

VYHODNOTENIE MEDZIREZORTNÉHO PRIPOMIENKOVÉHO KONANIA

Návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
a ktorým sa menia a dopĺňajú niektoré zákony

Spôsob pripomienkového konania

Počet vznesených pripomienok, z toho zásadných

381 /219

Počet vyhodnotených pripomienok

381

Počet akceptovaných pripomienok, z toho zásadných

140 /61

Počet čiastočne akceptovaných pripomienok, z toho zásadných

85 /67

Počet neakceptovaných pripomienok, z toho zásadných

156 /91

Rozporové konanie (s kým, kedy, s akým výsledkom)

Počet odstránených pripomienok

Počet neodstránených pripomienok

Sumarizácia vznesených pripomienok podľa subjektov

Č.	Subjekt	Pripomienky do termínu	Pripomienky po termíne	Nemali pripomienky	Vôbec nezaslali
1.	Asociácia kybernetickej bezpečnosti, o.z.	33 (0o,33z)	0 (0o,0z)		
2.	Americká obchodná komora v Slovenskej republike	16 (0o,16z)	0 (0o,0z)		
3.	Asociácia zamestnávateľských zväzov a združení Slovenskej republiky	4 (1o,3z)	0 (0o,0z)		
4.	Dopravný úrad	3 (2o,1z)	0 (0o,0z)		

5.	eustream, a.s.	3 (0o,3z)	0 (0o,0z)		
6.	Generálna prokuratúra Slovenskej republiky	14 (6o,8z)	0 (0o,0z)		
7.	Ministerstvo dopravy a výstavby Slovenskej republiky	17 (13o,4z)	0 (0o,0z)		
8.	Ministerstvo financií Slovenskej republiky	23 (14o,9z)	0 (0o,0z)		
9.	Ministerstvo hospodárstva Slovenskej republiky	15 (6o,9z)	0 (0o,0z)		
10.	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky	34 (7o,27z)	0 (0o,0z)		
11.	Ministerstvo kultúry Slovenskej republiky	6 (4o,2z)	0 (0o,0z)		
12.	Ministerstvo obrany Slovenskej republiky	8 (2o,6z)	0 (0o,0z)		
13.	Ministerstvo práce, sociálnych vecí a rodiny Slovenskej republiky	1 (1o,0z)	0 (0o,0z)		
14.	Ministerstvo spravodlivosti Slovenskej republiky	3 (3o,0z)	0 (0o,0z)		
15.	Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky	1 (1o,0z)	0 (0o,0z)		
16.	Ministerstvo vnútra Slovenskej republiky	26 (10o,16z)	0 (0o,0z)		
17.	Ministerstvo zdravotníctva Slovenskej republiky	3 (2o,1z)	0 (0o,0z)		
18.	Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky	11 (11o,0z)	0 (0o,0z)		
19.	Národná banka Slovenska	12 (10o,2z)	0 (0o,0z)		
20.	Republiková únia zamestnávateľov	38 (10o,28z)	0 (0o,0z)		
21.	Slovenská banková asociácia	16 (5o,11z)	0 (0o,0z)		

22.	Smart Consumer Institute	1 (0o,1z)	0 (0o,0z)		
23.	Slovenská informačná služba	3 (2o,1z)	0 (0o,0z)		
24.	SK-NIC, a.s.	19 (7o,12z)	0 (0o,0z)		
25.	Sociálna poisťovňa, Ul. 29 augusta č. 8 a 10, 813 63 Bratislava 1	1 (1o,0z)	0 (0o,0z)		
26.	Úrad jadrového dozoru Slovenskej republiky	28 (22o,6z)	0 (0o,0z)		
27.	Úrad pre reguláciu elektronických komunikácií a poštových služieb	1 (0o,1z)	0 (0o,0z)		
28.	Úrad priemyselného vlastníctva Slovenskej republiky	2 (2o,0z)	0 (0o,0z)		
29.	Verejnosť	15 (15o,0z)	0 (0o,0z)		
30.	Združenie bezpečnostného a obranného priemyslu Slovenskej republiky	5 (0o,5z)	0 (0o,0z)		
31.	Združenie poskytovateľov webhostingu	19 (5o,14z)	0 (0o,0z)		
32.	Štatistický úrad Slovenskej republiky (Úrad vlády Slovenskej republiky, odbor legislatívy ostatných ústredných orgánov štátnej správy)	0 (0o,0z)	0 (0o,0z)	x	
33.	Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky (Úrad vlády Slovenskej republiky, odbor legislatívy ostatných ústredných orgánov štátnej správy)	0 (0o,0z)	0 (0o,0z)	x	
34.	Ministerstvo pôdohospodárstva a rozvoja vidieka Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
35.	Úrad geodézie, kartografie a katastra Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
36.	Protimonopolný úrad Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	

37.	Ministerstvo životného prostredia Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
38.	Úrad vlády Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
39.	Úrad pre verejné obstarávanie	0 (0o,0z)	0 (0o,0z)		x
40.	Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
41.	Štatistický úrad Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
42.	Správa štátnych hmotných rezerv Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
43.	Najvyšší kontrolný úrad Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
44.	Najvyšší súd Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
45.	Národná rada Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
46.	Kancelária Ústavného súdu Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
47.	Odbor aproximácie práva sekcie vládnej legislatívy Úradu vlády SR	0 (0o,0z)	0 (0o,0z)		x
48.	Slovenská poľnohospodárska a potravinárska komora	0 (0o,0z)	0 (0o,0z)		x
49.	Združenie miest a obcí Slovenska	0 (0o,0z)	0 (0o,0z)		x
50.	Splnomocnenec vlády Slovenskej republiky pre rómske komunity	0 (0o,0z)	0 (0o,0z)		x
51.	Konfederácia odborových zväzov Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
52.	Úrad pre dohľad nad zdravotnou starostlivosťou	0 (0o,0z)	0 (0o,0z)		x
53.	Konferencia biskupov Slovenska	0 (0o,0z)	0 (0o,0z)		x

54.	Asociácia priemyselných zväzov	0 (0o,0z)	0 (0o,0z)		x
55.	Národný bezpečnostný úrad	0 (0o,0z)	0 (0o,0z)		x
	Spolu	381 (162o,219z)	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
AKB	Návrh znenia nového § 27a ods. 2 zákona: „(2) Úrad vypracuje a zverejní v jednotnom informačnom systéme kybernetickej bezpečnosti zoznam rizikových tretích strán alebo iných osôb. Rizikovosť tretích strán alebo iných osôb úrad vyhodnocuje v rámci analýzy rizík, pri ktorej zohľadňuje nasledovné kritériá: a) hybridné hrozby (Spoločné oznámenie európskemu parlamentu a rade Spoločný rámec pre boj proti hybridným hrozbám reakcia Európskej únie: https://eur-lex.europa.eu/legal-content/sk/ALL/?uri=CELEX:52016JC0018 (04.10.2020) a politické riziká, najmä potenciálny alebo skutočný vplyv krajiny mimo Európskej únie („tretia krajina“) na tretiu stranu alebo inú osobu, b) právne predpisy tretej krajiny v oblasti ochrany základných ľudských práv a slobôd, ochrany osobných údajov a ochrany informácií, c) vlastnícka a riadiaca štruktúra tretej strany alebo inej osoby, d) počet a typy odhalených zraniteľností a kybernetických bezpečnostných incidentov u tretej strany alebo inej osoby spolu so spôsobom a časovým obdobím ich odstránenia, e) miera, do akej tretia strana alebo iná osoba vykonáva kontrolu nad procesom výroby a dodania hardvéru alebo softvéru a riziká pre proces výroby a dodania hardvéru alebo softvéru. Úrad zoznam rizikových tretích strán a iných osôb pravidelne aktualizuje, a to aspoň raz za 12 mesiacov od poslednej analýzy rizík alebo pri každej významnej zmene majúcej vplyv na identifikované riziká alebo rozsah tretích strán.“.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

AKB	Návrh znenia nového § 27a ods. 3 zákona „(3) Výstupom analýzy rizík podľa ods. 2 je: a) vysoké riziko, pokiaľ tretia strana alebo iná osoba predstavuje vysoké riziká pre kybernetickú bezpečnosť alebo bezpečnostné záujmy Slovenskej republiky, pričom identifikované riziká nie je možné znížiť prijatím príslušných opatrení, b) stredné riziko, pokiaľ tretia strana alebo iná osoba predstavuje vysoké riziká pre kybernetickú bezpečnosť alebo bezpečnostné záujmy Slovenskej republiky, pričom identifikované riziká je možné znížiť prijatím príslušných opatrení na úroveň nízka alebo žiadna, c) nízke riziko, pokiaľ tretia strana alebo iná osoba predstavuje nízke riziká pre kybernetickú bezpečnosť alebo bezpečnostné záujmy Slovenskej republiky a identifikované riziká je možné odstrániť prijatím príslušných opatrení, alebo d) žiadne riziko, pokiaľ tretia strana alebo iná osoba nepredstavuje žiadne alebo len zanedbateľné riziká pre kybernetickú bezpečnosť alebo bezpečnostné záujmy Slovenskej republiky.“.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	Návrh znenia nového § 27a ods. 4 zákona „(4) Ak je výstupom analýzy rizík podľa ods. 2 vysoké alebo stredné riziko, úrad zaradí tretiu stranu alebo inú osobu na zoznam podľa ods. 1 spolu s kvantifikáciou rizika, ktoré bolo dôvodom na zaradenie tretej strany alebo inej osoby na zoznam. Tretia strana alebo iná osoba nachádzajúca sa na zozname podľa ods. 1 je oprávnená predložiť úradu námietky spolu s dôkazmi preukazujúcimi neexistenciu alebo zníženie vysokého alebo stredného rizika. Úrad o námietkach tretej strany alebo inej osoby rozhodne do [doplniť] dní odo dňa ich doručenia, v odôvodnených prípadoch je úrad oprávnený túto lehotu predĺžiť, o čom je povinný tretiu stranu alebo inú osobu pred uplynutím pôvodnej lehoty na	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	vybavenie námietok tretej strany alebo inej osoby informovať.“.			
AKB	Návrh znenia nového § 27a ods. 5 zákona „(5) V prípade, ak je výstupom analýzy rizík podľa ods. 2: a) vysoké riziko, prevádzkovateľ základnej služby, tretia strana alebo iná osoba nesmie začať používať služby, produkty alebo procesy tejto tretej strany alebo inej osoby a v prípade existujúcich vzťahov ukončiť používanie služieb, produktov alebo procesov tejto tretej strany alebo inej osoby do [doplniť] mesiacov odo dňa zaradenia tretej strany alebo inej osoby na zoznam podľa ods. 1, b) stredné riziko, prevádzkovateľ základnej služby, tretia strana alebo iná osoba nesmie začať používať služby, produkty alebo procesy tejto tretej strany alebo inej osoby a v prípade existujúcich vzťahov s treťou stranou alebo inou osobou môže používať služby, produkty alebo procesy tejto tretej strany alebo inej osoby v rozsahu platnom ku dňu zaradenia tretej strany alebo inej osoby na zoznam podľa ods. 1.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	Návrh znenia nového § 27a ods. 1 zákona „§ 27a Pôsobnosť úradu pri posudzovaní hybridných hrozieb a politických rizík tretích strán a iných osôb (1) Úrad rozhodnutím podľa osobitného predpisu (Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov) zakáže alebo obmedzí prevádzkovateľovi základnej služby, tretej strane podľa § 19 ods. 2 alebo inej osobe používať služby, produkty alebo procesy tretej strany alebo inej osoby s vysokým alebo stredným rizikom identifikovaným za podmienok podľa § 27a, ak je to potrebné na zaistenie kybernetickej bezpečnosti alebo z dôvodov bezpečnostného záujmu Slovenskej republiky.“. Odôvodnenie: Opätovne sa jedná sa o veľmi široké oprávnenie úradu zakázať alebo	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	obmedziť ktorémukoľvek prevádzkovateľovi základnej služby používať konkrétny produkt, proces alebo službu pod vägne koncipovanou podmienkou „ak je to potrebné na zaistenie kybernetickej bezpečnosti, alebo z dôvodov bezpečnostného záujmu Slovenskej republiky“, pod čo je možné subsumovať v zásade čokoľvek. Aj keď pôvodnou motiváciou pri koncipovaní tohto ustanovenia mohol byť záujem o implementáciu Európskeho toolboxu kybernetickej bezpečnosti 5G sietí (EU Toolbox) (nie je možné identifikovať ani z dôvodovej správy, keďže v nej je odôvodnením zavedenia takéhoto oprávnenia úradu prerozprávanie tohto nového oprávnenia inými slovami), platí, že len takýmto oprávnením úrad povinnosť implementácie EU Toolboxu rozhodne nedosiahne a súčasne sa jedná o oprávnenie úradu, ktoré je vysoko rizikové, zneužívateľné, netransparentné a nepreskúmateľné. EU Toolbox obsahuje hneď tri typy opatrení, a to: strategické, technické a tzv. podporné akcie / opatrenia. Samotné strategické opatrenia sa ďalej členia v kontexte adresátov týchto opatrení, a to: právomoci regulačných orgánov, dodávateľa - tretie strany, diverzifikácia dodávateľov – tretích strán a udržateľnosť a rozmanitosť dodávateľského a hodnotového reťazca. Súčasťou strategických opatrení siete je aj časť posilnenie regulačných právomocí orgánov, konkrétne oprávnenia týchto orgánov v podobe uloženia povinností týkajúcich sa bezpečnosti poskytovateľom 5G a ex-ante (teda nie aj spätne) obmedzenie, zákaz alebo uloženie konkrétnych požiadaviek poskytovateľom 5G, avšak na základe prístupu založenom na riziku a berúc do úvahy ďalšie EU Toolboxom označené parametre. Z uvedeného teda vyplýva, že malou súčasťou v rámci strategických opatrení EU Toolboxu je aj posilnenie oprávnení regulačných orgánov, avšak uvedené oprávnenia sú podmienené rizikovým			
--	--	--	--	--

	prístupom, vyhodnocovaním aj hybridných hrozieb a politických rizík a jasne danými parametrami, ktoré musí regulačný orgán vziať pri výkone týchto oprávnení do úvahy. Vychádzajú z textácie § 27 ods. 1 písm. e) je preto nutné konštatovať, že nielenže sa nejedná o náležitú implementáciu požiadaviek EU Toolbox, ale ani náležitú implementáciu čo i len jedného opatrenia či požiadavky EU Toolboxu. Úrad sa tak zrejme mohol inšpirovať jednou z častí EU Toolboxu, avšak vyňal si z neho len časť, ktorá mu najviac vyhovuje, a to bez akýchkoľvek súvisiacich povinností úradu pri výkone tohto oprávnenia, jeho limitácie a súvisiacich pravidiel. Naviac toto oprávnenie je použiteľné nielen ex-ante, ale aj ex-post a nielen voči poskytovateľom 5G, resp. v jazyku zákona prevádzkovateľom základných služieb prevádzkujúcich základne služby v sektore Elektronické komunikácie, podsektore siete a služby republiky pevných a mobilných elektronických komunikácií (predmet záberu EU Toolboxu), ale na všetkých prevádzkovateľov základných služieb. Nesúlad prístupu úradu vo vzťahu k tejto novozavedenej kompetencii v kontexte EU Toolboxu je preto daný hneď niekoľko krát, a to skutočnosťou, že úrad nereflektoval na všetky požiadavky EU Toolbox, vytiahol si z neho len časť, ktorá je pre neho najvyhovujúcejšia a túto bez akýchkoľvek dodatočných pravidiel, obmedzení či limitácií rozšíril na všetky sektory a podsektory a všetkých prevádzkovateľov základných služieb. EU Toolbox pritom jasne identifikuje, akým spôsobom sa má implementovať. V prvom rade sú štáty povinné vychádzať z dokumentu Spoločné európske posúdenie rizík súvisiacich s 5G sieťami a vlastného národného hodnotenia rizík, ktoré za Slovenskú republiku spracoval práve úrad. Následne sú štáty povinné tieto riziká (hybridné hrozby a v ich kontexte aj politické riziká)			
--	---	--	--	--

