsobiť dlhotrvajúci výpadok alebo narušiť softvérové funkcie systému. Taktiež upozorňujeme, že takýto zásah neupravuje ani samotná smernica č. 2016/1148/ES. | Z | A |  |
| **UpREKaPŠ** | **Čl. 1 - § 18 ods. 6**  Predmetné ustanovenie požadujeme vypustiť. Odôvodnenie: Vzhľadom na skutočnosť, že povinnosti vzťahujúce sa na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb by sa však nemali uplatňovať na podniky poskytujúce verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby v zmysle smernice Európskeho parlamentu a Rady 2002/21/ES (3), ktoré podliehajú osobitným požiadavkám týkajúcim sa bezpečnosti a integrity stanoveným v uvedenej smernici Úrad pre reguláciu elektronických komunikácií a poštových služieb nevidí dôvod, prečo by prevádzkovateľ základnej služby mal informovať podnik poskytujúci elektronické komunikačné služby. | Z | N | Záver: po vysvetlení aj za účasti MDaVSR rozpor odstránený. |
| **UpREKaPŠ** | **Čl. 9** Predmetný článok požadujeme vypustiť. Odôvodnenie: Úrad pre reguláciu elektronických komunikácií a poštových služieb upozorňuje na skutočnosť, že podľa ustanovenia článku 1 ods. 3 smernice č. 2016/1148/ES sa „bezpečnostné a oznamovacie požiadavky stanovené v tejto smernici nevzťahujú na podniky, ktoré podliehajú požiadavkám článkov 13a a 13b smernice 2002/21/ES, ani na poskytovateľov dôveryhodných služieb, na ktorých sa vzťahujú požiadavky článku 19 nariadenia (EÚ) č. 910/2014.“ V tejto súvislosti upozorňujeme, že úprava bezpečnosti podľa návrhu zákona o kybernetickej bezpečnosti je odlišnou úpravou ako je úprava podľa vyššie uvedených článkov 13a a 13b smernice č. 2002/21/ES. Taktiež upozorňujeme na skutočnosť, že recitál (7) smernice 2016/1148/ ES uvádza, že povinnosti vzťahujúce sa na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb by sa však nemali uplatňovať na podniky poskytujúce verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby v zmysle smernice Európskeho parlamentu a Rady 2002/21/ES (3), ktoré podliehajú osobitným požiadavkám týkajúcim sa bezpečnosti a integrity stanoveným v uvedenej smernici. Keďže ide o odlišné a od seba nezávislé právne úpravy, žiadame, aby sa z návrhu zákona vypustila akákoľvek zmena zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov. Okrem iného upozorňujeme na bod 38 prílohy č. 1 k Legislatívnym pravidlám vlády „Legislatívno-technické pokyny“, podľa ktorého poznámku pod čiarou spravidla nemožno novelizovať v samostatnom novelizačnom bode. Taktiež uvádzame, že podmienkou získania práv podľa § 55 ods. 6 zákona č. 351/2011 Z. z. o elektronických komunikáciách je naplnenie znakov „iného orgánu štátu“ uvedených v predmetnom ustanovení a nie citácia predpisu v poznámke pod čiarou, ktorá nemá normatívny charakter. | Z | N | Záver: Vypustené ustanovenia týkajúce sa zákona č. 351/2011 ZZ z čl. I. Po dohode s ÚpREKaPŠ upravené znenie novelizačného bodu k zákonu č. 351/2011 ZZ a upravená príloha č. 1, vypustený telekomunikačný sektor (akceptovanie aj pripomienky RÚZ). Problematika potreby hlásenia incidentov a spolupráce s NBÚ, ako aj prístupu k telekomunikačnému tajomstvu vysvetlená v rámci rozporových konaní a mejlovou komunikáciou a vzhľadom na túto potrebu došlo ku konsenzu a úprave textu návrhu zákona. MDaVSR precizovalo text a ÚpREKaPŠ navrhlo znenie novely zákona č. 351/2011 ZZ v zmysle uzavretej dohody na rozporovom konaní. |
| **UpREKaPŠ** | **k celému návrhu** Úrad pre reguláciu elektronických komunikácií a poštových služieb upozorňuje na skutočnosť, že podľa ustanovenia článku 1 ods. 3 smernice č. 2016/1148/ES sa „Bezpečnostné a oznamovacie požiadavky stanovené v tejto smernici nevzťahujú na podniky, ktoré podliehajú požiadavkám článkov 13a a 13b smernice 2002/21/ES, ani na poskytovateľov dôveryhodných služieb, na ktorých sa vzťahujú požiadavky článku 19 nariadenia (EÚ) č. 910/2014.“ V tejto súvislosti upozorňujeme, že úprava bezpečnosti podľa návrhu zákona o kybernetickej bezpečnosti je odlišnou úpravou ako je úprava podľa vyššie uvedených článkov 13a a 13b smernice č. 2002/21/ES. Z uvedeného dôvodu požadujeme aby v celom návrhu zákona o kybernetickej bezpečnosti boli vypustené všetky úpravy, ktoré zasahujú do úpravy bezpečnosti a integrity sietí podľa zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov. Taktiež upozorňujeme na skutočnosť, že recitál (7) smernice 2016/1148/ ES uvádza, že povinnosti vzťahujúce sa na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb by sa však nemali uplatňovať na podniky poskytujúce verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby v zmysle smernice Európskeho parlamentu a Rady 2002/21/ES, ktoré podliehajú osobitným požiadavkám týkajúcim sa bezpečnosti a integrity stanoveným v uvedenej smernici. | Z | A | Vypustené ustanovenia týkajúce sa zákona č. 351/2011 ZZ z čl. I. Po dohode s ÚpREKaPŠ upravené znenie novelizačného bodu k zákonu č. 351/2011 ZZ a upravená príloha č. 1, vypustený telekomunikačný sektor (akceptovanie aj pripomienky RÚZ). Problematika potreby hlásenia incidentov a spolupráce s NBÚ, ako aj prístupu k telekomunikačnému tajomstvu vysvetlená v rámci rozporových konaní a mejlovou komunikáciou a vzhľadom na túto potrebu došlo ku konsenzu a úprave textu návrhu zákona. MDaVSR precizovalo text a ÚpREKaPŠ navrhlo znenie novely zákona č. 351/2011 Z.z. v zmysle uzavretej dohody na rozporovom konaní. |
| **UpREKaPŠ** | **Čl. 1 - § 2 ods. 1** V druhej vete predmetného ustanovenia poukazujeme na potrebu upraviť text v súlade s Čl. 6 Legislatívnych pravidiel vlády. Odôvodnenie: Podľa Čl. 6 Legislatívnych pravidiel vlády návrh zákona musí byť zrozumiteľný a musí obsahovať len ustanovenia s normatívnym obsahom. Slová „rovnocenné alebo vyššie požiadavky“ a „môžu sa použiť“ z nášho pohľadu nespĺňajú požadované požiadavky kladené na zákon. | O | A |  |
| **UpREKaPŠ** | **Čl. 1 - § 2 ods. 1** V predmetnom ustanovení považujem za potrebné vypustiť z poznámky pod čiarou 1) ustanovenia § 64 až 68 zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov. V tejto súvislosti je potrebné upraviť aj dôvodovú správu k predmetnému ustanoveniu tak, aby neodkazovala na úpravu zákona č. 351/2011 Z. z. o elektronických komunikáciách. Odôvodnenie: Úprava bezpečnosti podľa návrhu zákona o kybernetickej bezpečnosti je odlišnou úpravou ako je úprava podľa vyššie uvedených článkov 13a a 13b smernice č. 2002/21/ES. Predmetná odlišnosť je vyjadrená aj v čl. 1 ods. 3 smernice č. 2016/1148/ES. | Z | A |  |
| **UpREKaPŠ** | **Čl. 1 - § 10 ods. 5 písm. f)** V predmetnom ustanovení požadujeme vypustiť písm. f) - Úrad pre reguláciu elektronických komunikácií a poštových služieb z výpočtu subjektov majúcich prístup do neverejnej časti jednotného informačného systému. Odôvodnenie: Upozorňujeme na skutočnosť, že úprava bezpečnosti podľa návrhu zákona o kybernetickej bezpečnosti je odlišnou úpravou ako je úprava podľa vyššie uvedených článkov 13a a 13b smernice č. 2002/21/ES a povinnosti vzťahujúce sa na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb by sa však nemali uplatňovať na podniky poskytujúce verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby v zmysle smernice Európskeho parlamentu a Rady 2002/21/ES (3), ktoré podliehajú osobitným požiadavkám týkajúcim sa bezpečnosti a integrity stanoveným v uvedenej smernici. Vzhľadom na uvedené skutočnosti, z nášho pohľadu neexistuje dôvod, aby Úrad pre reguláciu elektronických komunikácií a poštových služieb bol na základe svojej vecnej pôsobnosti zaradený medzi subjekty s prístupom k neverejnej časti jednotného informačného systému, preto požadujeme Úrad pre reguláciu elektronických komunikácií a poštových služieb z predmetného ustanovenia vypustiť. | Z | A |  |
| **UpREKaPŠ** | **prílohe č. 1** V prílohe č. 1 k návrhu zákona požadujeme vypustiť z predmetnej tabuľky celú položku č. 9 „Sektor elektronických komunikácií“. Odôvodnenie: Upozorňujeme na skutočnosť, že podniky poskytujúce elektronických komunikačných služieb (takisto sektor elektrokomunikačných služieb) z nášho pohľadu nenapĺňajú znaky, ktoré definujú prevádzkovateľa základnej služby tak ako ich ustanovujú článok 4 bod 4 a článok 5 ods. 2 smernice č. 2016/1148/ES. Z uvedeného dôvodu sa tak predmetné podniky ako aj celý sektor nenachádza ani v prílohe č. II „TYPY SUBJEKTOV NA ÚČELY ČLÁNKU 4 BODU 4“. Taktiež, z pohľadu Úradu pre reguláciu elektronických komunikácií a poštových služieb, by príloha č. 1 bola v obsahovom rozpore s navrhovaným ustanovením § 5 písm. c), kde je uvedený taxatívny výpočet vecne príslušných autorít a Úrad pre reguláciu elektronických komunikácií a poštových služieb v nich absentuje. | Z | A |  |
| **ÚPVSR** | **celému materiálu** Bez pripomienok. | O | A |  |
| **ÚVO** | **§ 28 ods. 1** Navrhujeme prehodnotiť znenie § 28 ods. 1 a zvážiť odkaz na čl. 1 ods. 3 ústavného zákona č. 227/2002 Z. z. Po komparácií českej textácie zákona o kybernetickej bezpečnosti máme za to, že pod stavom zníženia kybernetickej bezpečnosti sa rozumie stav, v ktorom je vo veľkom rozsahu ohrozená bezpečnosť informácií v informačných systémoch verejnej správy alebo bezpečnosť a integrita služieb. Na základe uvedeného by mohlo dôjsť k porušeniu alebo ohrozeniu záujmov Slovenskej republiky v zmysle zákona o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov. Odôvodnenie: textácia "bezpečnosti" v Čl. 1 ods. 3 Ústavného zákona č. 227/2002 Z. z. sa javí ako príliš všeobecná a nepresná vzhľadom na špecifiká kybernetického priestoru. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **ÚVO** | **§ 28 ods. 4** za účelom zachovania transparentnosti a informovanosti verejnosti považujeme za dôležité v návrhu zákona bližšie špecifikovať spôsob "ústneho prehlásenia", alternatívne tento spôsob z návrhu vypustiť. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **ÚVSR** | **Čl. IV k bodu 6** § 7, ods. 4), písm. b), bod 2 – Žiadame znenie ustanovenia z návrhu zákona vypustiť. Odôvodnenie: V zákone č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších zmien, ani v návrhu novely predmetného zákona podľa Čl. VIII predkladaného návrhu zákona o kybernetickej bezpečnosti, nie sú Ministerstvu obrany SR vymedzené žiadne kompetencie ani vecná pôsobnosť. | Z | N | Po dohode všetkých subjektov sa MOSR zaviazalo novelizovať právne predpisy v podobe nového textu. |
| **ÚVSR** | **Čl.IV k bodu 6** § 7, ods. 5) – Žiadame zo znenia ustanovenia návrhu zákona vypustiť povinnosť prevádzkovateľa prvku kritickej infraštruktúry poskytnúť centru informácie. Konkrétne navrhujeme vypustiť slová „a prevádzkovateľ prvku kritickej infraštruktúry 9e). Odôvodnenie: V zákone č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších zmien, ani v návrhu novely predmetného zákona podľa Čl. VIII predkladaného návrhu zákona o kybernetickej bezpečnosti, nie sú Ministerstvu obrany SR vymedzené žiadne kompetencie ani vecná pôsobnosť. | Z | N | Po dohode všetkých subjektov sa MOSR zaviazalo novelizovať právne predpisy v podobe nového textu. |
| **ÚVSR** | **Čl. IV k bodu 6**  § 7, ods. 6) – Žiadame text ustanovenia nahradiť textom v nasledujúcom znení: „Na účely zabezpečenia plnenia úloh podľa tohto zákona má centrum priamy prístup k obsahu jednotného informačného systému kybernetickej bezpečnosti podľa osobitného predpisu9g), v rozsahu vecnej pôsobnosti ministerstva, v elektronickej podobe a v reálnom čase.“ Odôvodnenie: Spresnenie vymedzenia rozsahu prístupu k jednotnému informačnému systému kybernetickej bezpečnosti. | Z | N | Po dohode všetkých subjektov sa MOSR zaviazalo novelizovať právne predpisy v podobe nového textu. |
| **ÚVSR** | **Čl. I §3** Definície pojmov odporúčame zosúladiť s termínmi podľa Terminologického slovníka krízového riadenia Bezpečnostnej rady Slovenskej republiky. | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **ÚVSR** | **Čl. I § 3, písm. d)**  Definíciu pojmu „kybernetická bezpečnosť“ odporúčame nahradiť definíciou z Terminologického slovníka krízového riadenia Bezpečnostnej rady Slovenskej republiky, t. j. „bezpečnosť kybernetického priestoru“. Odôvodnenie: Podľa Terminologického slovníka krízového riadenia Bezpečnostnej rady Slovenskej republiky sa pod pojmom „bezpečnosť“ rozumie stav spoločenského, prírodného, technického, technologického systému alebo iného systému, ktorý v konkrétnych vnútorných a vonkajších podmienkach umožňuje plnenie určených funkcií a ich rozvoj v záujme človeka a spoločnosti. Kybernetickou bezpečnosťou nie je len stav, v ktorom iba aktíva kybernetického priestoru, t. j. siete a informačné systémy pre účely návrhu zákona, sú schopné odolávať kybernetickým bezpečnostným incidentom. Predmetom kybernetickej bezpečnosti je aj ochrana ostatných aktív spoločnosti pred kybernetickými hrozbami a zraniteľnosťami. | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **ÚVSR** | **Čl. I § 3, písm. h)**  Definíciu pojmu „prevádzkovateľ základnej služby“ odporúčame formulovať jednoznačne a zosúladiť s prílohou č. 1 návrhu zákona. Odôvodnenie: V prílohe č. 1 návrhu zákona, v stĺpci PZS (skratka PZS zrejme znamená „prevádzkovateľ základnej služby“), sú uvedení napríklad manažéri infraštruktúry. Podľa nášho názoru tento pojem nevyjadruje právnické osoby, resp. fyzické osoby podnikateľov, ale funkcie fyzických osôb pôsobiacich v rámci týchto subjektov. Ďalej v definícii pojmu „prevádzkovateľ základnej služby“ sú uvedení správcovia ISVS. V prílohe č. 1 zákona sú pre sektor verejná správa v stĺpci PZS uvedení správcovia a prevádzkovatelia ISVS. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná z dôvodu, že bol upravený celý § 3 a boli zavedené nové pojmy. |
| **ÚVSR** | **Čl. I § 28 ods. 7)**  Druhú časť vety, vrátane odkazov na právne predpisy, navrhujeme upraviť nasledovne: „požiada vládu o vyhlásenie krízovej situácie“ nahradiť textom „predloží predsedovi Bezpečnostnej rady SR informáciu o predpokladaných dopadoch kybernetického ohrozenia na bezpečnosť štátu ako podklad na riešenie krízovej situácie“. Zároveň navrhujeme vložiť za slovo „štátu“ odkaz č. 27 s textom „čl. 1 ods. 3 ústavného zákona č. 227/2002 Z. z.“ a za slovo situácie text „čl. 1 ods. 4 ústavného zákona č. 227/2002 Z. z., § 2 písm. a) zákona č. 387/2002 Z. z.“. Odôvodnenie: Obdobne ako v predchádzajúcej pripomienke je potrebné informovanie nasmerovať na predsedu Bezpečnostnej rady SR. Ostatný text sa navrhuje zosúladiť so znením ustanovení citovaných právnych predpisov. | Z | A |  |
| **ÚVSR** | **Čl. I V § 10 ods. (1)**  Na konci odseku navrhujeme vypustiť text „výnimočného stavu a núdzového stavu“. Odôvodnenie: Jedná sa o duplicitu, nakoľko v tej istej vete uvádzaný text „mimo času vojny a vojnového stavu“ významovo zahŕňa aj výnimočný stav aj núdzový stav. | O | A |  |
| **ÚVSR** | **Čl. I § 3, písm. f)**  Návrh definície odporúčame zosúladiť s definíciou pojmu „bezpečnostný incident“ podľa Terminologického slovníka krízového riadenia Bezpečnostnej rady, t. j. „kybernetickým bezpečnostným incidentom je udalosť, ktorej dôsledkom je narušenie bezpečnosti aktíva kybernetickými prostriedkami alebo porušenie kybernetickej bezpečnostnej politiky subjektu“. Odôvodnenie: Navrhnutú definíciu pojmu „kybernetický bezpečnostný incident“ považujeme za zmätočnú. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že bol upravený celý § 3 a boli zavedené nové pojmy. |
| **ÚVSR** | **Čl. I § 3, písm. e)**  Návrh definície odporúčame zosúladiť s definíciou pojmu „riziko“, uvedenom v Terminologickom slovníku krízového riadenia Bezpečnostnej rady. Navrhujeme nasledujúce znenie definície pojmu „kybernetické riziko“: miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami. Ďalej § 3 odporúčame rozšíriť (v znení zosúladenom s Terminologickým slovníkom krízového riadenia Bezpečnostnej rady) o definície nasledujúcich pojmov: Kybernetické ohrozenie – aktivovaná kybernetická hrozba v priestore a čase. Kybernetická hrozba - hrozba voči aktívam kybernetického priestoru alebo hrozba realizovateľná kybernetickými prostriedkami. Hrozba - objektívne existujúca možnosť, ktorej naplnenie je schopné spôsobiť negatívny dôsledok. Odôvodnenie: Uvedené pojmy sú použité v § 28 návrhu zákona, ale v § 3 návrhu zákona nie sú definované. Vo všeobecnosti pojem „riziko“ vyjadruje subjektívnu mieru ohrozenia aktíva, resp. vzniku nežiaduceho javu, ako aj jeho dôsledkov. Text v návrhu zákona obsahuje vágnu formuláciu: každá primerane rozpoznateľná okolnosť alebo udalosť....Nie je špecifikované čo sa rozumie pod formuláciou „primerane rozpoznateľná okolnosť“. Formulácia: „okolnosť alebo udalosť, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť“ svojim zmyslom znamená hrozbu. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **ÚVSR** | **Čl. I § 11, ods. (1), písm. g)**  Navrhujeme preformulovať z dôvodu nesprávneho skloňovania. | O | A |  |
| **ÚVSR** | **Čl. I § 28** Navrhujeme upraviť text tak, aby jednoznačne vymedzoval kompetencie na vykonávanie štátnej správy a prijímanie záverov pri vyhodnocovaní informácií o kybernetickom bezpečnostnom incidente. V § 28 ods. 9 slovné spojenie „v potrebnom rozsahu“ nie je dostatočné vymedzenie na vykonávanie štátnej správy. V § 28 ods. 9 písm. c) v texte nie je stanovený orgán, ktorý vyhodnotí informácie o kybernetickom bezpečnostnom incidente, že sa môže jednať o kybernetický terorizmus. Odôvodnenie: Uvedené ustanovenia môžu viesť k nejednoznačnému výkladu, ktorý v tejto oblasti, v ktorej dôležitú úlohu zohráva aj časový faktor, môže spomaliť plnenie opatrení na odstránenie kybernetickej hrozby. | Z | A | Ustanovenie bolo vypustené, v čl. I je teda upravený len stav kybernetickej ochrany a nie obrany. Bol vypustený stav kybernetického ohrozenia a aj úlohy MOSR. MOSR sa zaviazalo novelizovať právne predpisy (zákon o ozbrojených silách a zákon o obrane) vo svojej vecnej pôsobnosti tak, aby zohľadňovali potreby zabezpečenia obrany vo vzťahu ku kybernetickému priestoru a súhlasilo s vypustením kompetencií MOSR (teda problematiky obrany, nie ochrany, ako je predmet úpravy v zákone o kybernetickej bezpečnosti návrhu zákona o kybernetickej bezpečnosti), keďže takáto úprava pri dodržaní legislatívno-technických zásad v záujme zabezpečenia riadneho výkonu verejnej moci má byť upravená v predpise vo vecnej pôsobnosti povinného štátneho orgánu. Po vysvetlení bol rozpor odstránený. |