	zohľadňovať a vyhodnotiť, či súčasné legislatívne nastavenie (požiadavky) je dostatočné a na tieto hybridné hrozby a politické riziká reflektuje. Ďalej sú štáty povinné v kontexte identifikovaných rizík (vrátane politických) a ich riadenia zvoliť príslušné opatrenia identifikované EU Toolboxom a tieto implementovať, príp. zaviesť ako príslušnú legislatívnu požiadavku. V zmysle uvedeného je teda zrejmé, že nielen novonavrhnutá kompetencia úradu, ale ani celá novela zákona nereflektuje na požiadavky EU Toolboxu, žiadnym spôsobom sa nevysporiadava s povinným rizikovým prístupom (hybridné hrozby, politické riziká) a zavádza kompetenciu, pri ktorej uplatnení úrad nie je povinný reflektovať a vyhodnocovať žiadne riziká (nielen politické) a ktorú úrad môže používať v zásade v neobmedzenom a nekontrolovateľnom rozsahu. V tomto kontexte je nutné poukázať aj na prístupy ostatných štátov implementujúcich EU Toolbox, ktoré sú omnoho čitateľnejšie, pragmatickejšie a hlavne súladné s požiadavkami EU Toolboxu. Jedným s využívaných prístupov je vytvorenie zoznamu „rizikových dodávateľov“ podľa vopred zadefinovaných parametrov, ktoré sú transparentné a objektívne a ktorý (zoznam) následne poskytuje rámec pre prevádzkovateľov základných služieb, akých dodávateľov nemôžu do budúcnosti využívať. Zoznam je priebežne aktualizovaný, je vytvorený priestor na „obranu“ zo strany dodávateľov na tomto zozname vyvinúť sa a preukázať, že dané hybridné hrozby a politické riziká na ich strane nie sú alebo už nie sú. Predmetný prístup je súčasne charakterizovaný zavedením presných vyhodnocovacích pravidiel a súčasne prechodných období na zosúladienie už existujúcich zmluvných vzťahov s takýmito rizikovými dodávateľmi, či už nachádzajúcimi sa v zozname stanovenom (napr.) úradom alebo vyplývajúcimi z analýzy rizík vykonanej v			
--	---	--	--	--

	súlade s EU Toolbox. Takýto prístup považujeme za vhodný a správny, vyhovuje požiadavke EU Toolboxu na implementáciu zo strany štátu (teda ponechanie požiadavky na vyhodnocovanie rizikovosti na strane štátu, nie jej prenos na prevádzkovateľov základných služieb, ktorí nevedia, čo a ako majú vyhodnocovať), pričom tento prístup je auditovateľný a riziká jeho možného zneužitia sú zásadne minimalizované. V prípade doplnenia zákona o takýto systém vyhodnocovania rizikovosti dodávateľov (hybridné hrozby, politické riziká) by následne prichádzalo do úvahy aj ponechanie novonavrhnutej kompetencie úradu, ktorá má aký taký základ a opodstatnenie aj v zmysle samotného EU Toolbox, aj keď v omnoho oklieštenejšej forme a ktorej využitie by bolo podmienené až nesúlalom prevádzkovateľa základnej služby so zoznamom rizikových dodávateľov, teda využívaním takéhoto dodávateľa aj po uplynutí príslušného prechodného obdobia na zosúladienie zmluvných vzťahov. Prístup len v podobe navrhnutého písm. e) v § 27 ods. 1 sa sám o sebe vyznačuje vysokými rizikami možného zneužitia, nevysporiadava sa s už existujúcimi (zmluvnými) vzťahmi, neobmedzuje sa len na 5G sieť, ale v zásade na akýkoľvek produkt, službu či proces. Takéto rozšírenie kompetencií jediného štátneho orgánu je nežiaduce, implementačnú povinnosť vo vzťahu k EU Toolbox plní prvoplánovo, rozhodne nedostatočne a súčasne aj v rozpore s požiadavkami EU Toolboxu. Zároveň dotknuté osoby strácajú relevantné právne nástroje na ochranu voči takémuto rozhodnutiu či postupu úradu, nakoľko postup úradu pri výkone tejto novej kompetencie je navrhnutý byť vyňatý z pôsobnosti správneho poriadku. Jediným účinným prostriedkom ochrany by teda bolo až súdne konanie. Vzhľadom k skutočnosti, že povinnosť náležitej implementácie EU Toolboxu je stále daná, upriamujeme pozornosť			
--	--	--	--	--

	na našu všeobecnú pripomienku, v kontexte ktorej pri zachovaní nového oprávnenia úradu podľa § 27 ods. 1 písm. e) navrhujeme v zákone vytvoriť priestor pre zavedenie systému vyhodnocovania politických / hybridných hrozieb dodávateľov súhrnne označených ako prevádzkovatelia základných služieb, tretie strany a iné osoby predpokladaný novovytvoreným nového § 27a zákona, ktorý by vytvoril základ pre vyhodnocovanie rizikovosti, určil proces vyhodnocovania rizík a stanovil prechodné obdobia na zosúladenie povinných osôb so zisteniami (výsledkami analýzy rizík). Novovytvorený § 27a zákona by tak jednak identifikovali povinnosti vyhodnocovania rizikovosti dodávateľov (kontext hybridných hrozieb a politických rizík), ktorú by podľa presných parametrov plnil úrad, ktorej výstupom by bol zoznam rizikových dodávateľov a ktorý by boli povinné osoby povinné reflektovať. Až v prípade nesúladu prevádzkovateľov základných služieb s predmetným zoznamom (blacklist) po uplynutí prechodného obdobia by bolo dané oprávnenie úradu zakázať využívanie takéhoto dodávateľa (súhrnne označeného ako tretia strana a iná osoba). Dôvod na zavádzanie pojmu iná osoba (popri tretej osobe, ktorá je v rámci zákona v platnom znení zadefinovaná v § 19 ods. 2 ako dodávateľ na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby) je obsiahnuť čo najširší okruh osôb, u ktorých by mohli byť vyhodnocované hybridné hrozby a politické riziká, nakoľko pojem tretia osoba tento účel v súčasnom znení zákona nenapĺňa (len dodávateľ na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby). V prípade, pokiaľ by návrh novely zákona v rámci § 19 ods. 2 zákona (viď bod 24 vlastného materiálu návrhu zákona, ktorým sa mení a			
--	--	--	--	--

	dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony) prešiel a došlo by k plánovanému vypusteniu definičného vymedzenia pojmu tretia strana, potom by pojem iná osoba nebol potrebný. Inou osobou sa na účely tohto návrhu rozumie napr. Úrad pre reguláciu elektronických komunikácií a poštových služieb, ktorý nespadá ako pod pojem prevádzkovateľ základnej služby, tak ani tretia strana v súčasnom znení zákona (§ 19 ods. 2). Záverom poukazujeme aj na prístup v rámci EÚ, kedy Rada podporuje závery Rady z 9. júna 2020 o formovaní digitálnej budúcnosti Európy. a ktorá vyzýva EÚ a členské štáty, aby plne využili súbor nástrojov 5G pre kybernetickú bezpečnosť prijatý 29. januára 2020 (EU Toolbox), a najmä aby uplatnil príslušné obmedzenia na vysoko rizikových dodávateľov pre kľúčové aktíva definované ako kritické a citlivé v EU coordinated risk assessments. hodnotenia. Rada ďalej zdôrazňuje, že potenciálnych dodávateľov 5G je potrebné posudzovať na základe spoločných objektívnych kritérií. Kompletné znenie je možné nájsť tu: https://www.consilium.europa.eu/media/45930/021020-euco-final-conclusions-sk.pdf. Aj v zmysle uvedenej pozície Rady vnímame nami navrhovaný prístup za správny, EÚ predpokladaný, vyžadovaný a očakávaný. V kontexte celého návrhu nového znenia § 27a navrhujeme primerane upraviť aj ostatné časti zákona, ktoré je potrebné previazať s týmito novými povinnosťami úradu.			
AKB	čl. I bod 33 „§ 27a sa vypúšťa.“. Pozn. nejde o § 27a v zmysle bodov 19 až 24 tohto návrhu. Ide o navrhované znenie § 27a, ktoré bolo predložené do MPK Odôvodnenie: Úrad si navrhuje novú kompetenciu /	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k

	oprávnenie, a to rozhodovať o blokovaní pri riešení kybernetického bezpečnostného incidentu. Úrad v dôvodovej správe uvádza, že sa jedná o zhmotnenie vznesenej spoločenskej požiadavky efektívneho zamedzovania škodlivých aktivít alebo škodlivého obsahu na internete, hoci takúto spoločenskú objednávku, či požiadavku sme nezaznamenali. Rovnako sme nezaznamenali širšiu spoločenskú diskusiu na túto tému, čoho dôsledkom je veľmi široko a neurčito koncipované oprávnenie úradu „pri riešení kybernetického bezpečnostného incidentu“ blokovať. Jedná sa teda o ďalšie oprávnenie úradu, pri ktorom absentujú konkrétne pravidlá zamedzujúce zneužitiu, ktoré je nepredvídateľné a nie je možné sa voči nemu účinne (právne) brániť, nakoľko konanie úradu v rozsahu tejto kompetencie je vyňaté z pôsobnosti správneho poriadku, v dôsledku čoho sú dotknuté osoby nútené domáhať sa ochrany svojich práv a nárokov výlučne súdnou cestou. Nebránime sa zavedeniu kompetencie blokovania do právneho poriadku, avšak s jasnými pravidlami, podmienkami a obmedzeniami namiesto neurčitého „pri riešení kybernetického bezpečnostného incidentu“. Výkon rozhodnutia o blokovaní totižto môže predstavovať významný zásah do základných práv a slobôd, napr. do súkromného vlastníctva, preto by nemalo byť v kompetencii jediného štátneho orgánu v zásade bez akejkoľvek kontroly. Súčasne nie je na základe týchto ustanovení zrejmé, ako bude úrad rozhodovať o blokovaní, hlavne o tom, na ktorej infraštruktúre je potrebné blokovanie vykonať (teraz nehovoríme o výkone právoplatného rozhodnutia oprávnených subjektov), čo sa vlastne blokovať bude, napr. iba IP adresa alebo doména, webové sídlo, DNS dotazy, spam? Alebo čokoľvek podľa vlastného uváženia? (priestor na cenzúru???) V bode 10 návrhu sa hovorí o blokovaní škodlivého obsahu respektíve		ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
--	--	--	---

	škodlivej aktivity, pričom ani jeden z týchto pojmov nebol doplnený do definícií. Zároveň sa podľa nášho názoru jedná o neprimerané rozšírenie povinných osôb – prevádzkovateľ infraštruktúry je oveľa širší pojem ako prevádzkovateľ základnej služby alebo poskytovateľ digitálnej služby. Rozhodnutie úradu o blokovaní je konečné – teda neexistuje žiaden opravný prostriedok. Čo, ak takéto zablokovanie znemožní poskytovanie základnej služby? Čo znášanie nákladov, ktoré prevádzkovateľovi vzniknú? Čo časové ohraničenie rozhodnutia? (z návrhu by malo byť zrejmé, že nebude trvať aj po odstránení škodlivého obsahu. Ako sa bude rozhodovať o odblokovaní? V akej lehote? Aj takéto rozhodnutie úradu bude konečné?			
AKB	Návrh znenia nového § 34a zákona „§ 34a Prechodné ustanovenia účinné od [dátum] Úrad vykoná prvú analýzu rizík podľa § 27a ods. 2 a vypracuje a zverejní prvý zoznam podľa § 27a ods. 1 do troch mesiacov odo dňa účinnosti tohto zákona.“. Odôvodnenie: Jedná sa o precizovanie, kedy je úrad povinný vykonať prvú analýzu rizík podľa § 27a ods. 2 a vypracovať a zverejniť prvý zoznam rizikových tretích strán a iných osôb, na čo je ďalej viazaný celý proces v zmysle § 27a zákona.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	čl. I bod 48 „V § 34 odsek 11 znie nasledovne: Prevádzkovateľ základnej služby podľa § 3 písm. k) druhý bod môže v období od 1. januára 2020 do 31. decembra 2023 pre kategóriu I. sietí a informačných systémov zabezpečiť plnenie povinnosti podľa § 29 vykonaním posúdenia účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek stanovených týmto zákonom, prostredníctvom manažéra	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej

	kybernetickej bezpečnosti podľa § 20 ods. 3 písm. a) funkcionalitou jednotného informačného systému kybernetickej bezpečnosti.“. Odôvodnenie: Doplnenie reflektuje na pôvodný zámer umožniť obciam do 6000 obyvateľov (viď Vyhlášku č. 179/2020 Z.z.) inak povinným na audit kybernetickej bezpečnosti vykonať tzv. „self-assessment“ prostredníctvom manažéra kybernetickej bezpečnosti namiesto podstúpenia auditu kybernetickej bezpečnosti. Súčasne doplnenie reflektuje na skutočnosť, že návrh nerozlišuje medzi typmi prevádzkovateľov základných služieb, kedy vnímame zásadný rozdiel medzi obcou do 6000 obyvateľov v zmysle Vyhlášky č. 179/2020 Z.z. a akýmkoľvek iným prevádzkovateľom základných služieb. Uvedené však navrhujeme len pre kategóriu I ako najmenej citlivú kategóriu, pre ktorú sa majú plniť požiadavky zákona a nesúhlasíme s rozšírením aj na II. kategóriu, kde by režim implementácie požiadaviek zákona mal podliehať auditu kybernetickej bezpečnosti. Zároveň by u väčšiny prevádzkovateľov základných služieb vznikla dvojznačnosť, podľa ktorej by prevádzkovatelia museli vykonávať samoposúdenie prostredníctvom JSIKB a zároveň aj vykonať audit kybernetickej bezpečnosti.			akceptovateľnej miere pripomienky všetkých subjektov.
AKB	Návrh znenia nového § 27a ods. 6 zákona „(6) V prípade, ak prevádzkovateľ základnej služby nepostupuje v súlade s ods. 5, úrad je oprávnený postupovať podľa ods. 1.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