| **ÚVSR** | **Čl. I § 12 ods. (1)** Navrhujeme v druhej vete bodku nahradiť bodkočiarkou a doplniť tieto slová „povinnosť mlčanlivosti sa nevzťahuje na oznámenie kriminality alebo inej protispoločenskej činnosti“. Odôvodnenie: Zosúladenie povinnosti mlčanlivosti so znením povinnosti mlčanlivosti štátneho zamestnanca ustanovenej v zákone č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov a zamestnanca pri výkone práce vo verejnom záujme ustanovenej v zákone č. 552/2003 Z. z. o výkone práce vo verejnom záujme v znení neskorších predpisov. Odlišná úprava tejto povinnosti by mohla spôsobovať problémy pri jej dodržiavaní podľa tohto zákona a podľa uvedených právnych predpisov. | Z | A | Do textu bol doplnený chýbajúci zákon (poznámka pod čiarou k odkazu 15), text bol preformulovaný v zmysle pripomienok ostatných subjektov a vysvetlený v dôvodovej správe. Váš predpoklad v texte pripomienky je nesporný a z navrhovaného znenia vyplýva, že sa týka aj FO – zamestnancov. Nie je preto potrebné znovu opakovať právny stav vyjadrený v odseku 3. Navrhovaná právna úprava je výsledkom rokovaní kompetentných vecne príslušných subjektov a bude predmetom obšírnejšieho vysvetlenia aj v dôvodovej správe. |
| **ÚVSR** | **Čl. I § 28 ods. 6)**  Navrhujeme vypustiť slovo „priebežne“. Zároveň v tomto odseku navrhujeme nahradiť slovo “vládu” slovným spojením „predsedu Bezpečnostnej rady SR“. Odôvodnenie Slovo priebežne je nadbytočné, nakoľko z predchádzajúce textu vyplýva, že popisované činnosti prebiehajú v čase, takže aj informovanie o ich vykonávaní bude prebiehať v čase až do ukončenia činnosti. Informácie je potrebné nasmerovať na predsedu Bezpečnostnej rady SR, pretože tento orgán plní poradnú funkciu v oblasti bezpečnosti smerom k vláde SR, k čomu má vytvorený aj Výbor pre kybernetickú bezpečnosť na úrovni expertov z jednotlivých rezortov. | Z | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené, v čl. I je teda upravený len stav kybernetickej ochrany a nie obrany. Bol vypustený stav kybernetického ohrozenia a aj úlohy MOSR. MOSR sa zaviazalo novelizovať právne predpisy (zákon o ozbrojených silách a zákon o obrane) vo svojej vecnej pôsobnosti tak, aby zohľadňovali potreby zabezpečenia obrany vo vzťahu ku kybernetickému priestoru a súhlasilo s vypustením kompetencií MOSR (teda problematiky obrany, nie ochrany, ako je predmet úpravy v zákone o kybernetickej bezpečnosti návrhu zákona o kybernetickej bezpečnosti), keďže takáto úprava pri dodržaní legislatívno-technických zásad v záujme zabezpečenia riadneho výkonu verejnej moci má byť upravená v predpise vo vecnej pôsobnosti povinného štátneho orgánu. Po vysvetlení rozor odstránený. |
| **ÚVSR** | **k celému materiálu** Navrhujeme vytvoriť nový § 8, ktorý by sa týkal Vládnej jednotky CSIRT a to v nasledujúcom znení: „§ 8 Vládna jednotka CSIRT (1) Vládna jednotka CSIRT zabezpečuje úlohy jednotky CSIRT podľa § 16 a príloh č. 1 a 2 v sektore Verejná správa pre podsektor ISVS. (2) Vládna jednotka CSIRT musí spĺňať podmienky podľa § 14. (3) Zriaďovateľom Vládnej jednotky CSIRT je Úrad vlády Slovenskej republiky.“. Súčasne navrhujeme primerane prečíslovať nasledujúce paragrafy a vnútorné odkazy na ne. V nadväznosti na nové ustanovenie, navrhujeme tomu prispôsobiť aj znenie § 7 ods. 1, kde sa uvedie aj vládna jednotka CSIRT. Odôvodnenie: Úrad vlády SR plní jedinečné úlohy pri zabezpečení infraštruktúry pre realizáciu e-služieb verejnej správy a elektronickej komunikácie verejnej správy na účely výkonu verejnej moci. Podľa zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy je správcom (organizácia NASES prevádzkovateľom): privátnej vládnej dátovej siete orgánov verejnej správy - Govnet, Centrálnej informačnej infraštruktúry a Ústredného portálu verejnej správy. Podľa zákona č. 305/2013 Z.z. o e-Governmente je Úrad vlády SR správcom a organizácia NASES prevádzkovateľom kľúčových informačných systémov pre podporu výkonu verejnej moci elektronicky (prístupový bod ÚPVS a spoločné moduly: modul elektronických stránok, centrálnej elektronickej podateľne, elektronických formulárov, elektronického doručovania, dlhodobého uchovávania, príslušné časti modulu úradnej komunikácie, autentifikačný a notifikačný modul). Aj na základe vyššie uvedených právnych predpisov je vhodné, aby bol pre sektor Verejná správa a podsektor ISVS vytvorená samostatná Vládna jednotka CSIRT pre uvedenú oblasť. | Z | A | Pripomienka bola akceptovaná a požiadavka a zapracovaná do textu návrhu zákona. |
| **ÚVSR** | **k celému materiálu** Navrhujeme vzhľadom na nové znenie § 8 (Vládna jednotka CSIRT) uvedené premietnuť aj do prechodných ustanovení návrhu zákona. (Navrhujeme odklad aspoň 2 roky na účely zriadenia vládnej jednotky CSIRT). | O | ČA | Prechodné ustanovenia upravené v zmysle doručených pripomienok. |
| **ÚVSR** | **Čl. IV k bodu 6.** Navrhujeme znenie „objektov obrannej infraštruktúry (§ 27 ods. 1)“ nahradiť slovami „objektov obrannej infraštruktúry (§ 27 ods. 5)“ a to v celom texte čl. IV bodu 6. Odôvodnenie: Navrhujeme lepšiu špecifikáciu znenia § 7 s tým, že Ministerstvo obrany SR bude na účely kybernetickej obrany vykonávať pôsobnosť nad objektmi, ktoré určuje vláda SR podľa § 6 písm. f). Uvedené korešponduje aj so znením § 27 ods. 5, keďže Ministerstvo obrany SR zodpovedá za obranu uvedených objektov. | Z | N | Po dohode všetkých subjektov sa MOSR zaviazalo novelizovať právne predpisy v podobe nového textu. |
| **ÚVSR** | **Čl. I § 5**  navrhujeme znenie ustanovenia rozšíriť o písm. d) „ministerstvá a ostatné ústredné orgány štátnej správy¹¹)“. Odôvodnenie: Navrhujeme uvedené znenie zosúladiť s § 35 ods.3 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov. | Z | A | Vaša pripomienka bola akceptovaná a text upravený. |
| **ÚVSR** | **Čl. I § 4, ods. 5)**  Odporúčame do textu vety medzi slová „prvkom“ a „kultúry“ vložiť nasledujúci text: „kultúry správania sa v kybernetickom priestore, ako aj“. Odôvodnenie: Kultúru správania sa v kybernetickom priestore považujeme za významný fenomén formovania povedomia bezpečnosti kybernetického priestoru. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **ÚVSR** | **Čl.I § 2, ods. 2), písm. a)**  odporúčame na konci vety doplniť slovo „skutočností“. Odôvodnenie: Legislatívno-technická pripomienka. | O | A |  |
| **ÚVSR** | **čl. I § 14, ods. 1) a ods. 2)**  Odporúčame slovo „preukazuje“ nahradiť slovom „preukáže“. Odôvodenie: Navrhujeme precizovanie uvedených ustanovení. | O | A |  |
| **ÚVSR** | **Čl. I § 9 ods. (2), písm. i)**  Odporúčame slovo „rôznych“ z textu vypustiť. Odôvodnenie: Súčasné znenie s vyššie uvedeným znením považujeme za nadbytočné a zmätočné. | O | A |  |
| **ÚVSR** | **Čl. I § 13, ods. (3)**  Odporúčame text „§ 15“ nahradiť textom“§ 14“ Odôvodnenie: § 15 rieši povinnosti prevádzkovateľa základných služieb. Podmienky akreditácie jednotky CSIRT rieši § 14. | O | A |  |
| **ÚVSR** | **Čl. I § 9 ods. (2), písm. h)**  Odporúčame text preformulovať. Odôvodnenie: Súčasnú formuláciu „riziko na účely identifikácie rizík“ považujeme za zmätočnú. | O | N | Vaša pripomienka nebola akceptovaná. Vysvetlenie poskytuje dôvodová správa. |
| **ÚVSR** | **Čl. I § 10, ods. (4)**  Odporúčame text ustanovenia nahradiť textom v nasledujúcom znení: Centrálny systém včasného varovania je informačný systém, ktorý zaisťuje včasnú výmenu informácií o kybernetických hrozbách, zraniteľnostiach, bezpečnostných incidentoch a rizikách s nimi spojených medzi úradom a subjektmi podľa odseku 5 a poskytujú sa z neho nevyhnutné informácie v rozsahu podľa ods. 2 písmeno j). Odôvodnenie: Hrozby a zraniteľnosti považujeme, za významné faktory bezpečnosti. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná. V texte bolo doplnené slovo "o hrozbách". |
| **ÚVSR** | **Čl. I § 8** odporúčame text ustanovenia preformulovať. Odôvodnenie: Celý text znenia je jediná veta na 11 riadkoch. Obsah je ťažko zrozumiteľný. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený a zaradený medzi úlohy úradu z dôvodu duplicitnej úlohy v zákone na účely konkrétnej definície stanovených opatrení v oblasti medzinárodných vzťahov a spolupráce. |
| **ÚVSR** | **Čl. I § 32, ods. 13)**  Odporúčame v návrhu zákona špecifikovať subjekt, ktorý je odvolacím orgánom v záležitostiach správneho konania vo veciach podľa návrhu tohto zákona. Odôvodnenie: Z návrhu zákona nie je zrejmé, kto koná v druhom stupni. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že odvolacím orgánom je úrad. |
| **ÚVSR** | **Čl. I § 29, ods. 11)** Odporúčame v návrhu zákona špecifikovať subjekt, ktorý je odvolacím orgánom v záležitostiach správneho konania vo veciach podľa návrhu tohto zákona. Odôvodnenie: Z návrhu zákona nie je zrejmé, kto koná v druhom stupni. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu nahradenia novým znením textu, ktorý bol preformulovaný aj vzhľadom na pripomienky ostatných subjektov. Národný bezpečnostný úrad je ústredným orgánom štátnej správy, konajúcim v prvom aj druhom stupni. |
| **ÚVSR** | **Čl. I § 28, ods. 1)**  Odporúčame význam pojmov: „hrozba, riziko ohrozenia“ špecifikovať v návrhu zákona alebo uviesť odkaz na iný zdroj. Odôvodnenie: V texte ustanovenia sa vyskytujú pojmy „hrozba, riziko ohrozenia“ bez uvedenia, čo sa pod týmito pojmami rozumie. Navrhujeme precizovanie uvedeného pojmu. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **ÚVSR** | **čl. I § 9, ods. (3)** Odporúčame znenie ustanovenia upraviť. Odôvodnenie: Sme toho názoru, že na vypracovaní národnej stratégie kybernetickej bezpečnosti sa podľa § 35 ods. 3 zákona č. 575/2001 majú podieľať aj ministerstvá a ostatné ústredné orgány štátnej správy, nie len VPA. | O | A | Vaša pripomienka bola akceptovaná. Bolo doplnené ustanovenie o úlohách iných ústredných orgánov štátnej správy v rámci nového paragrafu. |
| **ÚVSR** | **Čl. I § 30, ods. 3)**  Podľa ustanovenia § 30, ods. 1) návrhu tohto zákona je prevádzkovateľ základnej služby povinný sa podrobiť auditu kybernetickej bezpečnosti. Podľa ustanovenia § 30, ods. 3) návrhu tohto zákona audit je oprávnená vykonať osoba s praxou v audite informačnej bezpečnosti. Odporúčame v predmetnom znení text „informačnej bezpečnosti“ nahradiť textom „kybernetickej bezpečnosti alebo informačnej bezpečnosti“. Odôvodnenie: Zosúladenie ustanovení podľa ods. 1) a ods. 3) v § 30. | O | A |  |
| **ÚVSR** | **Čl. I § 3, písm. b)** Text navrhovanej definície pojmu „kybernetický priestor“ odporúčame upraviť v nasledujúcom znení: „b) kybernetickým priestorom globálny dynamický otvorený systém, ktorý tvoria aktivované siete a informačné systémy, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi týmito entitami.“. Odôvodnenie: Pojem „prvok kybernetického priestoru“ návrh zákona nedefinuje. Z kontextu predmetnej definície a definície pojmu „sieť a informačný systém“ v návrhu zákona vyplýva, že pre účely tohto zákona „siete a informačné systémy„ predstavujú prvky kybernetického priestoru. | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **ÚVSR** | **Čl. I § 12, ods. (2), písm. b)**  Text ustanovenia odporúčame nahradiť textom v nasledujúcom znení: vecne príslušnej autority vedúci vecne príslušnej autority. Odôvodnenie: Navrhujeme precizovanie uvedeného ustanovenia. | O | N | Vaša pripomienka nebola akceptovaná a bola upravená v zmysle pripomienky NBS. |
| **ÚVSR** | **Čl. I, § 3, písm. a)**  V texte definície pojmu „sieť a informačný systém“ odporúčame spojku „alebo“ nahradiť spojkou „ako aj“, resp. „a“. Odôvodnenie: Navrhnuté znenie ustanovenia so spojkou „alebo“ možno interpretovať tak, že údaje (ako entita pokrytá pojmom „sieť a informačný systém“) sú alternatívou k ostatným uvedeným entitám, ktoré tvoria obsah pojmu „sieť a informačný systém“. | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **ÚVSR** | **Čl. I § 19, ods. 1)**  V ustanovení sa na začiatku uvádza: „cieľom je zabezpečenie kybernetickej bezpečnosti počas celej doby životnosti informačného a komunikačného systému“. V ďalšom texte sa hovorí o „kategorizácií sietí a informačných systémov“. Odporúčame text „informačného a komunikačného systému“ nahradiť textom „sietí a informačných systémov“. Odôvodnenie: Z ustanovenia § 3, písm. a) návrhu zákona vyplýva, že informačné a komunikačné systémy sú podmnožinou sietí a informačných systémov v zmysle návrhu tohto zákona. | O | A |  |
| **ÚVSR** | **Čl. I § 15, ods. 5)**  V ustanovení sa uvádza, že na jednotku CSIRT,......., sa nevzťahujú žiadne práva vyplývajúce z tohto zákona. Ustanovenie odporúčame z návrhu zákona vypustiť. Odôvodnenie: V ustanoveniach návrhu zákona nie sú explicitne uvedené žiadne práva jednotky CSIRT, ani odkaz na iný predpis. | O | A | Vaša pripomienka bola akceptovaná a textácia bola vypustená. |
| **ÚVSR** | **Čl. I § 4, ods. 3)** V znení tohto ustanovenia je použitý pojem „kybernetická odolnosť“, odporúčame definovať jeho význam. Odôvodnenie: V návrhu zákona sa definícia uvedeného pojmu nenachádza a nie je uvedený ani odkaz na iný zdroj. Možno vychádzať z Terminologického slovníka krízového riadenia Bezpečnostnej rady. Odporúčame použiť definíciu v nasledujúcom znení: schopnosť aktív odolávať pokusom o naplnenie kybernetických hrozieb, minimalizovať dôsledky naplnených hrozieb a obnoviť ich funkčnosť. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **ÚVSR** | **Čl. IV § 2, ods. 2), písm. b)**  Žiadame definovať význam pojmu „kybernetický útok“. Odôvodnenie: V ustanovení sa uvedený pojem vyskytuje, ale v návrhu zákona sa špecifikácia jeho významu nenachádza. V Terminologickom slovníku krízového Bezpečnostnej rady Slovenskej republiky sa pod „kybernetickým útokom“ rozumie: „útok vedený kybernetickými prostriedkami.“. | Z | N | Pojem vypustený bez náhrady. Rozpor bol odstránený. |
| **ÚVSR** | **Čl. VI** Žiadame z predloženého materiálu vypustiť novelizačný článok VI, ktorým sa dopĺňa zákon č. 553/2003 Z. z. o odmeňovaní niektorých zamestnancov pri výkone práce vo verejnom záujme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Uvedenú pripomienku uplatňujeme ako zásadnú. Odôvodnenie: Zákon č. 553/2003 Z. z. o odmeňovaní niektorých zamestnancov pri výkone práce vo verejnom záujme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov obsahuje inštitút osobného platu, pričom dôvodom na jeho priznanie je vykonávanie osobitne významných pracovných činností alebo mimoriadne náročných pracovných činností. Ide o obdobné dôvody, pre ktoré predkladateľ materiálu navrhuje novelizovať uvedený zákon doplnením predmetného príplatku a z tohto dôvodu nie je novelizácia potrebná. Prípadné potreby zvýšenia funkčného platu je tak možné realizovať práve prostredníctvom osobného platu, ktorý je obsiahnutý v platnej právnej úprave. Osobný plat navyše nie je ohraničený (okrem minimálnej garancie), takže nie je vylúčený ani plat na úrovni, ktorá by zohľadňovala aj výšku navrhovaného príplatku (90 % platovej tarify). | Z | A |  |
| **ÚVSR** | **Čl. X**  Žiadame z predloženého materiálu vypustiť novelizačný článok X, ktorým sa dopĺňa zákon č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov. Uvedenú pripomienku uplatňujeme ako zásadnú. Odôvodnenie: Zákon č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov obsahuje inštitút osobného platu, pričom dôvodom na jeho priznanie je vykonávanie osobitne významných úloh alebo mimoriadne náročných úloh. Ide o obdobné dôvody, pre ktoré predkladateľ materiálu navrhuje novelizovať uvedený zákon doplnením predmetného príplatku a z tohto dôvodu nie je novelizácia potrebná. Prípadné potreby zvýšenia funkčného platu je tak možné realizovať práve prostredníctvom osobného platu, ktorý je obsiahnutý v platnej právnej úprave. Osobný plat navyše nie je ohraničený (okrem minimálnej garancie), takže nie je vylúčený ani plat na úrovni, ktorá by zohľadňovala aj výšku navrhovaného príplatku (90 % platovej tarify). | Z | A |  |
| **ÚVSR** | **Čl. IV § 7, ods. 2), písm. a)**  Žiadame znenie ustanovenia spresniť, t. j. na konci textu pridať nasledujúce slovo: „štátu“. Odôvodnenie: Sme toho názoru, že pod obranou štátu nemožno chápať zabránenie akémukoľvek kybernetickému útoku. Odporúčame rozlišovať medzi „obranou štátu“ – úloha ozbrojených síl a „obranou“, ktorá predstavuje reakciu na útok voči ostatným aktívam inými subjektmi v rámci chápania významu pojmu „kybernetická ochrana“. | Z | N | Po dohode všetkých subjektov sa MOSR zaviazalo novelizovať právne predpisy v podobe nového textu. |
| **Verejnosť** | **§ 19 ods. 1** Návrh zákona sa obmedzuje len na prevádzkovateľov základnej služby, čo nie je v zmysle § 3 návrhu zákona s ohľadom na vymedzenie pojmu kybernetická bezpečnosť dostatočné. Uvedené navrhujeme uviesť do súladu. Odôvodnenie: Nakoľko návrh zákona má ustanovovať súbor minimálnych bezpečnostných požiadaviek na zabezpečenie kybernetickej bezpečnosti, pričom kybernetickou bezpečnosťou sa rozumie stav, v ktorom sú siete a informačné systémy schopné odolávať kybernetickým bezpečnostným incidentom, bezpečnostné opatrenia ako samotný mechanizmus na elimináciu alebo aspoň minimalizáciu pravdepodobnosti naplnenia hrozby alebo jej následkov by mal rozhodne reflektovať na širší okruh subjektov v rámci kybernetického priestoru, ako len na prevádzkovateľov základných služieb (príp. poskytovateľov digitálnych služieb). Naviac prahové hodnoty základných služieb, na základe ktorých by sa mohol konkrétny subjekt vôbec ako prevádzkovateľ základných služieb identifikovať, nie je z obsahu návrhu zákona známy. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a prahové hodnoty boli do textu návrhu zákona doplnené. Okruh subjektov vyplýva zo smernice NIS. |