AKB	čl. I bod 31 „§ 24 odsek 7 sa vypúšťa.“. Odôvodnenie: Jedná sa o veľmi široké oprávnenie úradu požadovať po ktoromkoľvek prevádzkovateľovi základnej služby zasielať mu ním určené systémové informácie zo sietí a informačných systémov. Inými slovami povedané, úrad sa môže doslova kedykoľvek a vo vzťahu ku ktorémukoľvek prevádzkovateľovi základnej služby rozhodnúť, aby mu ním určeným spôsobom zasielal systémové informácie (logy), čo je neprijateľné a zároveň vysoko rizikové, koncentrovať takto citlivé záznamy, nevynímajúc informácie podliehajúce osobitnému režimu ochrany (napr. bankové tajomstvo, daňové tajomstvo a pod.) na jedinom štátnom orgáne podľa jeho ľubovôle, v ním určenom obsahu, rozsahu a forme. Takto koncipované oprávnenie úradu by prekračovalo pôvodný účel zákona, a to spolupráca subjektov vykonávajúcich pôsobnosť v oblasti kybernetickej bezpečnosti v snahe o zachovanie požadovanej úrovne kybernetickej bezpečnosti štátu a pre neho významných (kritických) základných služieb do pozície autoritatívnej, silovej a jednoducho zneužívateľnej. Súčasne úrad navrhuje pri tomto novom inštitúte vyňať pôsobnosť správneho poriadku, čo ešte viac oslabuje účinnú ochranu jednotlivcov pred takýmto výrazným zásahom a zásadne a neprimerane posilňuje kompetenciu úradu, ktorého konanie by mohol posudzovať až súd, a to dávno po tom, čo by jeho rozhodnutie o presmerovaní systémových informácií bolo vykonané. Prípadný výrok súdu o protiprávnosti alebo nezákonnosti rozhodnutia úradu by tak strácal akýkoľvek význam. V tomto kontexte navrhujeme primerane upraviť aj ostatné časti zákona, ktoré boli s touto novou kompetenciou úradu spojené (napr. správne delikty a pod.).	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
-----	---	---	----	---

AKB	Návrh znenia nového § 27a zákona: „§ 27a Pôsobnosť úradu pri posudzovaní hybridných hrozieb a politických rizík tretích strán a iných osôb (1) Úrad rozhodnutím podľa osobitného predpisu (Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov) zakáže alebo obmedzí prevádzkovateľovi základnej služby, tretej strane podľa § 19 ods. 2 alebo inej osobe používať služby, produkty alebo procesy tretej strany alebo inej osoby s vysokým alebo stredným rizikom identifikovaným za podmienok podľa § 27a, ak je to potrebné na zaistenie kybernetickej bezpečnosti alebo z dôvodov bezpečnostného záujmu Slovenskej republiky. (2) Úrad vypracuje a zverejní v jednotnom informačnom systéme kybernetickej bezpečnosti zoznam rizikových tretích strán alebo iných osôb. Rizikovosť tretích strán alebo iných osôb úrad vyhodnocuje v rámci analýzy rizík, pri ktorej zohľadňuje nasledovné kritériá: a) hybridné hrozby (Spoločné oznámenie európskemu parlamentu a rade Spoločný rámec pre boj proti hybridným hrozbám reakcia Európskej únie: https://eur-lex.europa.eu/legal-content/sk/ALL/?uri=CELEX:52016JC0018 (04.10.2020) a politické riziká, najmä potenciálny alebo skutočný vplyv krajiny mimo Európskej únie („tretia krajina“) na tretiu stranu alebo inú osobu, b) právne predpisy tretej krajiny v oblasti ochrany základných ľudských práv a slobôd, ochrany osobných údajov a ochrany informácií, c) vlastnícka a riadiaca štruktúra tretej strany alebo inej osoby, d) počet a typy odhalených zraniteľností a kybernetických bezpečnostných incidentov u tretej strany alebo inej osoby spolu so spôsobom a časovým obdobím ich odstránenia, e) miera, do akej tretia strana alebo iná osoba vykonáva kontrolu nad procesom výroby a dodania hardvéru alebo softvéru a riziká pre proces výroby	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
-----	--	---	----	---

	a dodania hardvéru alebo softvéru. Úrad zoznam rizikových tretích strán a iných osôb pravidelne aktualizuje, a to aspoň raz za 12 mesiacov od poslednej analýzy rizík alebo pri každej významnej zmene majúcej vplyv na identifikované riziká alebo rozsah tretích strán. (3) Výstupom analýzy rizík podľa ods. 2 je: a) vysoké riziko, pokiaľ tretia strana alebo iná osoba predstavuje vysoké riziká pre kybernetickú bezpečnosť alebo bezpečnostné záujmy Slovenskej republiky, pričom identifikované riziká nie je možné znížiť prijatím príslušných opatrení, b) stredné riziko, pokiaľ tretia strana alebo iná osoba predstavuje vysoké riziká pre kybernetickú bezpečnosť alebo bezpečnostné záujmy Slovenskej republiky, pričom identifikované riziká je možné znížiť prijatím príslušných opatrení na úroveň nízka alebo žiadna, c) nízke riziko, pokiaľ tretia strana alebo iná osoba predstavuje nízke riziká pre kybernetickú bezpečnosť alebo bezpečnostné záujmy Slovenskej republiky a identifikované riziká je možné odstrániť prijatím príslušných opatrení, alebo d) žiadne riziko, pokiaľ tretia strana alebo iná osoba nepredstavuje žiadne alebo len zanedbateľné riziká pre kybernetickú bezpečnosť alebo bezpečnostné záujmy Slovenskej republiky. (4) Ak je výstupom analýzy rizík podľa ods. 2 vysoké alebo stredné riziko, úrad zaradí tretiu stranu alebo inú osobu na zoznam podľa ods. 1 spolu s kvantifikáciou rizika, ktoré bolo dôvodom na zaradenie tretej strany alebo inej osoby na zoznam. Tretia strana alebo iná osoba nachádzajúca sa na zozname podľa ods. 1 je oprávnená predložiť úradu námietky spolu s dôkazmi preukazujúcimi neexistenciu alebo zníženie vysokého alebo stredného rizika. Úrad o námietkach tretej strany alebo inej osoby rozhodne do [doplniť] dní odo dňa ich doručenia, v odôvodnených prípadoch je úrad oprávnený túto lehotu predĺžiť, o čom je povinný tretiu stranu alebo inú osobu pred			
--	--	--	--	--

uplynutím pôvodnej lehoty na vybavenie námietok tretej strany alebo inej osoby informovať. (5) V prípade, ak je výstupom analýzy rizík podľa ods. 2: a) vysoké riziko, prevádzkovateľ základnej služby, tretia strana alebo iná osoba nesmie začať používať služby, produkty alebo procesy tejto tretej strany alebo inej osoby a v prípade existujúcich vzťahov ukončiť používanie služieb, produktov alebo procesov tejto tretej strany alebo inej osoby do [doplniť] mesiacov odo dňa zaradenia tretej strany alebo inej osoby na zoznam podľa ods. 1, b) stredné riziko, prevádzkovateľ základnej služby, tretia strana alebo iná osoba nesmie začať používať služby, produkty alebo procesy tejto tretej strany alebo inej osoby a v prípade existujúcich vzťahov s treťou stranou alebo inou osobou môže používať služby, produkty alebo procesy tejto tretej strany alebo inej osoby v rozsahu platnom ku dňu zaradenia tretej strany alebo inej osoby na zoznam podľa ods. 1. (6) V prípade, ak prevádzkovateľ základnej služby nepostupuje v súlade s ods. 5, úrad je oprávnený postupovať podľa ods. 1. Odôvodnenie: Opätovne sa jedná sa o veľmi široké oprávnenie úradu zakázať alebo obmedziť ktorémukoľvek prevádzkovateľovi základnej služby používať konkrétny produkt, proces alebo službu pod vágne koncipovanou podmienkou „ak je to potrebné na zaistenie kybernetickej bezpečnosti, alebo z dôvodov bezpečnostného záujmu Slovenskej republiky“, pod čo je možné subsumovať v zásade čokoľvek. Aj keď pôvodnou motiváciou pri koncipovaní tohto ustanovenia mohol byť záujem o implementáciu Európskeho toolboxu kybernetickej bezpečnosti 5G sietí (EU Toolbox) (nie je možné identifikovať ani z dôvodovej správy, keďže v nej je odôvodnením zavedenia takéhoto oprávnenia úradu prerozprávanie tohto nového oprávnenia inými slovami), platí, že len takýmto oprávnením úrad povinnosť			
--	--	--	--

	implementácie EU Toolboxu rozhodne nedosiahne a súčasne sa jedná o oprávnenie úradu, ktoré je vysoko rizikové, zneužiteľné, netransparentné a nepreskúmateľné. EU Toolbox obsahuje hneď tri typy opatrení, a to: strategické, technické a tzv. podporné akcie / opatrenia. Samotné strategické opatrenia sa ďalej členia v kontexte adresátov týchto opatrení, a to: právomoci regulačných orgánov, dodávatelia - tretie strany, diverzifikácia dodávateľov – tretích strán a udržateľnosť a rozmanitosť dodávateľského a hodnotového reťazca. Súčasťou strategických opatrení síce je aj časť posilnenie regulačných právomocí orgánov, konkrétne oprávnenia týchto orgánov v podobe uloženia povinností týkajúcich sa bezpečnosti poskytovateľom 5G a ex-ante (teda nie aj spätne) obmedzenie, zákaz alebo uloženie konkrétnych požiadaviek poskytovateľom 5G, avšak na základe prístupu založenom na riziku a berúc do úvahy ďalšie EU Toolboxom označené parametre. Z uvedeného teda vyplýva, že malou súčasťou v rámci strategických opatrení EU Toolboxu je aj posilnenie oprávnení regulačných orgánov, avšak uvedené oprávnenia sú podmienené rizikovým prístupom, vyhodnocovaním aj hybridných hrozieb a politických rizík a jasne danými parametrami, ktoré musí regulačný orgán vziať pri výkone týchto oprávnení do úvahy. Vychádzajú z textácie § 27 ods. 1 písm. e) je preto nutné konštatovať, že nielenže sa nejedná o náležitú implementáciu požiadaviek EU Toolboxu, ale ani náležitú implementáciu čo i len jedného opatrenia či požiadavky EU Toolboxu. Úrad sa tak zrejme mohol inšpirovať jednou z častí EU Toolboxu, avšak vyňal si z neho len časť, ktorá mu najviac vyhovuje, a to bez akýchkoľvek súvisiacich povinností úradu pri výkone tohto oprávnenia, jeho limitácie a súvisiacich pravidiel. Navyše toto oprávnenie je použiteľné nielen ex-ante, ale aj ex-post a			
--	--	--	--	--

	nielen voči poskytovateľom 5G, resp. v jazyku zákona prevádzkovateľom základných služieb prevádzkujúcich základne služby v sektore Elektronické komunikácie, podsektore siete a služby republiky pevných a mobilných elektronických komunikácií (predmet záberu EU Toolboxu), ale na všetkých prevádzkovateľov základných služieb. Nesúladi prístupu úradu vo vzťahu k tejto novozavedenej kompetencii v kontexte EU Toolboxu je preto daný hneď niekoľko krát, a to skutočnosťou, že úrad nereflektoval na všetky požiadavky EU Toolbox, vytiahol si z neho len časť, ktorá je pre neho najvyhovujúcejšia a túto bez akýchkoľvek dodatočných pravidiel, obmedzení či limitácií rozšíril na všetky sektory a podsektory a všetkých prevádzkovateľov základných služieb. EU Toolbox pritom jasne identifikuje, akým spôsobom sa má implementovať. V prvom rade sú štáty povinné vychádzať z dokumentu Spoločné európske posúdenie rizík súvisiacich s 5G sieťami a vlastného národného hodnotenia rizík, ktoré za Slovenskú republiku spracoval práve úrad. Následne sú štáty povinné tieto riziká (hybridné hrozby a v ich kontexte aj politické riziká) zohľadňovať a vyhodnotiť, či súčasné legislatívne nastavenie (požiadavky) je dostatočné a na tieto hybridné hrozby a politické riziká reflektuje. Ďalej sú štáty povinné v kontexte identifikovaných rizík (vrátane politických) a ich riadenia zvoliť príslušné opatrenia identifikované EU Toolboxom a tieto implementovať, príp. zaviesť ako príslušnú legislatívnu požiadavku. V zmysle uvedeného je teda zrejmé, že nielen novonavrhnutá kompetencia úradu, ale ani celá novela zákona nereflektuje na požiadavky EU Toolboxu, žiadnym spôsobom sa nevysporiadava s povinným rizikovým prístupom (hybridné hrozby, politické riziká) a zavádza kompetenciu, pri ktorej uplatnení úrad nie je povinný reflektovať a vyhodnocovať žiadne			
--	---	--	--	--

	riziká (nielen politické) a ktorú úrad môže používať v zásade v neobmedzenom a nekontrolovateľnom rozsahu. V tomto kontexte je nutné poukázať aj na prístupy ostatných štátov implementujúcich EU Toolbox, ktoré sú omnoho čitateľnejšie, pragmatickejšie a hlavne súladné s požiadavkami EU Toolboxu. Jedným s využívaných prístupov je vytvorenie zoznamu „rizikových dodávateľov“ podľa vopred zadaných parametrov, ktoré sú transparentné a objektívne a ktorý (zoznam) následne poskytuje rámec pre prevádzkovateľov základných služieb, akých dodávateľov nemôžu do budúcnosti využívať. Zoznam je priebežne aktualizovaný, je vytvorený priestor na „obranu“ zo strany dodávateľov na tomto zozname vyvinúť sa a preukázať, že dané hybridné hrozby a politické riziká na ich strane nie sú alebo už nie sú. Predmetný prístup je súčasne charakterizovaný zavedením presných vyhodnocovacích pravidiel a súčasne prechodných období na zosúladenie už existujúcich zmluvných vzťahov s takýmito rizikovými dodávateľmi, či už nachádzajúcimi sa v zozname stanovenom (napr.) úradom alebo vyplývajúcimi z analýzy rizík vykonanej v súlade s EU Toolbox. Takýto prístup považujeme za vhodný a správny, vyhovuje požiadavke EU Toolboxu na implementáciu zo strany štátu (teda ponechanie požiadavky na vyhodnocovanie rizikovosti na strane štátu, nie jej prenos na prevádzkovateľov základných služieb, ktorí nevedia, čo a ako majú vyhodnocovať), pričom tento prístup je auditovateľný a riziká jeho možného zneužitia sú zásadne minimalizované. V prípade doplnenia zákona o takýto systém vyhodnocovania rizikovosti dodávateľov (hybridné hrozby, politické riziká) by následne prichádzalo do úvahy aj ponechanie novonavrhnutej kompetencie úradu, ktorá má aký taký základ a opodstatnenie aj v zmysle samotného EU Toolbox, aj keď v			
--	---	--	--	--

	omnoho oklieštenejšej forme a ktorej využitie by bolo podmienené až nesúlalom prevádzkovateľa základnej služby so zoznamom rizikových dodávateľov, teda využívaním takéhoto dodávateľa aj po uplynutí príslušného prechodného obdobia na zosúladienie zmluvných vzťahov. Prístup len v podobe navrhnutého písm. e) v § 27 ods. 1 sa sám o sebe vyznačuje vysokými rizikami možného zneužitia, nevysporiadava sa s už existujúcimi (zmluvnými) vzťahmi, neobmedzuje sa len na 5G sieť, ale v zásade na akýkoľvek produkt, službu či proces. Takéto rozšírenie kompetencií jediného štátneho orgánu je nežiaduce, implementačnú povinnosť vo vzťahu k EU Toolbox plní prvoplánovo, rozhodne nedostatočne a súčasne aj v rozpore s požiadavkami EU Toolboxu. Zároveň dotknuté osoby strácajú relevantné právne nástroje na ochranu voči takémuto rozhodnutiu či postupu úradu, nakoľko postup úradu pri výkone tejto novej kompetencie je navrhnutý byť vyňatý z pôsobnosti správneho poriadku. Jediným účinným prostriedkom ochrany by teda bolo až súdne konanie. Vzhľadom k skutočnosti, že povinnosť náležitej implementácie EU Toolboxu je stále daná, upriamujeme pozornosť na našu všeobecnú pripomienku, v kontexte ktorej pri zachovaní nového oprávnenia úradu podľa § 27 ods. 1 písm. e) navrhujeme v zákone vytvoriť priestor pre zavedenie systému vyhodnocovania politických / hybridných hrozieb dodávateľov súhrnne označených ako prevádzkovatelia základných služieb, tretie strany a iné osoby predpokladaný novovytvoreným nového § 27a zákona, ktorý by vytvoril základ pre vyhodnocovanie rizikovosti, určil proces vyhodnocovania rizík a stanovil prechodné obdobia na zosúladienie povinných osôb so zisteniami (výsledkami analýzy rizík). Novovytvorený § 27a zákona by tak jednak identifikovali povinnosti vyhodnocovania rizikovosti dodávateľov (kontext hybridných			
--	--	--	--	--