| **Verejnosť** | **prílohe č. 1** Navrhujem do tabuľky (príloha č.1) doplniť sektor "Pošta". Zdôvodnenie: - nesúlad navrhovanej novelizácie Zákona č. 45/2011 Z. z. a Zákona o KB. V Zákone č. 45/2011 Z. z. sa uvedený sektor nachádza, v Zákone o KB nie. V dôsledku toho: - nie je jasné, či sa navrhovaný Zákon o KB vzťahuje aj na Slovenskú poštu, a. s., (jediným akcionárom je SR, prostredníctvom MDaV SR). Podľa predloženého návrhu zákona nie priamo, len okľukou cez Zákon č. 45/2011 Z. z. => právna neistota aj pre obchodných partnerov, vrátane verejnej správy; - nevynútiteľnosť poskytnutia služieb CSIRT-u (pretože SP, a. s., nie je uvedená ako poskytovateľ základnej služby); - nejasnosti v súvislosti so službami štátu, ktoré SP, a. s., sprostredkúva (IOM - výpisy z RT..., eKolky...); - NBÚ stráca možnosť kontrolovať KB týchto služieb (štátny orgán môže konať len v rozsahu zákona => nedostatok legitimity voči SP, a. s.); - rozsah dopadov možného útoku voči infraštruktúre SP, a. s., s dosahom na poskytované služby ( 5,5 mil. obyvateľov SR + zahraničný presah, > 1500 pobočiek, neplnenie poštovej licencie...). Pozn. SP. a. s., je aktuálne držiteľom certifikácie podľa ISO 27001, t.j. prechod do režimou KB by nemal predstavovať väčší problém. | O | A |  |
| **Verejnosť** | **§ 19 ods. 2** Navrhujeme zadefinovať pojmy dôvernosť, dostupnosť, integrita, kvalita a kontrolná činnosť a objasniť spôsob vykonávania klasifikácie informácií a kategorizácie sietí a informačných systémov predpokladaný všeobecne záväzným právnym predpisom podľa § 33 písm. g) návrhu zákona. Odôvodnenie: Bez znalosti obsahu používaných pojmov v rámci návrhu zákona nie je možné samotnú klasifikáciu informácií a kategorizáciu sietí a informačných systémov uskutočniť, nakoľko táto má byť vykonaná s ohľadom na uvedené atribúty bezpečnosti bez ich ďalšieho objasnenia. Rovnako v rámci návrhu zákona absentujú kategórie/stupne podľa ktorých sa kategorizujú siete a informačné systémy a klasifikujú informácie a rovnako absentuje proces vykonávania klasifikácie informácií a kategorizácie sietí a informačných systémov podľa § 11 ods. 1 písm. g) návrhu zákona. Uvedené považujeme za zásadnú pripomienku a vážny legislatívny nedostatok návrhu zákona a žiadame ho doplniť. | O | A | Vaša pripomienka bola akceptovaná. Klasifikácia a kategorizácia sietí a informačných systémov je v zmysle pripomienky SBA obsahom návrhu zákona, keďže je neúčelné, aby si prevádzkovatelia základnej služby menili svoje klasifikácie na iné, resp. viedli duálnu klasifikáciu. Každý prevádzkovateľ svojho informačného systému má reálnu vedomosť o svojich informačných systémoch a ich klasifikácii. Pojmy sú vysvetlené v dôvodovej správe, nejde o pojmy, ktorých obsah by bol všeobecne neznámy alebo nezrozumiteľný. STN ISO/IEC 27000:2014 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník: Dôvernosť - záruka, že informácia nie je prezradená neoprávneným entitám alebo procesom. Miera obmedzenia prístupu k informáciám len pre osoby, alebo skupiny osôb, ktoré sú oprávnené na prístup k príslušným informáciám. Zahŕňa tiež ochranu súkromia. Dostupnosť – záruka, že dáta, alebo informácie sú pre používateľa, systém alebo zariadenie prístupné vo chvíli, keď je informácia potrebná a požadovaná Integrita - miera bezchybnosti, úplnosti, správnosti informácie. Podmienka, ktorá je zachovaná vtedy, ak údaje získané zo zdroja informácií neboli náhodne alebo zámerne modifikované, poškodené alebo zničené. |
| **Verejnosť** | **§ 19 ods. 1** Navrhujeme nahradiť pojem „celej doby životnosti informačného a komunikačného systému“ pojmom „celého životného cyklu informačného a komunikačného systému“ a tento zakomponovať do návrhu zákona s jeho obsahovým vymedzením. Odôvodnenie: Životný cyklus informačného systému je pojem širší ako pojem životnosť informačného systému. Z uvedeného dôvodu a s ohľadom na skutočnosť, že hovoríme a informačných a komunikačných systémoch prevádzkovateľov základných služieb je nevyhnutné, aby boli bezpečnostné opatrenia implementované od procesu plánovania až po proces vyradenia informačného alebo komunikačného systému. Životný cyklus informačného systému štandardne pozostáva z fázy jeho návrhu (inicializácie), vývoja (obstaraní), zavedenia (implementácie), prevádzky (vrátane údržby) a vyradenia (odstránenia). Implementácia bezpečnostných opatrení len počas aktívnej fázy "životnosti" informačného systému nie je dostatočná. | O | A |  |
| **Verejnosť** | **§ 19 ods. 5** Navrhujeme odstrániť stav, že návrh zákona nestanovuje obsahové náležitosti bezpečnostnej dokumentácie, rovnako ako ani bezpečnostné opatrenia, ich obsah a rozsah, ktoré je nutné implementovať v zmysle § 18 ods. 1 návrhu zákona. Uvedené časti a náležitosti žiadame doplniť. Odôvodnenie: Absencia všeobecne záväzných právnych predpisov, ktoré by rozhodne mali byť súčasťou návrhu zákona spôsobuje,že nie je možné v súčasnosti identifikovať bezpečnostné opatrenia rámcovo a nedostatočne v návrhu zákona obsiahnuté. Z uvedeného dôvodu je nutné, aby súčasťou návrhu zákona bol všeobecne záväzný právny predpis podľa § 33 písm. c) návrhu zákona a ktorý by nadobudol účinnosť spolu s návrhom zákona. Pripomienku považujeme za zásadnú. | O | A | Vaša pripomienka nebola akceptovaná z dôvodu, že nie je reálne možné stanoviť výslovne obsahové náležitosti bezpečnostnej dokumentácie, ani taxatívne vymedziť bezpečnostné opatrenia. Nebolo by to efektívne a najmä účelné. Tieto požiadavky sú odporúčané v príslušných technických normách a zákon definuje okruhy, ktoré majú byť predmetom úpravy. |
| **Verejnosť** | **§ 29 ods. 6** Navrhujeme vypustiť kompetenciu vstupovať do komunikačných a informačných systémov do úrovne správcu systému. Odôvodnenie: Kompetencia vstupovať do komunikačných a informačných systémov do úrovne správcu systému je vzhľadom na bežný výkon kontrolnej činnosti neprimeraná. V súvislosti s uvedeným nie je rovnako vylúčené, že v dôsledku navrhovaného rozsahu kompetencií pri výkone kontroly môže v prípade zmeny hardvérovej alebo softvérovej konfigurácie systému dôjsť k vzniku škody (napr. nefunkčnosť systému, príp. časti systému). Nakoľko orgány štátnej správy sú povinné na plnenie úloh v zmysle zákona a znefunkčnením systémov by túto povinnosť neboli schopné plniť, je rovnako potrebné bližšie vymedziť oprávnenia príslušníkov úradu pri výkone kontroly a vyriešenie problémov, ako zodpovednosti za prípadnú škodu, uvedenia systémov do pôvodného stavu a iné. V ďalšom spojení s § 6 ods. 2 návrhu zákona je uvedená kompetencia čo do rozsahu absolútne neprijateľná a sama o sebe môže znamenať bezpečnostné riziko. | O | A |  |
| **Verejnosť** | **§ 23**  Opätovne absentuje všeobecne záväzný právny predpis, ktorý by prahové hodnoty pre jednotlivé už návrhom zákona stanovené kategórie kybernetických bezpečnostných incidentov spresňoval. Navrhujeme, aby súčasťou návrhu zákona bol všeobecne záväzný právny predpis podľa § 33 písm. d) návrhu zákona a ktorý by nadobudol účinnosť spolu s návrhom zákona. Odôvodnenie: Povinné osoby v zmysle návrhu zákona, pokiaľ by boli schopné sa identifikovať ako prevádzkovatelia základnej služby (čo momentálne nie sú) rovnako nie sú schopné určiť, čo sa považuje za kybernetický bezpečnostný incident a čo nie. Uvedené bude možné posúdiť až na základe prahových hodnôt obsiahnutých vo všeobecnom záväznom právnom predpise, ktorý však nie je súčasťou návrhu zákona. Pripomienku považujeme za zásadnú. | O | N | Vaša pripomienka bola akceptovaná a znenie bolo vypustené. Právna úprava bola premietnutá v preformulovanej podobe s obsahom aj jednotlivých kriteriálnych parametrov v rámci § o hlásení kybernetických bezpečnostných incidentov. Parametre sú v súlade so smernicou NIS na určenie závažného kybernetického bezpečnostného incidentu. Jednotlivé kategórie sú odstupňované od závažnosti od 1 po 3, v záujme flexibilného reagovania na bezpečnostné prostredie je nevyhnutné špecifikáciu prenechať do vykonávacieho predpisu. |
| **Verejnosť** | **§ 6 ods. 2** S uvedenou textáciou nesúhlasíme a túto žiadame vypustiť, príp. stanoviť podstatné náležitosti dohody o spolupráci, najmä predmet dohody za účelom jednoznačnej identifikácie právomocí alebo rozsahu právomocí, ktoré sa majú na fyzickú alebo právnickú osobu na základe dohody preniesť. Odôvodnenie: Nakoľko Návrh je okrem iného aj transpozičným zákonom Smernice EP a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii a vzhľadom na to, že sa prostredníctvom neho má zaviesť systém zabezpečenia kybernetickej bezpečnosti (predmet zákona) a chrániť tie najvýznamnejšie a najdôležitejšie služby poskytované v niektorom zo sektorov alebo podsektorov podľa prílohy č. 2 návrhu zákona, ktorých ohrozenie alebo narušenie môže znamenať významný dopad na fungovanie štátu, práva a právom chránené záujmy fyzických osôb a iné, plnenie úloh vyplývajúcich z návrhu zákona by mal zostať v rukách štátu, ktorý ho zabezpečí vlastnými silami a prostriedkami, nie delegovaním na tretie strany (súkromný sektor). Uvedené nie je rovnako prípustné z dôvodu, že sú to práve štátne orgány, ktorým zákon zveruje do kompetencie príslušné práva, oprávnenia a povinnosti s cieľom zaviesť vyváženosť a rovnováhu, pričom štátne orgány sú pri plnení zverených úloh a kompetencií povinné postupovať výlučne na základe zákona a v súlade s článkom 2 ods. 2 Ústavy Slovenskej republiky. Štátne orgány sú povinné postupovať výlučne v súlade so zákonom, pričom nesmú konať spôsobom (čo nie je zákonom zakázané, je dovolené). Pokiaľ by bolo možné na základe zmluvy previesť na akúkoľvek fyzickú alebo právnickú osobu práva alebo povinnosti dané úradu, mohlo by to významným spôsobom narušiť princíp právnej istoty ako nevyhnutného atribútu právneho štátu. Uvedený prístup nie je v právnom štáte akceptovateľný. Pripomienku považujeme za zásadnú. | O | A |  |
| **Verejnosť** | **§ 19 ods. 3** S uvedeným nie je možné súhlasiť. Bezpečnostné opatrenia sa neprijímajú pre oblasti, ale tieto sú súčasťou oblastí a z týchto oblastí sa následne vyberajú a implementujú. Oblasti označené v § 19 ods. 3 nie sú úplné. Navrhujeme uviesť do súladu s existujúcimi medzinárodnými štandardmi informačnej bezpečnosti a dodržiavať ustálenú terminológiu. Odôvodnenie: Bezpečnostné opatrenia slúžia na elimináciu alebo aspoň minimalizáciu pravdepodobnosti naplnenia hrozby (dopadu na aktíva). V súlade s uvedeným, prostredníctvom bezpečnostných opatrení sa znižuje pravdepodobnosť naplnenia hrozby, a to s ohľadom na zabezpečenie dôvernosti, dostupnosti, integrity aktív, príp. ďalších bezpečnostných požiadaviek. Bezpečnostné opatrenia sú súčasťou oblastí, ktoré sú z týchto oblastí vyberané s ohľadom na potrebu dosiahnutia cieľovej úrovne bezpečnosti. Okrem uvedeného oblasti označené v rámci § 19 ods. 3 návrhu zákona nie sú úplné. | O | A | Vaša pripomienka bola akceptovaná a text bol upravený v zmysle ISO 27002. |
| **Verejnosť** | **Členovia Slovenskej aliancie pre inovatívnu ekonomiku pripravili nasledovné pripomienky k zákonu o kybernetickej bezpečnosti** Smernica 2016/1148 zahŕňa podporu a dobrovoľnú spoluprácu medzi orgánmi verejnej moci privátnym sektorom, ktorá je nevyhnutná pre efektívnu ochranu informačného prostredia. Preto pokladáme za vhodné a prospešné zapracovať možnosti spolupráce a transparentnosti do návrhu zákona. Taktiež použitie termínu „Kybernetika“ vzhľadom na jeho nepresnosť odporúčame nahradiť štandardným pomenovaním „informačné systémy a siete“ čo je presné pomenovanie dotknutých oblastí navrhovaným zákonom. Pripomienky: §4 c) pridať 10. Slovenská Informačná Služba §5 bod (1) doplniť pod písmeno q) Úradom podpredsedu vlády SR pre investície a informatizáciu pridať bod t) Vypracovať a predkladať verejne prístupnú súhrnnú správu o počte prijatých oznámení, ako aj údaje o povahe oznamovaných incidentov, ako je druh porušenia bezpečnosti, jeho závažnosť alebo dĺžka jeho trvania. bod (2) a) poskytuje súčinnosť a prijatie dobrovoľných oznámení od subjektov, ktoré nepatria do rozsahu pôsobnosti tejto smernice, ale môžu byť vystavené incidentom, ktoré majú významný vplyv na služby, ktoré poskytujú, b) informuje dotknuté subjekty ktorých nahlásený bezpečnostný incident si vyžaduje medzinárodnú spoluprácu o postupe a riešení v zmysle §6, c) informuje dotknuté subjekty ktoré nahlásili bezpečnostný incident o výsledku spracovania a navrhnutých odporúčaniach. §8 systém včasného varovania má jednoznačne dopad na širokú verejnosť, preto by sa IS mal skladať s uzavretej a verejnej časti. Túto potrebu treba zohľadniť a doplniť v bode (1) a (4). §10 (1) Súčasná zákonná úprava dáva možnosti režimového spracovania informácií a mlčanlivosti v štátnej službe. Preto nie je potrebné široké taxatívne utajenie, ktoré by bolo kontraproduktívne v procese transparentnosti a získavania dôvery medzi orgánmi verejnej moci a súkromným sektorom. Preto navrhujeme bod 1 vypustiť. (5) Zákon 211/2000 dostatočne chráni sprístupňovanie osobných údajov, preto odporúčame tento bod vypustiť. §17 (4) navrhujeme pridať písmeno d) zabezpečenia segregácií významných administratívnych činností §21 číslo (1) odporúčame pridať časový rámec do 24 hodín od zistenia bezpečnostného incidentu. Zásadná pripomienka č.1: Žiadame do návrhu zákona doplniť novú kapitolu pod názvom „Kybernetická bezpečnosť a internet“, ktorá bude nasledovať po kapitole Systém zabezpečenia kybernetickej bezpečnosti Zdôvodnenie: Táto kapitola bola súčasťou Návrhu zákona o informačnej bezpečnosti z roku 2015 a považujeme ju za opodstatnenú. Nemáme vedomosť o tom, že by téma bezpečnosti a stability internetu ako aj súvisiaca správa národnej domény bola súčasťou nejakej právnej úpravy. Tieto témy však podľa nás sú významnou súčasťou kybernetickej bezpečnosti a preto rozumieme a stotožňujeme sa s pôvodnou ambíciou predmetného návrhu zákona z roku 2015 ich riešiť. Zásadná pripomienka č.2: Žiadame do novej kapitoly Kybernetická bezpečnosť a internet doplniť nový § 29 pod názvom „Bezpečnosť a stabilita Internetu“ v nasledovanom znení: 1. Národný bezpečnostný úrad vykonáva úlohu gestora štátu pre kritické zložky internetu, ktorými sú najmä národná doména .sk, doména druhej úrovne, internetové adresy a internetové protokoly a pre ďalšie prvky týkajúce sa správy internetu na národnej úrovni. 2. Národný bezpečnostný úrad vypracuje zásady a usmernenia pre odolnosť a stabilitu internetu pre štátnu správu a vydá ich vo forme pravidiel. 3. Na stanovenie bezpečnostných požiadaviek na ochranu informačných systémov verejnej správy a kritických informačných systémov v kybernetickom priestore Slovenskej republiky sa primerane použijú ustanovenia tohto zákona. Zdôvodnenie: Spoločné so zdôvodnením k pripomienke č. 3 Zásadná pripomienka č.3: Žiadame do novej kapitoly „XXX“ doplniť nový § 30 pod názvom „Správa národnej domény“ v doleuvedenom znení: 1. Správcom národnej domény .sk je Úrad podpredsedu vlády SR pre investície a informatizáciu („Úrad“) 2. Prevádzkovateľom databázy menného priestoru domén druhej úrovne doménových menných serverov je verejná organizácia Národná doména.sk (ďalej len „organizácia ND.SK“), zriadená pre tento účel Úradom podpredsedu vlády SR pre investície a informatizáciu, ktorá je povinná: a. zabezpečovať nepretržitú, bezpečnú a bezporuchovú prevádzku databázových doménových menných serverov a poskytovať menný priestor domén druhej úrovne v súlade s pravidlami podľa § 29 ods. 2, b. poskytovať službu prístupu k databáze serverov registrátorom doménových mien druhej úrovne, c. zabezpečovať vzájomné prepojenia databázových menných serverov druhej úrovne a medzinárodných databázových menných serverov. 3. Úrad a organizácia ND.SK a. prijmú legislatívne, technické a technologické opatrenia, za účelom bezpečného a vierohodného rozpoznávania a používania doménových mien v Slovenskej republike, b. podporia nové technológie pre zvýšenie bezpečnosti prevádzky národnej domény. 4. Organizácia ND.SK je oprávnená za poskytované služby požadovať od registrátorov doménových mien druhej úrovne finančnú úhradu nákladov v primeranej výške. Účtovníctvo organizácie ND.SK podlieha kontrole Úradu. Výnos z platieb za poskytovanie služieb je príjmom štátneho rozpočtu a je určený na rozvoj internetu Slovenskej republiky. 5. Registrátorom domény druhej úrovne je organizácia, ktorú touto činnosťou na základe výberového konania poverí Úrad. Registrátor je povinný dodržiavať pravidlá poskytovania menného priestoru národnej domény, schválené Úradom a vydané organizáciou ND.SK. 6. Registrátor je oprávnený za poskytovanie služieb registrácie domény druhej úrovne vyberať od konečného užívateľa finančnú náhradu vo výške stanovenej v cenníku služieb a výkonov, ktorý je nedeliteľnou súčasťou pravidiel podľa § 29 ods.2. 