	hrozieb a politických rizík), ktorú by podľa presných parametrov plnil úrad, ktorej výstupom by bol zoznam rizikových dodávateľov a ktorý by boli povinné osoby povinné reflektovať. Až v prípade nesúladu prevádzkovateľov základných služieb s predmetným zoznamom (blacklist) po uplynutí prechodného obdobia by bolo dané oprávnenie úradu zakázať využívanie takéhoto dodávateľa (súhrnne označeného ako tretia strana a iná osoba). Dôvod na zavádzanie pojmu iná osoba (popri tretej osobe, ktorá je v rámci zákona v platnom znení zadefinovaná v § 19 ods. 2 ako dodávateľ na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby) je obsiahnuť čo najširší okruh osôb, u ktorých by mohli byť vyhodnocované hybridné hrozby a politické riziká, nakoľko pojem tretia osoba tento účel v súčasnom znení zákona nenapĺňa (len dodávateľ na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby). V prípade, pokiaľ by návrh novely zákona v rámci § 19 ods. 2 zákona (viď bod 24 vlastného materiálu návrhu zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony) prešiel a došlo by k plánovanému vypusteniu definičného vymedzenia pojmu tretia strana, potom by pojem iná osoba nebol potrebný. Inou osobou sa na účely tohto návrhu rozumie napr. Úrad pre reguláciu elektronických komunikácií a poštových služieb, ktorý nespadá ako pod pojem prevádzkovateľ základnej služby, tak ani tretia strana v súčasnom znení zákona (§ 19 ods. 2). Záverom poukazujeme aj na prístup v rámci EÚ, kedy Rada podporuje závery Rady z 9. júna 2020 o formovaní digitálnej budúcnosti Európy, a ktorá vyzýva EÚ a			
--	--	--	--	--

	členské štáty, aby plne využili súbor nástrojov 5G pre kybernetickú bezpečnosť prijatý 29. januára 2020 (EU Toolbox), a najmä aby uplatnil príslušné obmedzenia na vysoko rizikových dodávateľov pre kľúčové aktíva definované ako kritické a citlivé v EU coordinated risk assessments. hodnotenia. Rada ďalej zdôrazňuje, že potenciálnych dodávateľov 5G je potrebné posudzovať na základe spoločných objektívnych kritérií. Kompletne znenie je možné nájsť tu: https://www.consilium.europa.eu/media/45930/021020-euco-final-conclusions-sk.pdf . Aj v zmysle uvedenej pozície Rady vnímame nami navrhovaný prístup za správny, EÚ predpokladaný, vyžadovaný a očakávaný. V kontexte celého návrhu nového znenia § 27a navrhujeme primerane upraviť aj ostatné časti zákona, ktoré je potrebné previazať s týmito novými povinnosťami úradu.			
AKB	V § 32 odsek 1 sa dopĺňa nové písm. i), ktoré znie: „i) metodiku posudzovania a hodnotenia kybernetickej bezpečnosti.”. Odôvodnenie: Vzhľadom k skutočnosti, že zámerom nového § 34 ods. 11 zákona umožniť prevádzkovateľom základných služieb podľa § 3 písm. k) druhý bod pre I. kategóriu sietí a informačných systémov vykonať tzv. self-assessment namiesto podstúpenia auditu kybernetickej bezpečnosti, navrhujeme, aby v záujme jednotného prístupu a predchádzania rôznorodým výkladom zo strany dotknutých prevádzkovateľov základných služieb podmienky, pravidlá a náležitosti uvedeného self-assessmentu ustanovil vykonávací právny predpis k zákonu, na ktorého vydanie by bol splnomocnený úrad.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	čl. I bod 19 „V § 17 ods. 1 znie: Ak prevádzkovateľ služby v sektore podľa prílohy č. 1 zistí, že došlo k prekročeniu identifikačných kritérií	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť

	prevádzkovej služby podľa § 18, je povinný to oznámiť úradu do 30 dní odo dňa, keď prekročenie zistil.“. Odôvodnenie: Navrhujeme návrat k pôvodnému zneniu § 17 ods. 1 zákona, a to z dôvodu, že úpravou tohto ustanovenia sa navrhuje vypustiť poznanie / vedomie prevádzkovateľa základnej služby o prekročení identifikačných kritérií prevádzkovej služby podľa § 18 ako významného predpokladu na vznik povinnosti toto prekročenie úradu oznámiť. Predkladateľ namiesto toho navrhuje vznik povinnosti viazať na prekročenie ako také a bez ohľadu na to, či o tom prevádzkovateľ služby vedel. Alternatívne si vieme predstaviť súčasné znenie § 17 ods. 1 na konci doplniť o slová „alebo mal zistiť“, čím by bola vyjadrená požiadavka na akúsi odbornú starostlivosť prevádzkovateľa služby vo vzťahu k vyhodnocovaniu prekračovania identifikačných kritérií.			návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	čl. I bod 24 „V § 19 ods. 3 navrhujeme nasledovné doplnenie: „(3) Povinnosť uzatvoriť zmluvu podľa odseku 2 neplatí, ak je tretia strana podnikom na poskytovanie elektronických komunikačných služieb alebo sietí podľa osobitného predpisu x), ku ktorému je sieť alebo informačný systém základnej služby pripojený.“ . x) Doplniť aj poznámku s odkazom na príslušné ust. zákona č. 351/2011 Z. z. Odôvodnenie: Navrhuje sa zaviesť výnimka z inak danej povinnosti uzatvoriť zmluvu podľa § 19 ods. 2 zákona pre prípad, že by tretou stranou bol prevádzkovateľ základnej služby alebo poskytovateľ digitálnej služby. Dôvodnosť takejto úpravy vníma tvorca návrhu zákona v tom, že (viď dôvodová správa): „Uvedené ustanovenie odseku 3 zároveň reaguje na možné prípady duplicity, kedy v situácii, ak by bol zmluvnou stranou samotný prevádzkovateľ	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	základnej služby alebo poskytovateľ digitálnej služby, by došlo k neprimeranej požiadavke v súvislosti so zabezpečením plnenia bezpečnostných opatrení a notifikačných povinností, ktoré sú tieto subjekty už povinné plniť podľa tohto zákona.“. S uvedeným sa rozhodne nedá súhlasiť, nakoľko nie je pravdou, že povinnosti dané prevádzkovateľom základnej služby a poskytovateľom digitálnej služby v zmysle zákona pokrývajú aj ich prípadne zmluvné vzťahy. Teda nie je pravdou, že poskytovateľ digitálnej služby vykonávajúci činnosti pre prevádzkovateľa základnej služby, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby alebo naopak, prevádzkovateľ základnej služby, využívaný poskytovateľom digitálnej služby na poskytovanie jeho digitálnej služby, sú pokrytí v zmysle im patriacich povinností vyplývajúcich zo zákona. Uvedené povinnosti sa totižto vzťahujú len na ich vlastné základné a digitálne služby, v kontexte ktorých sú povinní postupovať podľa zákona. Zákon však neobsahuje také ustanovenia, v zmysle ktorých by bolo možné založiť povinnosť v oblasti kybernetickej bezpečnosti aj voči akémukoľvek inému subjektu (vrátane prevádzkovateľa základnej služby a poskytovateľa digitálnej služby) podieľajúcemu sa na prevádzke základnej služby či poskytovaní digitálnej služby iného subjektu. Práve z tohto dôvodu vznikla potreba zavedenia inštitútu zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností, nakoľko tieto subjekty „podporujúce“ základné či digitálne služby bez ohľadu na ich status v zmysle zákona nie sú v rámci výkonu týchto činností zákonom regulovaní. V zmysle uvedeného je preto nevyhnutné povinnosť uzavretia zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností zachovať vo			
--	---	--	--	--

	vzťahu k akejkoľvek fyzickej alebo právnickej osobe, ktorá napĺňa predpoklad (vykonáva činnosť) podľa § 19 ods. 2 alebo § 22 ods. 4 zákona. Súčasne navrhujeme, aby sa jednoznačne vylúčili aj podniky poskytujúce verejné služby a siete pre prípad. Podniky elektronických komunikácií musia inak pri poskytovaní sietí a služieb implementovať primerané bezpečnostné opatrenia už na základe ustanovení §64 zák. č. 351/2011 Z. z. o elektronických komunikáciách a prenášanie ďalších individuálnych bezpečnostných opatrení na podniky, by bolo nevykonateľné a nesystémové. Verejné elektronické komunikačné služby sú totiž poskytované všetkým účastníkom v rovnakom rozsahu a za rovnakých podmienok z hľadiska dostupnosti a kvality. Nie je teda možné, aby zmluvy s účastníkmi definovali individuálne požiadavky na bezpečnosť sietí a služieb.			
AKB	čl. I bod 28 „V § 20 sa odsek 4 písm. a) vypúšťa.“. Odôvodnenie: Navrhujeme celé nové znenie § 20 sa odsek 4 písm. a) zákona vypustiť, nakoľko sa jedná o nereálnu (neexistencia takeého množstva manažérov KB v SR, resp. osôb so spôsobilosťami byť manažérom KB) a veľmi excesívnu požiadavku na všetkých prevádzkovateľov základných služieb, ktorá nemusí zodpovedať rizikám na strane toho ktorého prevádzkovateľa základných služieb, a teda ani potrebe v oblasti a) organizácie kybernetickej bezpečnosti a informačnej bezpečnosti nevyhnutne manažéra kybernetickej bezpečnosti určiť. Vieme si predstaviť presun celého navrhnutého § 20 ods. 4 písm. a) zákona do § 20 ods. 3 písm. a), kde by táto textácia bola doplnená na koniec § 2 ods. 3 písm. a) do zátvorky ako príkladný výpočet (napr.) možného opatrenia pre danú oblasť.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

AKB	čl. I bod 29: „V § 22 odsek 4 znie: (4) Ak poskytovateľ digitálnej služby využíva na poskytovanie svojej digitálnej služby tretiu stranu, je povinný uzatvoriť s treťou stranou zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby, keď poskytovateľ digitálnej služby využíva na poskytovanie svojej digitálnej služby tretiu stranu. Povinnosť uzatvoriť zmluvu podľa predchádzajúcej vety neplatí, ak je tretia strana podnikom na poskytovanie elektronických komunikačných služieb alebo sietí podľa osobitného predpisu x)“. Odôvodnenie: Nerozumieme, ani nevidíme žiaden význam v zavádzaní nového pojmu, ako dodávateľ činností, nakoľko sa stále jedná o akýkoľvek subjekt využívaný na poskytovanie digitálnej služby. Pokiaľ teda § 19 ods. 2 zákona využíva pojem tretia strana ako neurčitú množinu kohokoľvek vykonávajúceho činnosti predpokladané § 19 ods. 2, nevidíme dôvod, prečo by takáto neurčitá množina subsumujúca súčasne iných prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb nemohla byť použitá aj v § 22 ods. 4 zákona. Pokiaľ by argumentom na textáciu § 22 ods. 4 zákona mal byť článok 16 ods. 10 Smernica NIS v znení: „Bez toho, aby bol dotknutý článok 1 ods. 6, členské štáty nesmú ukladať poskytovateľom digitálnych služieb žiadne ďalšie bezpečnostné ani oznamovacie požiadavky“, takýto argument by neobstál, nakoľko znenie § 22 ods. 4 zákona ako v pôvodnom, tak aj tomto novelizovanom znení je pravdepodobne v rozpore s článkom 16 ods. 10 Smernice NIS, nakoľko poskytovateľovi digitálnej služby ukladá ďalšie povinnosti a nad rámec Smernice NIS. Dôvodnosť takéhoto postupu je daná aj tým, že v § 19 ods. 2 sa upúšťa od pôvodného definovania pojmu tretia strana ako dodávateľa na výkon činností,	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
-----	--	---	----	---

	ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby, a preto je tento pojem (tretia strana) použiteľný aj na účely § 22 ods. 4, kde sa po novom hovorí o dodávateľovi na výkon činností, ktoré priamo súvisia s poskytovaním digitálnej služby. Vzhľadom na neexistenciu relevantného dôvodu na zavedenie nového pojmu dodávateľ činností a v záujme predchádzania vnášaniu zbytočnej zmätočnosti do zákona navrhujeme tento pojem vypustiť a ponechať len pojem tretia strana ako pojem všeobecný, zahŕňajúci neurčitú množinu osôb vykonávajúcich činnosti či už podľa § 19 ods. 2 alebo § 22 ods. 4 zákona. Súčasne sa jedná o zosúladenie povinnosti uzatvoriť zmluvu s treťou stranou v rovnakom režime ako je to u poskytovateľa základnej služby podľa novo navrhovaného znenia §19 ods. 3.			
AKB	čl. I bod 32 „V § 27 odsek 1 písm. e) sa vypúšťa.“. Odôvodnenie: Dôvodom vypustenia je presun a komplexnejšia úprava v inom ustanovení zákona (novovytvorený § 27a) z dôvodu prehľadnosti a logickej súvislosti. V tomto kontexte navrhujeme primerane upraviť aj ostatné časti zákona, ktoré boli s touto novou kompetenciou úradu spojené (napr. správne delikty a pod.).	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	čl. I bod 4 a 5: „V § 3 sa písm. a) a b) vypúšťajú.“. Odôvodnenie: Ustanovenie § 3 zákona sa dopĺňa novými definíciami v zmysle písm. a) (informačný systém) a b) (elektronická komunikačná sieť), ktorými dochádza k oddeleniu pôvodnej siete a informačného systému v rámci jedinej definície. Novo navrhovaný súbor informačný systém a elektronická	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a

	komunikačná sieť však čo do rozsahu nie je totožný s pojmom sieť a informačný systém v zmysle súčasného znenia § 3 písm. a) zákona, pričom dochádza k zúženiu prvkov kybernetického priestoru, ktoré sú súčasťou definície siete a informačného systému podľa súčasného znenia zákona, avšak už nie súčasťou nového definičného vymedzenia siete a informačného systému, ktoré má tvoriť samostatne zadefinovaný informačný systém a elektronická komunikačná sieť. Súčasne platí, že pojem sieť a informačný systém vyplýva zo Smernice EP a Rady (EÚ) č. 2016/1148 (Smernica NIS), pričom jeho zúženie čo do prvkov / komponentov kybernetického priestoru (napr. absencia aplikačnej vrstvy a i.) je súčasne v rozpore so Smernicou NIS a požiadavkou jej náležitej transpozície. Z uvedeného dôvodu trváme na vypustení nových definícií a ponechaní pôvodného definičného vymedzenia siete a informačného systému subsumujúceho všetky komponenty kybernetického priestoru.			odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	čl. I bod 6 „V § 3 sa písm. h) sa na konci vypúšťajú tieto slová: „činnosti potrebné na ochranu sietí a informačných systémov, užívateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami,“. Odôvodnenie: Navrhované znenie už je súčasťou pôvodného definičného vymedzenia pojmu kybernetická bezpečnosť, nakoľko je logické a zrejmé, že definíciou predpokladaný stav je dosahovaný aj činnosťami potrebnými na ochranu sietí a informačných systémov, užívateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami. Súčasne nepovažujeme za vhodné do inak statickej definície (stav) zanášať dynamické prvky, ako činnosti. Navrhujeme ponechať	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	pôvodnú definíciu kybernetickej bezpečnosti.			
AKB	čl. I bod 7: „V § 3 sa písm. q) až t) vypúšťajú.“. Odôvodnenie: Ustanovenie § 3 zákona sa dopĺňa novými definíciami, z ktorých definície pod písm. q) až t) tvoria definície skopírované z nariadenia R a EP (EÚ) č. 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/ 2013 (ďalej len „akt o kybernetickej bezpečnosti“). Vzhľadom na priamu aplikovateľnosť nariadenia a zákaz bránenia tejto priamej aplikovateľnosti preberaním znenia nariadenia do vnútroštátnych predpisov navrhujeme definície v bodoch q) až t) vypustiť a nahradiť ich odkazmi na vyššie citovaný akt o kybernetickej bezpečnosti (čl. 2 body 9 – 14 aktu o kybernetickej bezpečnosti).	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	čl. I bod 7 „V § 3 sa písm. u) vypúšťá.“. Odôvodnenie: Nie je zrejmé, čím sa predkladateľ pri tvorbe definičného vymedzenia pojmu audit inšpiroval, je však potrebné poukázať na skutočnosť, že definičné vymedzenie pojmu audit len z pohľadu zamýšľaného výsledku nie je presné a správne. Na vymedzenie pojmu audit odporúčame použiť definíciu z technickej normalizácie (napr. ISO/IEC 17000) a toto vymedzenie zaniest' do § 29 zákona.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	čl. I bod 44 „V § 32 odsek 1 sa v písm. f) vypúšťá „podrobnosti o akreditácii certifikačných orgánov certifikujúcich audítorov kybernetickej	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť

	bezpečnosti“. Odôvodnenie: Podrobnosti o akreditácii certifikačných orgánov certifikujúcich audítorov kybernetickej bezpečnosti stanovuje v zmysle Čl. 2 bod 13 nariadenia Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13. 8. 2008) Slovenská národná akreditačná služba, nie úrad. Z uvedeného dôvodu je potrebné oprávnenie patriace Slovenskej národnej akreditačnej službe z „pôsobnosti / oprávnenia“ úradu vypustiť.			návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	čl. I bod 46 „V § 32 odsek 2 sa slová „so súhlasom úradu“ nahrádzajú „v spolupráci s úradom“. Odôvodnenie: Rozhodne nesúhlasíme s predstavou predkladateľa o akomsi schvaľovaní návrhov všeobecne záväzných právnych predpisov iných štátnych orgánov pre oblasť kybernetickej bezpečnosti v rámci vlastného sektora / podsektora. Pôvodný zámer zákona bol umožniť iným ústredným orgánom vykonávajúcim pôsobnosť v oblasti kybernetickej bezpečnosti v zmysle § 4 písm. b) zákona v spolupráci s úradom vypracovať osobitný predpis upresňujúci požiadavky zákona (špecifikujúci sektorové bezpečnostné opatrenia pre ten ktorý sektor) nad rámec všeobecných požiadaviek daných osobitným predpisom v zmysle § 32 ods. 1 písm. c) zákona, teda dnešnej Vyhlášky č. 362/2018 Z.z. Zámerom tejto pripomienky teda nie je vypustiť „vplyv“ úradu na znení príslušného osobitného predpisu pre ten ktorý sektor v zmysle § 32 ods. 2 zákona, ale ponechanie expertného „dohľadu“ a expertných potrieb ústredného orgánu v zmysle § 4 písm. b) zákona, ktorý najlepšie pozná bezpečnostné požiadavky a potreby v rámci	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	toho ktorého sektoru. V zmysle uvedeného navrhujeme ponechanie pôvodného znenia § 32 ods. 2 zákona namiesto predstavy úradu schvaľovať (odsúhlasovať = veto) znenie všeobecne záväzných právnych predpisov mimo odbornej a legislatívnej pôsobnosti úradu.			
AKB	čl. I bod 47 „V § 33 odsek 1 znie: Na konanie úradu podľa § 13 ods. 7, § 16 ods. 2 a 3 a § 27a ods. 4 sa nevzťahuje správny poriadok.“. Odôvodnenie: Úrad novelou zákona plánoval rozšíriť vylúčenú pôsobnosť správneho poriadku aj na ďalšie typy „konaní“ úradu, a to na novozavedené kompetencie úradu podľa § 24 ods. 7, 27 ods. 1 písm. e) a 27a zákona. Ako je uvedené vyššie, so zavádzaním uvedených kompetencií úradu v ním navrhovanej forme a obsahu nesúhlasíme, a preto nie je dôvod na rozširovanie § 32 ods. 1 zákona o ďalšie konania vyňaté z pôsobnosti správneho poriadku. Pokiaľ sa jedná o vylúčenie pôsobnosti správneho poriadku pri konaniach a činnostiach úradu podľa § 17 ods. 6, § 21 ods. 4 a § 27, ani pri nich nesúhlasíme s vylúčením pôsobnosti správneho poriadku. Jedná sa totižto o konania a činnosti úradu, ktorých výsledkom je značný zásah do práv a právom chránených záujmov fyzických a právnických osôb, či už v podobe ich zaradenia do registra prevádzkovateľov základných služieb, poskytovateľov digitálnych služieb alebo v podobe široko koncipovaných oprávnení úradu uložiť povinnosť riešiť kybernetický bezpečnostný incident, vykonať reaktívne opatrenie alebo navrhnuť ochranné opatrenie. Absencia pôsobnosti správneho poriadku pri postupoch úradu vo vyššie naznačených konaniach úradu umožňuje bez akýchkoľvek obmedzení konať a svojim konaním zasahovať do práv a právom chránených záujmov osôb, ktoré nedisponujú žiadnym účinným	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	prostriedkom ochrany a ktoré z titulu absencie pôsobnosti správneho poriadku nemajú žiadne procesné práva, ktoré by inak mohli pri rozhodovaní úradu ako správneho orgánu uplatňovať. Dotknuté subjekty majú teda jedinou možnosť, ako sa ochrany svojich práv a právom chránených záujmov domáhať, a to prostredníctvom súdu. Uvedené nástroj je však neadresný a neefektívny, nakoľko v čase podania žaloby na súd už bude príslušné „rozhodnutie“ úradu podľa § 17 ods. 6, § 21 ods. 4 a § 27 dávno vykonateľné a väčšinou aj vykonané. Prípadný ex post výrok súdu o protiprávnom či nezákonnom rozhodnutí či postupe úradu preto nemožno považovať za účinný prostriedok ochrany, nakoľko v danom čase (mesiace až roky po uložení povinnosti zo strany úradu vrátane možných sankčných postihov zo strany úradu za nesplnenie povinnosti) už nie je efektívny a uložená povinnosť je zo strany povinného subjektu dávno splnená.			
AKB	čl. I bod 10 „V § 5 sa ods. 1 písm. ac) dopĺňa na konci nasledovne: „v súlade s § 9.“. Odôvodnenie: Vzniká podozrenie, že úrad sa svojim vynechaním v rámci § 4 písm. b), na ktoré je naviazaný § 9 zákona, snaží vyhnúť plneniu povinností, ktoré z § 9 každému ústrednému orgánu patria a namiesto toho si „postavenie ústredného orgánu“ bez kontextu na § 9 uchováva v rámci textácie „plní úlohy ústredného orgánu podľa prílohy č. 1“. Pre vylúčenie akejkoľvek vyššie uvedených pochybnosti preto navrhuje toto doplnenie, nakoľko máme za to, že úrad ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť by ako prvý mal plniť požiadavky zákona a zodpovedať za zabezpečenie kybernetickej bezpečnosti v rozsahu § 9 ods. 1 zákona.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

AKB	čl. I bod 10 „V § 5 sa ods. 1 písm. ad) sa slová „zoznam certifikačných orgánov audítorov kybernetickej bezpečnosti“ nahrádzajú slovami „zoznam orgánov vykonávajúcich certifikáciu osôb v kybernetickej bezpečnosti“. Odôvodnenie: Nedáva zmysel v zmysle textácie „zoznam certifikačných orgánov audítorov kybernetickej bezpečnosti“ vopred obmedzovať objekty posudzovania len na audítorov kybernetickej bezpečnosti, nakoľko v budúcnosti môže vzniknúť potreba certifikácie aj iných osôb (napr. manažér kybernetickej bezpečnosti). Z uvedeného dôvodu navrhuje pojem audítor nahradiť pojmom osoby v kybernetickej bezpečnosti.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	čl. I bod 12 „V § 5a sa ods. 3 znie: Orgán posudzovania zhody10ad), ktorý nie je vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti, certifikuje produkty, služby a procesy podľa osobitného predpisu10ah) v rámci systému certifikácie kybernetickej bezpečnosti.“. Odôvodnenie: Pojmy certifikačný orgán a orgán posudzovania zhody sú totožné, a preto je v záujme prehľadnosti potrebné pojmy zosúladiť. Vzhľadom na to, že nariadenie (EÚ) č. 2019/881 používa pojem (vnútroštátny) orgán posudzovania zhody, navrhujeme, aby bolo rovnaké názvoslovie použité aj v novom § 5a ods. 3 zákona, a teda certifikačný orgán bol nahradený pojmom orgán posudzovania zhody. Pokiaľ sa jedná o vypustenie časti „orgánu posudzovania zhody podľa osobitného predpisu,10af“, kde odkaz 10af) znel Čl. 60 ods. 2 a príloha nariadenia (EÚ) č. 2019/881, s týmto návrhom nie je možné súhlasiť, nakoľko uvedeným orgánom posudzovania zhody by bol opätovne, ako v novom § 5a ods. 2 úrad, resp. niektorá z jeho organizačných jednotiek. Nakoľko	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	§ 5a ods. 3 má ambíciu upraviť, kto iný ako vnútroštátny orgán posudzovania zhody, teda úrad, je oprávnený certifikovať produkty, služby a procesy, nesúhlasíme so zúžením len na orgán úradu rovnako ako nesúhlasíme so zúžením len na verejné subjekty, nakoľko napr. certifikáciu na stupeň dôveryhodnosti základný a pokročilý môžu v zmysle nariadenia (EÚ) č. 2019/881 vykonávať aj súkromné subjekty.			
AKB	čl. I bod 12 „V § 5a sa v odkaze 10ad) slová „Napríklad STN EN ISO/IEC 17065 Posudzovanie zhody. Požiadavky na orgány vykonávajúce certifikáciu výrobkov, procesov a služieb (ISO/IEC 17065) (01 5256)“ nahrádzajú slovami „Napríklad STN EN ISO/IEC 17000 Posudzovanie zhody. Slovník a všeobecné zásady (ISO/IEC 17000: 2004).“. Odôvodnenie: V záujme zjednotenia pojmov a zamedzeniu používania synonym ako certifikačný orgán a orgán posudzovania zhody je potrebné v záujme nahradenia pojmu certifikačný orgán v rámci §5a ods. 3 pojmom orgán posudzovania zhody (viď pripomienku č. 9) odkaz na STN EN ISO/IEC 17065 nahradiť odkazom na STN EN ISO/IEC 17000 Posudzovanie zhody - Slovník a všeobecné zásady, ktorý pojem orgán posudzovania zhody definuje.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	čl. I bod 21 „Všeobecná pripomienka.“. Navrhujeme uvedené preformulovať. Slovo výmaz nepovažujeme za adekvátny. Navrhujeme použiť slovné spojenie „vyradenie základnej služby zo zoznamu základných služieb a jej prevádzkovateľa z registra prevádzkovateľov základných služieb“.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej

				akceptovateľnej miere pripomienky všetkých subjektov.
AKB	čl. I bod 22 „Všeobecná pripomienka.“. Navrhujeme znenie § 18 ods. 1 zákona doplniť o ďalšiu vetu v nasledovnom znení: „V prípade, ak pre niektorý zo sektorov nie sú určené žiadne dopadové kritériá alebo špecifické sektorové kritériá, tieto sa u prevádzkovateľa služby na účely § 17 ods. 1 v takomto sektore považujú za prekročené.“. Jedná sa o precizovanie obsahu povinnosti v zmysle § 17 ods. 1 zákona, kedy niektorí prevádzkovatelia služieb absenciu určenia špecifických sektorových kritérií pre niektorý zo sektorov vykladali ako nemožnosť prekročenia identifikačných kritérií podľa § 17 ods. 1 zákona. V zmysle uvedeného doplnenia tak bude platiť, že absencia dopadových alebo špecifických sektorových kritérií bude znamenať „ich“ automatické prekročenie.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	čl. I bod 12 „Všeobecná pripomienka.“. Ustanovenie § 5a odsek 1 poveruje úrad plnením úloh podľa osobitného predpisu. V poznámke pod čiarou je odkaz na čl. 58 ods. 6 až 9 aktu o kybernetickej bezpečnosti (nariadenie (EÚ) č. 2019/881). Avšak z aktu o kybernetickej bezpečnosti vyplýva pre členský štát viacero úloh (napríklad z čl. 23 nominovať člena do siete národných styčných úradníkov). Máme to chápať tak, že tieto úlohy nebude plniť úrad? Kto potom? Obdobne v čl. 58 ods. 2 povinnosť členského štátu notifikovať Komisii určenie vnútroštátneho certifikačného orgánu, čl. 60 oznamovacie povinnosti - kto túto povinnosť splní? Z pohľadu implementácie aktu o kybernetickej bezpečnosti upozorňujeme, že z návrhu nie je zrejmé, kto bude tým vnútroštátnym orgánom pre certifikáciu	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	kybernetickej bezpečnosti zodpovedným za dozor respektíve dohľad nad touto činnosťou v členskom štáte (čl. 58 ods. 1). V návrhu v § 5 ods. 1 je totiž uvedené, že úrad plní úlohy podľa osobitného predpisu, pričom v poznámke pod čiarou odkazuje iba na čl. 58 ods. 6 až 9 aktu o kybernetickej bezpečnosti. Uvedené je dôležité upraviť v zákone nielen z dôvodu náležitosti a úplnej implementácie aktu o kybernetickej bezpečnosti, ale taktiež pre posúdenie, či sú dodržané aj iné požiadavky aktu o kybernetickej bezpečnosti, napr. požiadavka oddelenosti činností podľa článku 56 ods. 5 písm. a) a článku 56 ods. 6 od činností dohľadu podľa čl. 58. Vzhľadom na skutočnosť, že nie je zabezpečené plnenie všetkých úloh z aktu o kybernetickej bezpečnosti, v podmienkach Slovenskej republiky nemožno dosiahnutie zhody s Európskym právom chápať ako úplné, aj keď ju predkladateľ ako úplnú uvádza v doložke zlučiteľnosti. Akt o kybernetickej bezpečnosti je potrebné doplniť do prílohy č. 3 návrhu zákona a adekvátne k tomu zmeniť názov prílohy.			
AKB	čl. III bod 5 „Všeobecná pripomienka“ Tým, že sa zruší splnomocňovacie ustanovenie na prijatie osobitného predpisu sa ešte automaticky nezruší platná vyhláška č. 179/2020 Z.z., aj keď zostane bez právneho základu. V prípade ak je cieľom predkladateľa zrušiť túto existujúcu vyhlášku, navrhujeme do čl. II. návrhu doplniť zrušovacie ustanovenie s textom: „Zrušuje sa vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.“.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AKB	Všeobecná pripomienka „EU Toolbox“ Slovenská republika je spolu s ďalšími európskymi štátmi adresátom	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety,