7. Ministerstvo môže zrušiť poverenie výkonu činnosti registrátorovi, ak tento napriek písomnej výzve porušuje pravidlá. Ministerstvo koná v tomto prípade na základe a. oznámenia organizácie ND.SK, b. vlastného šetrenia, c. výzvy iných registrátorov. Zdôvodnenie: Správu národnej domény považujeme za významnú a neoddeliteľnú súčasť bezpečnosti internetu na Slovensku. Nakoľko bezpečnosť internetu a elektronických komunikačných sietí sa stáva čoraz citlivejšou témou vzhľadom na zvyšovanie ich dôležitosti v čase budovania Jednotného digitálneho trhu v EÚ a digitálnej ekonomiky všeobecne, funkčnosť a bezpečnosť národnej domény považujeme za otázku národnej bezpečnosti. Pôvodný Návrh zákona o internetovej bezpečnosti z roku 2015 túto skutočnosť náležite odzrkadľoval a správu národnej domény navrhoval po vzore väčšiny vyspelých krajín sveta ponechať vo verejnej inštitúcii pod dohľadom štátu a odbornej verejnosti. Ako súkromná spoločnosť, ktorá čoraz väčšiu časť svojich aktivít realizuje on-line, chceme mať istotu, že doména .sk je bezpečná a spoľahlivá. Len prostredníctvom našej stránky a pridruženého elektronického obchodu realizujeme denne do 10% celkových tržieb za služby a tovar priamo, ďalších takmer 40% nepriamo a komunikujeme s desať tisíckami zákazníkov. Je preto pre nás kľúčové mať istotu, že v prípade výpadku domény čo i len na 1 deň existuje inštitúcia, ktorá nám bude schopná v prípade žaloby kompenzovať vzniknuté hospodárske škody. Máme vážne pochybnosti, či súčasne platný systém správy národnej domény .sk takúto vymožiteľnosť garantuje, alebo aspoň predpokladá. Keďže národná doména je verejným majetkom, za ktorý nesie zodpovednosť príslušný orgán štátnej správy, máme za to, že musí mať kontrolu nad jeho správou. Nie je nám známe, kedy a prečo sa štát tejto úlohy vzdal, ale považujeme za nevyhnutné, aby tento stav prehodnotil z dôvodov bezpečnostných ako aj ekonomických. Hospodárske škody pre štátne inštitúcie v prípade výpadku domény .sk by boli totiž tiež enormné. Zároveň máme pochybnosť, či štát disponuje dostatočnými technologickými kapacitami na zálohovanie dát a teda či v prípade prípadného výpadku vedel zónu .sk zrekonštruovať v celom rozsahu. Dovoľujeme si zodpovedným odporučiť, aby sme v tejto citlivej oblasti zvolili cestu podobnú ostatným krajinám EÚ, napr. ČR. Prvoradou úlohou správy národnej domény je podľa nášho názoru práve neustále zvyšovanie jej bezpečnosti a následne kvality ďalších služieb poskytovaných majiteľom jednotlivých domén, ktorí si za túto službu platia. Na základe skúsenosti zo zahraničia máme za to, že hore vedný návrh je dobým základom na dosiahnutie tohto cieľa. | O | ČA | Text preformulovaný a precizovaný v zmysle doručených pripomienok zaoberajúcich sa predmetnými bodmi zákona. |
| **Verejnosť** | **§ 3 písm. e)** Uvedená definícia je chybná a zamieňa pojmy riziko a hrozba. Žiadame zosúladiť. Odôvodnenie: Riziko vyjadruje potenciálnu možnosť (pravdepodobnosť), že práve hrozba zneužije zraniteľnosť (aktíva), aby spôsobila stratu alebo poškodenie aktív alebo skupiny aktív (napr. narušenie dôvernosti, dostupnosti alebo integrity), zatiaľ čo hrozba je práve akákoľvek okolnosť alebo udalosť, ktorá môže mať na bezpečnosť nepriaznivý vplyv, a teda v tomto prípade vplyv v podobe narušenia dôvernosti, dostupnosti alebo integrity aktíva. Definícia teda zamieňa pojmy riziko a hrozba a je potrebné ich upraviť.Uvedenú pripomienku považujeme za zásadnú. | O | A | Vaša pripomienka nebola akceptovaná z dôvodu, že bol upravený celý § 3 a boli zavedené nové pojmy. |
| **Verejnosť** | **§ 3 písm. g)** V zmysle § 3 písm. g) v spojení s § 3 písm. h) a § 17 ods.1 návrhu zákona nie je možné identifikovať, kto je a kto nie je prevádzkovateľom základnej služby. Uvedené žiadame odstrániť a stanoviť kritériá (prahové hodnoty) na identifikáciu základnej služby, ktoré by boli súčasťou návrhu zákona alebo jeho vykonávacieho právneho predpisu a nadobudli účinnosť súčasne s návrhom zákona. Odôvodnenie: Návrh zákona predpokladá v rámci § 33 vydanie deviatich vykonávacích právnych predpisov, pričom jedným z nich je vykonávací právny predpis stanovujúci prahové hodnoty pre identifikáciu základnej služby podľa § 17 ods. 1 (§ 33 písm. b). Nakoľko z jednotlivých ustanovení návrhu zákona nie je možné jednoznačne identifikovať, kto je prevádzkovateľom základnej služby a kto nie je, resp. kto základnú službu prevádzkuje, je nutné, aby súčasťou návrhu zákona stanovujúceho povinným osobám konkrétne povinnosti a sankcie za ich nesplnenie, boli aj všeobecne záväzné právne predpisy slúžiace na jeho vykonanie a ktoré by nadobudli účinnosť spolu s návrhom zákona. Opačný prístup by mohol byť rovnako v rozpore s požiadavkami stanovenými v čl. 6 ods. 1 Legislatívnych pravidiel vlády Slovenskej republiky. Absentujúcu zrozumiteľnosť a určitosť právnej úpravy považujeme celkovo za vážny nedostatok návrhu zákona. Uvedenú pripomienku považujeme za zásadnú. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že bol upravený celý § 3 a boli zavedené nové pojmy. |
| **Verejnosť** | **§ 14** Z uvedenej textácie nie je zrejmé, aké „požadované technické, technologické a personálne vybavenie“ jednotka CSIRT preukazuje. Opätovne nie je možná identifikácia požiadaviek, v tomto prípade na jednotku CSIRT v rámci jej akreditácie, a to z dôvodu absencie všeobecne záväzného právneho predpisu podľa § 33 písm. a) podrobnosti o technickom, technologickom a personálnom vybavení podľa § 14 ods. 1 písm. a) a rovnako tak znemožňuje prípravy na plnenie povinností podľa § 15 návrhu zákona. Vyššie uvedené absentujúce časti návrhu zákona žiadame doplniť. Odôvodnenie: Z ustanovení návrhu zákona nie je možné identifikovať požadované technické, technologické a personálne vybavenie jednotky CSIRT, nakoľko tieto majú byť obsiahnuté buď priamo v návrhu zákona alebo vo všeobecne záväznom právnom predpise, ktorý však nie je súčasťou predloženého návrhu zákona. Okrem uvedeného, proces budovania spôsobilostí jednotiek CSIRT je záležitosťou vyžadujúcou si značné finančné prostriedky, odborné zázemie a čas nevyhnutný na preukázanie proklamovaných alebo deklarovaných spôsobilostí v rámci jej prevádzky, a teda sa nejedná o jednoduchý proces zavedenia zákonnej povinnosti a jej následného bezodkladného plnenia. Z dôvodu efektívneho využitia času do uplynutia prechodného obdobia, ako aj v záujme poznania podrobností o technickom, technologickom a personálnom vybavení jednotky CSIRT je aj v tomto prípade nutné, aby súčasťou návrhu zákona bol všeobecne záväzný právny predpis podľa § 33 písm. a) návrhu zákona a ktorý by nadobudol účinnosť spolu s návrhom zákona. | O | N | Vaša pripomienka nebola akceptovaná. Odôvodnená je v dôvodovej správe. |
| **Verejnosť** | **§ 2 ods. 1** Z uvedenou textáciou nie je možné súhlasiť a žiadame o jej úpravu v tom zmysle, aby rovnocennosť požiadaviek podľa osobitných právnych predpisov bola skúmaná a porovnávaná v rámci rovnocenných kategórií, tzn. súboru požiadaviek podľa Návrhu (rozumej súbor ako komplexný celok, nielen požiadavky jednotlivo) so súborom požiadaviek podľa osobitnej právnej úpravy. Odôvodnenie: Návrh zákona síce má ambíciu ustanoviť súbor minimálnych požiadaviek na zabezpečenie kybernetickej bezpečnosti, no na strane druhej a v zmysle § 2 ods. 1 návrhu zákona postačuje, aby osobitný predpis ustanovoval rovnocenné alebo vyššie, podľa všetkého aj jednotlivé požiadavky na zabezpečenie sietí a informačných systémov ako návrh zákona, pričom sa tieto ďalej môžu použiť. Pod pojmom súbor bezpečnostných požiadaviek je možné rozumieť komplexný systém požiadaviek, dodržiavaním ktorého je sledované zabezpečenie kybernetickej bezpečnosti. Jednotlivé požiadavky sami o sebe však nemusia automaticky znamenať rovnakú úroveň bezpečnosti, zatiaľ čo ich ich kombinácia áno. Pokiaľ návrh zákona na jednej strane ustanovuje súbor minimálnych bezpečnostných požiadaviek, pričom na strane druhej v zmysle osobitnej právnej úpravy postačuje ustanoviť rovnocenné alebo vyššie, ale už len jednotlivé požiadavky a nie súbor požiadaviek podľa prvej vety navrhovanej právnej úpravy, uvedené môže v závere spôsobiť reálne zníženie úrovne bezpečnosti plnením vybraných požiadaviek podľa osobitnej právnej úpravy a zvyšných sa v osobitnej právnej úprave nenachádzajúcich v zmysle návrhu zákona. | O | ČA | Vaša pripomienka bola čiastočne akceptovaná a zapracovaná. |
| **Verejnosť** | **§ 3 písm. f)** Žiadame o zadefinovanie pojmov dôvernosť, integrita, dostupnosť, vysoká pravdepodobnosť kompromitácie činnosti základnej služby, ohrozenie bezpečnosti informácií. Odôvodnenie: Z dôvodu absencie vymedzenia pojmov dôvernosť, integrita, dostupnosť, vysoká pravdepodobnosť kompromitácie činnosti základnej služby či ohrozenie bezpečnosti informácií následne použitých na samotnú definíciu pojmu kybernetický bezpečnostný incident nie je rovnako možné pochopiť obsah samotnej definície kybernetického bezpečnostného incidentu, nakoľko sa odvoláva na obsahovo neznáme pojmy. Uvedenú pripomienku považujeme za zásadnú. | O | A | Vaša pripomienka bola akceptovaná, bol upravený celý § 3 a boli zavedené nové pojmy. |