povinnosti náležitej implementácie požiadaviek Európskeho toolboxu kybernetickej bezpečnosti 5G sietí („EU Toolbox“) do vnútroštátnej právnej úpravy. Implementácia EU Toolboxu nie je oprávnením, ale povinnosťou štátov vrátane Slovenskej republiky. Všetky aktivity vo vzťahu ku koncipovaniu EU Toolboxu vrátane vypracovania vstupu do jednotného dokumentu Spoločné európske posúdenie rizík súvisiacich s 5G sieťami za Slovenskú republiku uskutočňoval Národný bezpečnostný úrad („úrad“). Súčasne platí, že vzhľadom na povahu a obsah EU Toolboxu a ním identifikovaných opatrení by jeho požiadavky mali byť implementované práve do zákona ako jediného právneho predpisu svojho druhu, ktorý vo všeobecnej rovine a celoplošne naprieč všetkými sektormi a podsektormi ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti, a teda aj požiadavky na zaistenie bezpečnosti pre sektor Elektronické komunikácie, podsektor siete a služby republiky pevných a mobilných elektronických komunikácií, kam patrí aj 5G. Bolo by veľmi nelogické a nevhodné, pokiaľ by sa úrad jednak ako gestor zákona a jednak ako subjekt, ktorý ako jediný za Slovenskú republiku od počiatku participoval na koncipovaní EU Toolboxu, vyhýbal jeho implementácii. Navyše v kontexte, že to bol Národný bezpečnostný úrad, ktorý ako jediný za Slovenskú republiku vyhodnocoval riziká spojené s využívaním 5G sietí. Účelom EU Toolboxu je najmä stanovenie spoločného súboru opatrení, ktoré sú schopné zmierniť hlavné riziká kybernetickej bezpečnosti sietí 5G, ktoré boli identifikované v rámci dokumentu Spoločné európske posúdenie rizík súvisiacich s 5G sieťami, kde riziká súvisiace s 5G sieťami, ako bolo uvedené skôr, za Slovenskú republiku posudzoval úrad. EU Toolbox identifikuje opatrenia, ktoré sú štáty vrátane Slovenskej republiky povinné implementovať do		postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
--	--	--

	svojich vnútroštátnych poriadkov, pričom tieto opatrenia sa delia na strategické a technické a tzv. podporné činnosti. Práve tzv. strategické opatrenia sú oblasťou, na ktorú zákon žiadnym spôsobom nereflektuje (príp. len veľmi okrajovo a účelovo, vyťahujúc si z nich oprávnenia bez akejkoľvek kontroly), nakoľko mu nie sú známe pojmy ako politické riziká, riziká spojené s vplyvmi tretích štátov na dodávateľov, hybridné hrozby a pod. a „obmedzuje“ sa na hrozby, zraniteľnosti a riziká technického či technologického charakteru. V nadväznosti na uvedené považujeme za vysoko prioritné a dôležité zákon doplniť o nový rozmer tzv. hybridných hrozieb, politických rizík, ktoré by prevádzkovatelia základných služieb pri vyhodnocovaní rizikovosti využívania konkrétného produktu, služby či procesu boli povinní zohľadňovať. Uvedený model nie je žiadnym výmyslom, ale prístupom iných štátov už implementujúcich EU Toolbox, ako napríklad Poľsko alebo Francúzsko. Uvedeným prístupom by bolo možné upustiť od zavádzania prvoplánových kompetencií na strane úradu, ktoré síce vo forme ako „zakázať využívať konkrétny produkt, službu, proces“ môžu veľmi marginálne naplniť implementačnú úlohu vo vzťahu k niektorým častiam EU Toolbox, vyznačujú sa však vysokou rizikovosťou, zneužívateľnosťou, netransparentnosťou, nepredvídateľnosťou a zároveň sťaženou až žiadnou preskúmateľnosťou. Sme toho názoru, že koncept hybridných hrozieb a politických rizík by mal byť zanesený do zákona, a to do samostatného paragrafu vzhľadom na špecifickosť a unikátnosť zanášanej právnej úpravy v kontexte EU Toolbox. Vzhľadom na dostupné informácie, že v príprave je aj sektorová vyhláška vydaná podľa § 32 ods. 2 zákona o kybernetickej bezpečnosti pre sektor Elektronické komunikácie a v ktorej by bolo vysoko žiaduce			
--	--	--	--	--

	rozviesť prípadné podrobnosti o procese vyhodnocovania rizík / rizikovosti na strane dodávateľov. Potreba a nevyhnutnosť implementácie EU Toolboxu do právneho poriadku Slovenskej republiky je podčiarknutá aj závermi, ktoré prijala Európska rada na svojom mimoriadnom zasadnutí 1. a 2. októbra 2020 : „11. Európska rada schvaľuje závery Rady z 9. júna 2020 o formovaní digitálnej budúcnosti Európy. Vyzýva EÚ a členské štáty, aby v plnej miere využívali súbor nástrojov EÚ pre kybernetickú bezpečnosť 5G prijatý 29. januára 2020, a najmä aby uplatňovali príslušné obmedzenia týkajúce sa vysokorizikových dodávateľov v prípade kľúčových aktív, ktoré sú v koordinovaných posúdeniach rizík EÚ vymedzené ako kritické a citlivé. Európska rada zdôrazňuje, že potenciálni dodávatelia technológií 5G sa musia posudzovať na základe spoločných objektívnych kritérií.“			
AmCham Slovakia	Bod 10 Bod 10. Navrhujeme upraviť § 5 a odsek 1 písm. y) nasledovne: „y) v rámci riešenia opatrení o blokovani podľa osobitných predpisov10aa) zabezpečuje vykonanie rozhodnutia o blokovani škodlivého obsahu alebo škodlivej aktivity,“ Odôvodnenie: Rozhodnutie o blokovani môže byť len na základe príkazu súdu podľa osobitného predpisu, čo poskytuje dostatočnú právnu istotu, že ide o blokovanie relevantné a odôvodnené.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AmCham Slovakia	Bod 24 Bod 24. V § 19 ods. 3 navrhujeme nasledovné doplnenie: „(3) Povinnosť uzatvoriť zmluvu podľa odseku 2 neplatí, ak je tretia strana prevádzkovateľom základnej služby alebo poskytovateľom digitálnej služby alebo podnikom na poskytovanie elektronických	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text

	komunikačných služieb alebo sietí podľa osobitného predpisu x).“. x) Doplniť aj poznámku s odkazom na príslušné ust. zákona č. 351/2011 Z. z. Odôvodnenie: Navrhujeme aby sa jednoznačne vylúčili aj podniky poskytujúce verejné služby a siete pre prípad, ak by nespádali do skupiny PZS resp. poskytovateľov digitálnych služieb. Podniky elektronických komunikácií musia inak pri poskytovaní sietí a služieb implementovať primerané bezpečnostné opatrenia už na základe ustanovení §64 zák. č. 351/2011 Z. z. o elektronických komunikáciách a prenášanie ďalších individuálnych bezpečnostných opatrení na podniky, by bolo nevykonateľné a nesystémové. Verejné elektronické komunikačné služby sú totiž poskytované všetkým účastníkom v rovnakom rozsahu a za rovnakých podmienok z hľadiska dostupnosti a kvality. Nie je teda možné, aby zmluvy s účastníkmi definovali individuálne požiadavky na bezpečnosť sietí a služieb.			tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AmCham Slovakia	Bod 29 Bod 29. navrhujeme upraviť nasledovne: V § 22 odseky 4 a 5 znejú: „(4) Ak poskytovateľ digitálnej služby využíva tretiu stranu na výkon činností, ktoré priamo súvisia s poskytovaním digitálnej služby, je povinný uzatvoriť s treťou stranou na výkon týchto činností zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby, keď poskytovateľ digitálnej služby využíva na poskytovanie svojej digitálnej služby tretiu stranu. Povinnosť uzatvoriť zmluvu podľa predchádzajúcej vety neplatí, ak je tretia strana prevádzkovateľom základnej služby poskytovateľom digitálnej služby, alebo podnikom na poskytovanie elektronických komunikačných služieb alebo sietí podľa osobitného predpisu x). (5) Ak by sa plnenie zmluvy podľa	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	odseku 4 stalo nemožným, poskytovateľ digitálnej služby o hlásenom kybernetickom bezpečnostnom incidente v nevyhnutnom rozsahu informuje tretiu stranu, pokiaľ úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.“. Odôvodnenie: Uvedené ustanovenie podľa nášho názoru nie je zrozumiteľné, ani riadne vykonateľné – prečo sa má uzatvárať táto nadbytočná vzájomná zmluva, keď prevádzkovateľovi základnej služby aj poskytovateľovi digitálnej služby vyplýva notifikačná povinnosť aj ostatné povinnosti priamo z tohto zákona a navyše prevádzkovateľ základnej služby ju nemá uzatvárať v opačnom vzťahu už podľa bodu 24 samotného tohto návrhu. V praxi to znamená, že každý poskytovateľ digitálnej služby môže vyžadovať od prevádzkovateľa základnej služby zmluvu s inými podmienkami, keďže zmluva je dvojstranný právny akt, pričom prevádzkovateľ poskytuje základnú službu všetkým rovnako, a takáto zákonná povinnosť má zásadný dopad vo všetkých aspektoch vzájomného vzťahu týchto subjektov a narušuje riadne poskytovanie základnej služby za riadnych podmienok. Uvedené znenie je nutné zosúladiť s princípmi obdobného znenia v § 19, pričom totožný problém je už v aktuálne platnom znení. Zosúladenie povinnosti uzatvoriť zmluvu s treťou stranou v rovnakom režime ako je to u poskytovateľa základnej služby podľa novo navrhovaného znenie §19 ods. 3.			
AmCham Slovakia	Bod 31 Bod 31. Navrhujeme upraviť nový § 24 ods. 7 nasledovne: „(7) Na hlásenie kybernetických bezpečnostných incidentov alebo na zaistenie kybernetickej bezpečnosti po nahlásení bezpečnostného incidentu je prevádzkovateľ základnej služby určený rozhodnutím úradu, ktorý je orgánom štátnej správy povinný zasielať	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a

automatizovaným spôsobom a v rozsahu ustanovenom týmto zákonom určené systémové informácie zo sietí a informačných systémov. Uloženie povinnosti nemôže byť v rozpore s inými právnymi predpismi, najmä s ohľadom na oblasť ochrany súkromia a povinnosti mlčanlivosti vyplývajúcimi z platnej právnej úpravy.“. Odôvodnenie: Uvedené ustanovenie ide podľa nášho názoru úplne nad rámec ohlasovania incidentov a snaží sa neregulovaným spôsobom získavať neznámy rozsah informácií, ktoré môžu byť aj predmetom inej zákonnej ochrany a núti prevádzkovateľa programovo vytvárať nejaké aplikačné riešenia k tejto osobitnej oznamovacej povinnosti, ku ktorým nemusí mať ani prostriedky, ani schopnosť ich urobiť, pričom úrad si môže svojvoľne určiť ľubovoľného prevádzkovateľa základnej služby. Navrhované znenie javí rovnaký problém nesúladu s Ústavou a nezaistenia právnej istoty ako body 32 a 33. Celé ustanovenie je nutné vypustiť, k osobitným spôsobom ohlasovania je postačujúci § 24 odsek 6. Navrhujeme aby boli jasne vopred určené subjekty, ktoré budú podliehať takejto povinnosti s odvolaním sa na príslušné sektory v prílohe I a bol vylúčený súkromný sektor. Uloženie takejto povinnosti pre podnikateľské subjekty by bolo neprimerane zaťažujúce a reálne nevykonateľné vzhľadom na požiadavku automatizovaného spôsobu. Nie je jasné ani aké systémové informácie by mali byť zasielané a mali by byť jasne vymedzené v ZoKB. Zavádzať uvedené ako povinnosť môže spôsobiť napríklad konflikt s ustanovením § 63 Telekomunikačné tajomstvo Zákona 351/2011 o elektronických komunikáciách, telekomunikačné podniky nemôžu konať nad rámec zákona č. 351/2011 Z.z. najmä pokiaľ ide o spracúvanie a poskytovanie informácií o prevádzke		odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
--	--	--

	koncových užívateľov.			
AmCham Slovakia	Bod 36 Bod 36. navrhujeme preformulovať nasledovne: „4) Právnická osoba zabezpečuje audit kybernetickej bezpečnosti prostredníctvom certifikovaného audítora kybernetickej bezpečnosti alebo certifikovaných audítorov kybernetickej bezpečnosti. Zabezpečovanie auditu kybernetickej bezpečnosti je podnikaním podľa osobitného predpisu 31d), ak nejde o audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby alebo poskytovateľa digitálnej služby vykonávaný vlastným zamestnancom, alebo zamestnancom iného podniku v rámci skupiny podnikov. Ak audit kybernetickej bezpečnosti realizuje audítor kybernetickej bezpečnosti prostredníctvom právnickej osoby, zodpovedá za škodu spôsobenú pri výkone auditu kybernetickej bezpečnosti táto právnická osoba.“ Odôvodnenie: Spresnenie; aby spoločnosť, ktorá si bude vykonávať vlastný audit prostredníctvom svojho zamestnanca, alebo zamestnanca iného podniku – ovládanej alebo ovládajúcej osoby, nemusela ohlasovať výkon auditu kyber. bezpečnosti ako novú podnikateľskú činnosť.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AmCham Slovakia	Bod 47 Bod 47 navrhujeme vypustiť a ponechať súčasné znenie § 33 ods. 1 ZoKB. Odôvodnenie: Ide o rozhodnutia, ktorými sa zasahuje do zásadných práv, resp. určujú aj prevádzkovateľa základných služieb a vzhľadom na dôsledky by mali byť zachované aj všetky práva na prípadné opravné prostriedky. V zmysle Ústavy SR čl. 46 ods. 2, základné práva a slobody nemožno vyňať ani spod preskúmateľnosti nezávislým súdom.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky

				všetkých subjektov.
AmCham Slovakia	Bod 24 Odsek 2 navrhujeme doplniť, nakoľko zavádza povinnosť uzatvoriť zmluvu v súvislosti s akýmikoľvek sieťami a informačnými systémami prevádzkovateľa základnej služby a nie iba tými, ktoré sú nutné pre poskytovanie základnej služby. Uvedený problém sa nachádza už aj v pôvodnom znení, čím presahuje rámec pôvodného zámeru a snaží sa regulovať aktíva, ktoré nie sú predmetom tohto zákona.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AmCham Slovakia	Bod 45 Písmeno h) požadujeme vypustiť – požiadavky s tak závažným dopadom je v prípade ponechania ustanovenia o blokovani potrebné zadefinovať priamo v zákone. Nejasnosť navrhovaného § 27a neodstránia ani pravidlá pre blokovanie, ktorý by mali byť vydané úradom, nakoľko dané pravidlá si opäť stanoví, vydá a môže kedykoľvek zmeniť sám úrad. Sme presvedčení, že bližšie vymedzenie nejasných a neurčitých pojmov použitých v návrhu, ktoré umožňujú úradu zasiahnuť do viacerých ústavných práv jednotlivcov nemôžu byť vykonané formou podzákonného právneho predpisu ale musí byť súčasťou predpisu s právnou silou zákona. V opačnom prípade by došlo k zjavnému porušeniu ústavných garancií upravujúcich striktné podmienky, za splnenia ktorých môžu byť základné práva obmedzené napríklad rozhodnutím štátneho orgánu (napríklad čl. 13 Ústavy SR a čl. 26 ods. 4 Ústavy SR).	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AmCham	K analýze podnikateľského prostredia Popísaná analýza je podľa nášho názoru nepresná a skutkovo	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety,

Slovakia	nesprávna – v prvom rade sa dotýka akéhokoľvek prevádzkovateľa základnej služby a nie iba podnikov s viac ako 250 zamestnancami a za druhé má návrh vážny negatívny vplyv, ktorý je tu skonštatovaný ako „nepredpokladá priamy vplyv na podnikateľské prostredie“. Negatívny vplyv vyplýva najmä z nutnosti - implementovať funkčné automatizované zasielanie údajov podľa bodu 31, čo môže znamenať programátorský zásah do neznámeho množstva systémov, vrátane možnosti ohrozenia bezpečnosti keď daný systém nie je stavaný na akýkoľvek takýto export a dotknuté údaje podliehajú rôznym typom právnej ochrany, - prestať používať ľubovoľnú technológiu resp. produkt podľa bodu 32, čo môže znamenať nutnosť úplnej výmeny hardvéru alebo softvéru alebo dokonca znefunkčnenie služieb, ku ktorým sa viažu právne aj legislatívne záväzky a sankcie, - vyčleniť finančné prostriedky na zamestnanie bezpečnostného manažéra podľa bodu 28 a - vykonávať neznáme ľubovoľné opatrenia na blokovanie podľa bodu 33, ktoré môže úrad uložiť, a to technického, organizačného či akéhokoľvek iného charakteru bez ohľadu na možnosti a zdroje dotknutého subjektu (predpoklad, že pri blokovaní sa nepredpokladajú finančné dopady je v tomto tiež nesprávny, pretože minimálne procesno-technická implementácia má vysokú pravdepodobnosť osobitných výdajov), a vo všetkých prípadoch bez možnosti primerane reagovať alebo namietat' voči vecne neprimeraným rozhodnutiam, resp. dôjsť k racionálnemu riešeniu.			postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AmCham Slovakia	bod 3 a 51 v čl. I a článok III Požadujeme vypustiť bod 3 a 51 v čl. I a článok III z návrhu. Súčasne navrhujeme, aby bol sektor Elektronických komunikácií vypustený ako celok z prílohy 1 zákona č. 69/2018 Z.z.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k

	Odôvodnenie: Ponechanie resp. rozšírenie zoznamu prevádzkovateľov základných služieb v sektore Elektronické komunikácie nie je v súlade so smernicou NIS, ktorá v ustanovení článku 1 ods. 3 smernice č. 2016/1148/ES výslovne uvádza, že „bezpečnostné a oznamovacie požiadavky stanovené v tejto smernici sa nevzťahujú na podniky, ktoré podliehajú požiadavkám článkov 13a a 13b smernice 2002/21/ES“. Zo strany Úradu pre reguláciu elektronických komunikácií a poštových služieb bola už pri prijímaní ZoKB komunikovaná zásadná požiadavka, aby došlo k vypusteniu celého sektora Elektronických komunikácií z regulačného rámca zákona o kybernetickej bezpečnosti a to z dôvodu, že telekomunikačný sektor nie je predmetom Smernice NIS a je regulovaný vlastným regulačným rámcom, ktorý obdobné povinnosti už ukladá. Na jednej strane sa v súlade so Smernicou NIS ponecháva vylúčenie z pôsobnosti pre poskytovateľov dôveryhodných služieb z dôvodu existencie vlastného regulačného rámca, keďže podliehajú požiadavkám článku 19 nariadenia (EÚ) č. 910/2014. Na druhej strane sa paradoxne telekomunikačný sektor začleňuje do pôsobnosti ZoKB resp. rozširuje o nové oblasti, hoci rovnako nespadá do pôsobnosti Smernice NIS z dôvodu vlastného regulačného rámca pre oblasť bezpečnosti a integrity verejných elektronických komunikačných sietí a služieb. Poukazujeme tiež na recitál 19 Smernice NIS a uvádzaný cieľ Smernice NIS, aby sa zabezpečil konzistentný prístup a rovnaké uplatňovanie v jednotlivých členských štátoch pri vymedzení prevádzkovateľov základných služieb. „V záujme zaistenia konzistentného prístupu by sa vymedzenie pojmu „prevádzkovateľ základných služieb“ malo jednotne uplatňovať vo všetkých členských štátoch“. Na tento účel sa v smernici stanovuje posúdenie subjektov pôsobiacich v		ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
--	--	--	---

	konkrétnych odvetviach a pododvetviach, vytvorenie zoznamu základných služieb..“. Súčasná zmena zákona č. 351/2011 Z.z. ako sa navrhuje v čl. III návrhu by znamenala dualitu a nesystémovosť právnej úpravy, prekrývanie kompetencií dvoch samostatných orgánov dozoru (NBÚ a Úrad pre reguláciu elektronických komunikácií a poštových služieb), ktoré môžu samostatne a nezávisle bližšie určovať obsah a rozsah bezpečnostných a organizačných opatrení, ktoré majú podniky prijímať. Je nejasné ako sa budú riešiť príp. rozpory alebo odchýlky pri rovnakých či obdobných opatreniach, taktiež by mali byť podniky kontrolované a postihované za rovnaké nedostatky dvoma orgánmi dohľadu, čo považujeme za rozporné s princípmi právneho štátu. Znamenalo by to v konečnom dôsledku zrejme aj iné podmienky v úrovni služieb pre účastníkov, ak by sa mali selektívne uplatňovať osobitné požiadavky podľa ZoKB len pre niektoré podniky pri vymedzení identifikačných kritérií. Keďže ide o odlišné a od seba nezávislé právne úpravy, žiadame, aby sa z novely zákona o kybernetickej bezpečnosti vypustila akákoľvek zmena zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.			
AmCham Slovakia	Bod 33 Požadujeme vypustiť bod 33 v čl. I z návrhu. Odôvodnenie: Obdobne ako bod 32, uvedené ustanovenie § 27a zavádza nad rámec predmetu tohto zákona extrémne široko definovanú kompetenciu zásahov do fungovania a činnosti ľubovoľných subjektov, a to dokonca subjektov, ktoré ani nie sú predmetom tohto zákona (tzv. nedefinovaný pojem „prevádzkovateľ infraštruktúry“). Pojem „prevádzkovateľ infraštruktúry“ je tak neurčitým a vágnym pojmom, umožňujúcim svojvoľnú a účelovú interpretáciu zo strany úradu,	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	resp. ďalších štátnych orgánov. Ods. 5 uvádza pravidlá blokovania, ktoré však nie sú na rozdiel napr. od odkazovaného návrhu zákona č. .../2020 Z. z. o dohľade v oblasti ochrany spotrebiteľa v návrhu pre posúdenie dopadu k dispozícii, v skutočnosti tak dotknuté ustanovenie ponecháva plnú svojvôľu určiť akékoľvek opatrenie nezávisle od jeho vykonateľnosti a dopadu na subjekt, ktorý ho má vykonať, a takisto nezávisle od možností a časovej, vecnej či právnej realizovateľnosti na strane daného subjektu a takisto zaväzuje k súčinnosti ďalšie subjekty, vrátane orgánov verejnej moci, vykonať niečo, čo nemusí byť z ich strany vykonateľné. Ods. 6 neumožňuje žiadnu právnu ochranu, čím navrhuje dať úradu vyššie kompetencie ako majú súdy Slovenskej republiky alebo Policajný zbor, čo nie je pri takto vágnej kompetencii súladné so základnými princípmi právneho štátu. Navrhované znenie je v rozpore s princípom právnej istoty, ktorý je v právnom poriadku implicitne zakotvený v čl. 1 ods. 1 Ústavy SR a vyjadruje požiadavku aj na jasnosť, zrozumiteľnosť a predvídateľnosť právnych noriem a predvídateľnosť postupu orgánov verejnej moci. Návrh (ani súčasné znenie zákona) neobsahuje žiadnu konkrétnu definíciu blokovania ani obsahu, ktorý môže podliehať blokovaniu, resp. neobsahuje žiadne legislatívne vymedzenie pojmu „škodlivý obsah“ a „škodlivá aktivita“. Je pritom nevyhnutné legislatívne vymedziť predmet podliehajúci blokovaniu zo strany úradu ako aj jednotlivé formy a postupy blokovania. V opačnom prípade budú úradu priznané extrémne široké právomoci, pričom úrad tak v podstate môže rozhodnúť o blokovaní akéhokoľvek obsahu alebo aktivity. Neurčitosť a vágnosť pojmov „blokovanie“, „škodlivý obsah“ a „škodlivá aktivita“ je navyše v rozpore s princípom právnej istoty zakotveným v čl. 1 ods. 1 Ústavy SR, ktorá spôsobuje nepredvídateľnosť aplikácie predmetnej normy.			
--	---	--	--	--

	Oprávnenie úradu svojvoľne rozhodnúť o blokovaní bližšie nevymedzeného obsahu môže napĺňať znaky cenzúry, ktorá je v zmysle čl. 26 ods. 3 Ústavy SR zakázaná. Nevymedzenie pojmu „škodlivý obsah“ a „škodlivá aktivita“ považujeme za nedostatočné aj z pohľadu oprávnenosti obmedzenia základných ľudských práv a slobôd, resp. politických práv upravených Ústavou SR, a to najmä v súvislosti s obmedzením slobody prejavu a práva na informácie garantovaného v čl. 26 Ústavy SR (v rámci európskeho právneho priestoru je blokovanie prístupu k obsahu považované za flagrantný zásah do práva na slobodu prejavu). Podľa čl. 26 ods. 4 Ústavy SR právo na slobodu prejavu a právo vyhľadávať a šíriť informácie možno obmedziť zákonom, ak ide o opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti. Príslušný cieľ obmedzenia musí byť v zákone stanovený jasne a zrozumiteľne. Zo všeobecnej formulácie „škodlivý obsah“ a „škodlivá aktivita“ však nie je možné vyvodiť, či má blokovaniu podliehať obsah a aktivity, ktoré ohrozujú práva a slobody iných, bezpečnosť štátu, verejný poriadok, verejné zdravie alebo mravnosť. Iné právne predpisy zakotvujúce možnosť „blokovania“ obsahujú nielen konkretizované formy takejto blokácie, ale aj vymedzenie obsahu, resp. aktivity podliehajúc takémuto obmedzeniu. Vid' napr. § 16a ods. 1 zákona č. 43/1993 Z. z. o Slovenskej informačnej službe v alebo § 85 ods. 8 zákona č. 30/2019 Z. z. o hazardných hrách. Navyše odsek 7 neponecháva dotknutému subjektu vykonať úkon podľa zvyklosti, štandardných postupov a bežného práva, ale snaží sa mu priamo nadiktovať čo a ako má urobiť, opäť nezávisle od jeho technických, ľudských či iných možností, diskusie a analýzy dopadov. Takisto nie je zrejmé, ako chce úrad vykonať v			
--	--	--	--	--

	štandardných právnych podmienkach blokovanie na aktívach a majetku tretej strany. Návrh ponecháva výlučne na rozhodnutí úradu, aby stanovil spôsob (metódu) blokovania, pričom jediným kritériom podľa § 27a ods. 5 návrhu je, aby takýto spôsob bol „účinný, účelný a primeraný vo vzťahu k možným rizikám spojeným s blokováním“. Úradu by tak v podstate prináležala právomoc uložiť tretiemu subjektu povinnosť výlučne podľa svojho vlastného rozhodnutia a uváženia, a to bez ohľadu na reálnu vykonateľnosť takejto povinnosti z technického, ekonomického či časového hľadiska, ako aj bez ohľadu na dopad vykonania povinnosti na povinný subjekt (tzv. prevádzkovateľa infraštruktúry) alebo iné osoby, či bez ohľadu na efektívnosť a bezpečnosť takéhoto kroku. Podľa rozhodovacej praxe Európskeho súdu pre ľudské práva je pritom v rozpore s princípmi právneho štátu taká právna úprava, v ktorej je právna úvaha poskytnutá výkonnej moci vyjadrená ako neobmedzená právomoc. Zákon tak podľa ESĽP musí vyjadriť s dostatočnou jasnosťou rozsah úvahy udelenej príslušným orgánom a tiež aj spôsob jej výkonu. Z vyššie uvedeného vyplýva, že prijatím Návrhu by bola úradu v oblasti blokovania poskytnutá v podstate neobmedzená rozhodovacia aj výkonná moc, čo je v rozpore so základnými princípmi právneho štátu. Návrh navyše v rozpore s rozhodovacou praxou ESĽP nedostatočne a nejednoznačne vyjadruje rozsah úvahy udelenej úradu v oblasti rozhodovania o pristúpení k blokovaní ako i v oblasti spôsobu výkonu blokovania. Náklady na vykonanie blokovania podľa znenia návrhu v akejkoľvek situácii v plnom rozsahu znáša dotknutý subjekt, čo nie je možné napr. ani pri postupoch podľa GDPR, pričom v prípade, že je rozhodnutie priamo zo strany úradu, tento neprevezme ani len zodpovednosť za škodu, ktorá môže vyplývať z jeho rozhodnutia, t.j. dopad a riziko na strane			
--	---	--	--	--

subjektu, ktorý má vykonať blokovanie sú ešte vyššie. V tejto súvislosti je nutné všeobecne skonštatovať, že návrh je aj v rozpore s právom na súdnu a inú právnu ochranu zakotveným v čl. 46 Ústavy SR. Vzhľadom na to, že rozhodnutie Úradu o blokovaní sa podľa § 27a ods. 6 návrhu doručí len tzv. prevádzkovateľovi infraštruktúry, ďalšie osoby, do ktorých práv môže byť blokovaním zasiahnuté (napr. držiteľ domény, prevádzkovateľ blokovanej webovej stránky), sa o tomto zásahu v prvom rade ani nemusia dozvedieť a v druhom rade nemajú k dispozícii účinný prostriedok nápravy, prípadne obrany proti danému rozhodnutiu. Držiteľ domény, prevádzkovateľ webovej stránky alebo iná osoba, ktorá blokovaním utrpela zásah do svojich práv nemá možnosť žiadať o preskúmanie rozhodnutia úradu v odvolacom konaní a ani v rámci správneho súdnictva (napríklad v prípade obrany pred vydaním nezákonného rozhodnutia). Dané osoby totiž nemajú aktívnu legitimáciu na podanie správnej žaloby proti rozhodnutiu orgánu verejnej správy podľa Správneho súdneho poriadku. Návrh nezabezpečuje účinné mechanizmy nápravy nezákonných rozhodnutí a nerešpektuje procesné záruky pre tieto tretie osoby (napríklad pre držiteľov domén). Upozorňujeme aj na to, že i keď v iných právnych predpisoch existuje možnosť vydania príkazu na zamedzenie prevádzky webového sídla alebo prístupu na doménové meno, príslušné rozhodnutie vydáva súd na žiadosť orgánu výkonnej moci. Takýmto spôsobom je na rozdiel od predloženého návrhu zabezpečené aspoň minimálne preskúmanie dôvodnosti a rozsahu blokovania (tzn. zásahu do práv iných osôb), jeho trvania a vyváženosti zo strany nezávislého a nestranného súdu. Navrhované ustanovenie zasahuje aj do práva vlastníť a pokojne užívať majetok garantovaného čl. 20 Ústavy SR ako aj do práva podnikateľ zakotveného v čl. 35 Ústavy SR. Znenie návrhu totiž			
---	--	--	--

	pripúšťa možnosť výkonu blokovania priamo úradom a to nielen v prípade, že by tzv. prevádzkovateľ infraštruktúry nevykonával blokovanie na základe rozhodnutia úradu, ale v podstate v akejkoľvek situácii. Uvedené znamená, že úradu ako orgánu verejnej moci by mohli byť priznané právomoci zasiahnuť do infraštruktúry, systémov, priestorov či iného technického vybavenia daného prevádzkovateľa a teda obmedziť jeho vlastnícke práva. Nútené obmedzenie vlastníckych práv je dovolené, iba ak sa uskutoční v súlade s kumulatívne určenými podmienkami stanovenými v čl. 20 ods. 4 Ústavy. V danom prípade nie sú splnené kritéria oprávnenosti zásahu do majetku zo strany štátnych orgánov, nakoľko návrh nielenže neupravuje nevyhnutnú mieru takéhoto zásahu, súčasne predložené znenie neobsahuje ani žiadne vysvetlenie, z ktorého by bolo možné odôvodniť verejný záujem na zásahu štátu do vlastníctva fyzických či právnických osôb. Nad rámec toho návrh žiadnym spôsobom nerieši povinnosť štátu poskytnúť prevádzkovateľovi infraštruktúry primeranú náhradu za spôsobený zásah do vlastníckeho práva. Blokovanie čísiel a služieb upravuje zákon č. 351/2011 Z.z o elektronických komunikáciách (ďalej len „ZEK“), ktorý v § 41 ods. 4 ustanovuje, že blokovať sa môže iba na základe žiadosti orgánu činného v trestnom konaní. Toto ustanovenie tak, ako aj celý ZEK plne implementuje nariadenie č. 2015/2120 o sieťovej neutralite. Hlavnou ideou tohto nariadenie je: Koncoví užívatelia majú právo na prístup k informáciám a obsahu a právo šíriť informácie a obsah, využívať a poskytovať aplikácie a služby a využívať koncové zariadenie podľa vlastného výberu, bez ohľadu na umiestnenie koncového užívateľa alebo poskytovateľa, alebo na umiestnenie, pôvod či určenie informácií, obsahu, aplikácie alebo služby prostredníctvom ich služby prístupu k internetu.			
--	---	--	--	--