| **Verejnosť** | **§ 4** Žiadame vypustiť alebo prepracovať v súlade s legislatívnymi pravidlami vlády Slovenskej republiky. Odôvodnenie: Na základe článku 6 legislatívnych pravidiel vlády Slovenskej republiky, zákon okrem iného musí obsahovať len ustanovenia s normatívnym obsahom. Uvedené nie je v zmysle § 4 návrhu zákona dodržané, nakoľko tento obsahuje všeobecné konštatácie, odporúčania, návody na spoluprácu či správanie sa v kybernetickom priestore. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že text bol vypustený. |
| **Verejnosť** | **§ 28 ods. 8** Žiadame zadefinovať pojem kybernetický terorizmus a doplniť pojem kybernetický útok. Odôvodnenie: Obsah pojmu kybernetický terorizmus nie je známy. V tejto súvislosti je rovnako vhodné zaviesť aj pojem útok (vrátane kybernetického), ktorý je v zmysle medzinárodného práva štandardne používaný a v prípade jeho naplnenia Ozbrojené sily Slovenskej republiky plnia úlohy na úseku obrany štátu. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že ustanovenie bolo vypustené. Pripomienky subjektov boli rozporné a text zjednodušený a vecne upravený v rámci ustanovení o riešení kybernetických bezpečnostných incidentov. Text bol preformulovaný a vysvetlenie je v dôvodovej správe. |
| **VšZP** | **Čl. I, § 29, 30** Navrhujeme detailnejšie upraviť výkon kontrol a auditov (ako aj akreditáciu). Odôvodnenie: Predchádzanie prípadným rozporom pri výkone kontrol a auditov. | O | A |  |
| **VšZP** | **Čl. I, § 19 ods. 4** Navrhujeme spresniť uvedené ustanovenie v tom zmysle, aby bolo možné určiť aaspoň minimálne technológie, ktoré musia byť impementované. | O | N | Vaša pripomienka nebola akceptovaná z dôvodu, že taxatívne vymenovanie je neúčelné. |
| **VšZP** | **čl. I §3** Navrhujeme v zákone presnejšie vymedziť pojem "kybernetická bezpečnosť". Odôvodnenie: Stotožňovanie / zamieňanie pojmov "informačná bezpečnosť" a "kybernetická bezpečnosť" v praxi. | O | A |  |
| **VšZP** | **Čl. I § 18 ods. 4** V prípade plnenia predmetných povinností zo strany zdravotných poisťovní, upozorňujeme na možný rozpor s § 76 zákona č. 581/2004 Z.z. o zdravotných poisťovniach, dohľade nad zdravotnou starostlivosťou a o zmene a doplnení niektorých zákonov v znení neskroších predpisov (povinnosť mlčanlivosti). | O | N | Nejde o pripomienku. |
| **ZPW** | **Návrh Združenia poskytovateľov webhostingu (ZPW) na doplnenie Návrhu zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov** Návrh Združenia poskytovateľov webhostingu (ZPW) na doplnenie Návrhu zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov Vzhľadom nato, že: ------------------- - štát dlhodobo nemá pod kontrolou svoju národnú doménu .SK a jej správu zabezpečuje prostredníctvom súkromnej firmy bez majetkovej účasti štátu; - štát nemá prístup k databázam registrovaných .SK domén, ani vlastníkov a registrátorov príslušných domén, a ani k zálohám týchto údajov; - pravidlá a systém správy národnej domény .SK nereflektujú požiadavky modernej doby a potrieb verejného a súkromného sektora; - je potrebné minimalizovať riziká spojené s prevádzkou národnej domény .SK a to aj s ohľadom na možné prípady kybernetických útokov alebo sabotáže. Navrhujeme: ----------- Doplniť do návrhu zákona do časti Systém zabezpečenia kybernetickej bezpečnosti nový paragraf Správa národnej domény s nasledujúcim znením: § 29 Správa národnej domény 1. Správcom národnej domény .sk je Úrad podpredsedu vlády SR pre investície a informatizáciu. 2. Prevádzkovateľom databázy menného priestoru domén druhej úrovne doménových menných serverov je verejná organizácia Národná doména.sk (ďalej len „organizácia ND.SK“), zriadená pre tento účel Úradom podpredsedu vlády SR pre investície a informatizáciu, ktorá je povinná: a. zabezpečovať nepretržitú, bezpečnú a bezporuchovú prevádzku databázových doménových menných serverov a poskytovať menný priestor domén druhej úrovne v súlade s pravidlami podľa § 29 ods. 2, b. poskytovať službu prístupu k databáze serverov registrátorom doménových mien druhej úrovne, c. zabezpečovať vzájomné prepojenia databázových menných serverov druhej úrovne a medzinárodných databázových menných serverov. 3. Úrad a organizácia ND.SK a. prijmú legislatívne, technické a technologické opatrenia, za účelom bezpečného a vierohodného rozpoznávania a používania doménových mien v Slovenskej republike, b. podporia nové technológie pre zvýšenie bezpečnosti prevádzky národnej domény. 4. Organizácia ND.SK je oprávnená za poskytované služby požadovať od registrátorov doménových mien druhej úrovne finančnú úhradu nákladov v primeranej výške. Účtovníctvo organizácie ND.SK podlieha kontrole Úradu. Výnos z platieb za poskytovanie služieb je príjmom štátneho rozpočtu a je určený na rozvoj internetu Slovenskej republiky. 5. Registrátorom domény druhej úrovne je organizácia, ktorú touto činnosťou na základe výberového konania poverí Úrad. Registrátor je povinný dodržiavať pravidlá poskytovania menného priestoru národnej domény, schválené Úradom a vydané organizáciou ND.SK. 6. Registrátor je oprávnený za poskytovanie služieb registrácie domény druhej úrovne vyberať od konečného užívateľa finančnú náhradu vo výške stanovenej v cenníku služieb a výkonov, ktorý je nedeliteľnou súčasťou pravidiel podľa § 29 ods.2. 7. Ministerstvo môže zrušiť poverenie výkonu činnosti registrátorovi, ak tento napriek písomnej výzve porušuje pravidlá. Ministerstvo koná v tomto prípade na základe a. oznámenia organizácie ND.SK, b. vlastného šetrenia, c. výzvy iných registrátorov. Zdôvodnenie: ------------ Národná doména SK patrí Slovenskej republike a je základným stavebným kameňom slovenského internetu. Je používaná nielen súkromným, ale i verejným sektorom, a to vrátane štátnych elektronických služieb poskytovaných občanom. Doména SK má dopad na všetky aspekty života občanov Slovenskej republiky. Subjekty pôsobiace v rámci Slovenskej republiky pri svojej činnosti doménu .SK používajú. V mnohých prípadoch ide o služby, ktoré okrem internetu nemajú žiadnu inú alternatívu. Je preto nevyhnutné zabezpečiť stabilnú a bezporuchovú prevádzku internetovej infraštruktúry, vrátane národnej domény .SK. Elektronické služby sa používajú na dennej báze a ich potenciálny výpadok by mal ďalekosiahle nepriaznivé až fatálne dôsledky na fungovanie celej našej spoločnosti. Neexistuje iná slovenská národná doména. Doména .SK je len jedna, a preto je nutné i vhodné, aby jej správa bola náležite upravená zákonom. Tým jej bude poskytnutý legitímny právny rámec nateraz aj do budúcnosti. Zároveň je nutné starostlivo vybrať správcu i prevádzkovateľa domény .SK vzhľadom na uvedené okolnosti a potreby. Súčasným správcom domény .SK je súkromná spoločnosť SK-NIC, a.s. Vo svete národných domén (ccTLD) ide o netypický model fungovania. Národná doména sa iných krajinách považuje za verejný statok a obvykle jej prevádzku zabezpečuje štátom zriadená organizácia, tak ako je navrhnuté v tejto pripomienke. Súčasný správca domény .SK spoločnosť SK-NIC, a.s., nie je vystavený žiadnemu konkurenčnému trhovému tlaku, ani priamym sankciám vyplývajúcim zo zmluvného vzťahu. Preto je národná doména .SK dlhodobo zanedbávaná a jej problémy ignorované. V zóne .SK chýba zabezpečovací mechanizmus DNSSEC, API, webstránka www.sk-nic.sk je len v slovenskom jazyku, a pod. Svojím konaním resp. nekonaním spoločnosť SK-NIC, a.s. brzdí rozvoj slovenského internetu, verejných služieb a súkromného podnikania. Keďže navyše ide o súkromnú spoločnosť, štát na ňu nemá priamy dosah. Rovnako tak štát nemá dosah ani na svoju národnú doménu .SK, pretože nevlastní databázy k predmetným doménam a ich vlastníkom a registrátorom, a nedisponuje ani zálohami týchto databáz. V prípade útoku alebo sabotáže nebude v silách štátnych orgánov obnoviť prevádzku celej domény .SK. O problém správy národnej domény sa zaujíma odborná i laická verejnosť. Na stránke NasaDomena.sk aktuálne prebieha internetová petícia za vrátenie .SK domény spať ľuďom a komunite. Petícia, ktorú podporilo už viac ako 8700 ľudí, si kladie za cieľ: 1. Pripraviť plán na presunutie správy .SK domény na novú nezávislú a neziskovú organizáciu 2. Zabezpečiť, aby sa správa .sk domény dostala mimo kontrolu jediného súkromného subjektu, a aby sa dostala pod väčšiu kontrolu štátu a komunity Oba tieto ciele sú v súlade s navrhovaným doplnením zákona. Myslíme si, že pôvodný návrh zákona o informačnej bezpečnosti z roku 2015 náležite riešil všetky načrtnuté problémy. Považujeme tento návrh za dobrý, preto navrhujeme sa k pôvodným bodom o správe národnej domény vrátiť a zapracovať ich do aktuálneho zákona. | Z | N | Vaša pripomienka nebola akceptovaná, problematika si vyžaduje širšiu diskusiu, snahy NBÚ o úpravy v rámci konzultácií boli (a aj sú), ale v rámci takto krátkeho obdobia sa nepodarilo nájsť komplexné riešenie a preto, v prípade pretrvávajúceho záujmu spoločnosti, bude problematika systémovo riešenie pri najbližšej novele tohto zákona. |