	Uvedené znamená, že každý má právo na prístup k elektronickým komunikačným službám, pokiaľ orgán činný v trestnom konaní nepožiada o zablokovanie. Navrhované ustanovenie je príliš všeobecné a je v rozpore s ZEK ako aj s nariadením a legislatívou EU, keďže v prípade jeho prijatia nie sú garantované uvedené práva užívateľov. Zároveň zakladá neistotu vo využívaní čísel a služieb z dôvodu príliš všeobecného návrhu ustanovenia bez garancie ochrany základných práv. Problematika blokovania je riešená napr. aj v zákone o SIS, kde blokovanie je realizované až po doručení súdneho príkazu, čiže existuje „právna istota“ v tom, že ide o blokovanie, ktoré je relevantné a odôvodnené. Ďalšia situácia je riešená v zákone o hazardě, kde je blokovanie vykonávané na základe príkazu súdu. Odporúčame zjednotiť legislatívu, a to v tom smere, že blokovanie je možné len na základe súhlasu/príkazu súdu, čo poskytuje dostatočnú právnu istotu, že ide o blokovanie relevantné a odôvodnené. Taktiež je nevyhnutné zdefinovať rozsah blokovania (vyšpecifikovať čo môže byť predmetom blokovania), ktorý bude uplatňovaný rovnako pre všetkých operátorov/poskytovateľov služieb. Blokovanie musí byť transparente odkomunikované smerom na užívateľa úradom/orgánom, ktorý o blokovanie žiada, napr. presmerovaním na stránky úradu/orgánu, kde sa užívateľ dozvie o dôvode blokovania. Musia byť zohľadnené aktuálne technické možnosti výkonu blokovania. Tzn. úrad nemôže žiadať operátorov o blokovanie obsahu služieb, ktorých nie je prevádzkovateľom (napr. obsah na Facebook, správy zasielané cez WA, Viber,...). Ak úrad bude požadovať blokovanie, ktoré vyžaduje dodatočnú technickú implementáciu na strane poskytovateľa služby musí sa podieľať na nákladoch s tým spojených. Podniky nemôžu konať v oblastiach,			
--	---	--	--	--

	ktoré sú regulované zákonom č. 351 /2011 Z.z. nad jeho rámec.			
AmCham Slovakia	Bod 50 Požadujeme vypustiť bod 50 v čl. I z návrhu, ktorým sa v prílohe 1 pre Sektor Digitálna infraštruktúra“ rozširujú prevádzkovatelia základnej služby. Odôvodnenie: Elektronický obchod ako taký nemožno považovať za základnú službu, navyše zahrnutie poskytovateľa akéhokoľvek malého elektronického obchodu do podmienok takejto striktnej regulácie je zásadne neprimerané a preto je potrebné ho vypustiť. Zároveň sa týmto zavádza neadekvátna nepriama regulácia subjektov už regulovaných napr. zákonom č. 22/2004 Z. z. o elektronickom obchode a ďalšími predpismi, ako napr. tými z oblasti zdravotníctva či bankovníctva, ktoré takisto definíčne spĺňajú navrhované znenie a zároveň sú krížovo zahrnuté aj pod inými sektormi podľa tejto prílohy. Túto časť je preto nutné vypustiť. Ide o rozšírenie na oblasti služieb, ktoré nie sú upravené smernicou NIS a tieto sa nenachádzajú v prílohe II Smernice NIS. Nie je jasné, z akej terminológie sa vychádza pri vymedzení nových služieb tak pre sektor Elektronické komunikácie ako aj sektor Digitálna infraštruktúra a aké je ich obsahové a pojmové určenie. Vychádzajúc aj z pojmológie, ktorú zavádza smernica 2018/1972 (EECC) by systematicky služby prístupu do internetu mali spadať pod elektronické komunikačné služby. Prevádzkovateľ obchodu na internete s možnosťou vyhľadávania, objednávaní a nákupu tovarov a služieb sa javí ako iná obdoba on-line trhoviska, ktoré však spadá pod digitálnu službu, rovnako aj služby DNS hostingu a webhostingu, pričom členské štáty nemajú ukladať poskytovateľom digitálnych služieb žiadne ďalšie bezpečnostné ani oznamovacie požiadavky nad rámec Smernice NIS (čl. 16 Smernice). Rovnako nie	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	sú bližšie určené ani identifikačné kritéria pre zaradenie.			
AmCham Slovakia	Bod 28 Uvedené má zásadný finančný a funkčný dopad na prevádzkovateľa základnej služby, pretože mu vnucuje povinné zamestnanie konkrétnej osoby so zásahom do jeho organizačnej štruktúry nezávisle od možností a počtu zamestnancov prevádzkovateľa základnej služby a navyše nepriamo vyžaduje povinnú certifikáciu takejto osoby. Uvedené ustanovenie požadujeme vypustiť alebo preformulovať do podoby, ktorá nemá takýto vážny dopad.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AmCham Slovakia	K § 29 ods. 4 V § 29 ods. 4 navrhujeme slová “Prevádzkovateľ základnej služby” nahradiť slovami “certifikovaný auditor kybernetickej bezpečnosti” Odôvodnenie: Pre zachovanie integrity správy z auditu a aj celkového procesu auditu, je vhodné, aby správu z auditu predkladal na úrad auditor a nie PZS.	Z	N	navrhovaný odsek 4 neobsahuje slova prevádzkovateľ základnej služby
AmCham Slovakia	Bod 16 Za bod 16. navrhujeme zaradiť nový bod: V §12 ods. 3 sa na konci vkladá veta: „Povinnosť zachovávať mlčanlivosť podľa odseku 1 sa tiež nevzťahuje na toho, kto vykonáva úlohy jednotky CSIRT podľa §15 a jeho zamestnancov v prípade trestného konania, oznamovania skutočnosti nasvedčujúcej tomu, že bol spáchaný trestný čin, alebo oznamovania kriminality.“ Odôvodnenie: V prípade trestného konania, alebo v prípade oznamovania skutočností, že bol spáchaný trestný čin, nie je akceptovateľné aby zamestnanci CSIRT nemohli poskytovať OČTK informácie. Práve jednotky CSIRT majú najviac informácií v rámci celého kontextu bezp. incidentu a práve preto má	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	jednotka CSIRT primárne spolupracovať s OČTK.			
AmCham Slovakia	Bod 6 Za bod 6. navrhujeme zaradiť nový bod: V § 3 písm. o) znie: „o) poskytovateľom digitálnej služby právnická osoba alebo fyzická osoba – podnikateľ, ktorá poskytuje digitálnu službu a zároveň poskytovanie digitálnej služby zabezpečuje prostredníctvom aspoň 50 zamestnancov a má ročný obrat z činnosti, ktorá je digitálnou službou, alebo celkovú ročnú bilanciu z činnosti, ktorá je digitálnou službou, viac ako 10 000 000 eur,“ Odôvodnenie: Z hľadiska kritéria rozsahu digitálnej služby je potrebné upresniť, že tieto kritéria sa majú vzťahovať výlučne na činnosť, ktorá je digitálnou službou a nie na celého podnikateľa. V opačnom prípade je totiž regulovanou digitálnou službou aj marginálna služba/ činnosť u relatívne veľkého subjektu. Nemalo by byť cieľom legislatívy regulovať z hľadiska verejného záujmu bezvýznamnú činnosť, ktorá síce má povahu digitálnej služby avšak nie je relevantná z hľadiska rozsahu. Napr. malé dátové centrum veľkej spoločnosti využívané predovšetkým pre vlastné potreby.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
AZZZ SR	návrhu zákona ako celku Návrh zákona dostatočne nezohľadňuje odporúčania Súboru nástrojov EÚ pre bezpečnosť 5G (https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures), predovšetkým vôbec nereflektuje navrhované tzv. strategické opatrenia, vrátane zohľadnenia politických rizík pri vyhodnocovaní rizikového profilu dodávateľov. Žiadame preto do zákona explicitne premietnuť opatrenia Súboru, predovšetkým: Strategické opatrenie 1: "Posilnenie úlohy štátnych orgánov ": Štátne úrady by mali mať právomoc sprísniť povinnosti operátorov (napr. z	Z	A	zapracované v § 27a

	hľadiska bezpečnostných opatrení) alebo ex-ante obmedziť/zakázať dodanie a prevádzku vybraných dodávateľov 5G zariadení s ohľadom na: a) kritické časti 5G sietí, b) bezpečnosť daného zariadenia, c) riziko ovplyvňovania 5G dodávateľského reťazca treťou krajinou alebo d) riziko ohrozenia národnej bezpečnosti. Strategické opatrenie 2: "Vykonanie auditov operátorov a vyžadovanie informácií": Príslušný úrad by si v prípade nutnosti mal právo vyžiadať audit kritických prvkov 5G sietí, vyžadovať od operátorov aktuálne informácie o plánoch dodávok 5G zariadení (vrátane informácií o dodávateľoch tretích strán) či vyžadovať od operátorov dokumentáciu týkajúcu sa implementácie základných bezpečnostných technických opatrení siete. Strategické opatrenie 3: "Hodnotenie rizikovosti profilov dodávateľov; obmedzenie vysokorizikových dodávateľov s cieľom zmiernenia rizík pre kľúčové prvky infraštruktúry": Stanoviť jasné kritériá pre posudzovanie rizikovosti dodávateľov; vykonať podrobné posúdenia rizikovosti všetkých dodávateľov, na základe ktorých sa pristúpi k reštrikciám na zmiernenie rizík pre prvky infraštruktúry definované ako zraniteľné podľa "Správy o koordinovanom posúdení rizík na úrovni EÚ, pokiaľ ide o bezpečnosť sietí 5G" (https://ec.europa.eu/commission/presscorner/detail/sk/IP_19_6049). Zaistiť, aby dodávatelia mali primerané kontrolné procesy manažovania rizík (audit dodávateľského reťazca a pod.) Strategické opatrenie 4: "Kontrola využívania poskytovateľov manažovaných služieb a podpory zabezpečovanej pre dodávateľa treťou stranou": Vytvorenie právneho rámca, ktorý by stanovil prevádzkovateľom 5G sietí, za akých podmienok môžu outsourcovať určité aktivity poskytovateľom riadených služieb (Managed Service Providers (MSPs)) - uplatnenie obmedzení pre zraniteľné časti 5G sietí (napr.			
--	--	--	--	--

bezpečnostné a sieťové prevádzkové funkcie, MSPs vyhodnotení ako vysokorizikovní...), schválenie dodatočných bezpečnostných opatrení pre výkon funkcií outsourcovaných na MSP V súlade so Súborom by zo zákona tiež mala jasne vyplývať povinnosť, že pri posudzovaní rizikovosti profilov dodávateľov 5G technológií z hľadiska ich vystavenia vládnym rozhodnutiam krajín mimo EÚ (politické kritériá), sa bude zohľadňovať: a) úzke prepojenie medzi dodávateľom a vládou tretej krajiny; b) právny rámec danej tretej krajiny (existencia demokratických kontrolných mechanizmov alebo medzivládnych dohôd o ochrane dát); c) črty vlastnickej štruktúry dodávateľa; d) možnosti vlády tretej krajiny vyvíjať na dodávateľa akýkoľvek tlak, napr. s ohľadom na geografické umiestnenie výroby dodávanej 5G technológie odôvodnenie: Vzhľadom na skutočnosť, že rozvoj 5G sietí bude mať priamy dopad na všetky sektory hospodárstva, považujeme za dôležité upozorniť na nutnosť dôslednej implementácie Súboru nástrojov EÚ pre bezpečnosť 5G, ktorý obsahuje škálu bezpečnostných opatrení na zmiernenie rizík a efektívne zavádzanie bezpečných 5G sietí. Jednoznačná a zrozumiteľná transpozícia týchto opatrení do zákona, vrátane (politických) kritérií pre posudzovanie rizikovosti dodávateľov, by vytvorila jasný a stabilný právny rámec, ktorý podporí odolnosť a bezpečnosť slovenského hospodárstva a jeho aktérov vo výrobnnej i nevýrobnej sfére. Vloženie kritérií do obvyčajnej vyhlášky by vytvorilo priestor na ich ľahkú zmenu bez verejnej diskusie do budúcnosti, čo podľa nás v tomto prípade, keď ide o bezpečnosť kritickej infraštruktúry štátu a jeho informačných systémov, nie je účelné ani žiadateľné. Komplexné zohľadnenie strategických a technických opatrení Súboru v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti je nevyhnutným predpokladom pre			
--	--	--	--

	zaistenie kľúčovej infraštruktúry Slovenskej republiky pred možnými neželanými aktivitami tretích strán.			
AZZZ SR	k Bodu 48. §34 odsek 6 Návrh: §34 odsek 6 nahradiť novým znením: “Prevádzkovateľ základnej služby zaradený do registra prevádzkovateľov základných služieb podľa odseku 5 je povinný do troch rokov odo dňa účinnosti tohto zákona prijať bezpečnostné opatrenia podľa § 20.” Odôvodnenie: Návrh, ktorého cieľom je predĺženie lehôt pre prevádzkovateľov základnej služby o jeden rok. Časová náročnosť, ekonomické dopady a komplikujúca sa spolupráca so subdodávateľmi prác a služieb pri plnení úloh vyplývajúcich zo Zákona o KB súvisiaca s opatreniami pri riešení aktuálnej epidemiologickej situácie, sú pre prevádzkovateľov základných služieb narastajúcim problémom.	Z	N	neodôvodnená pripomienka nad rámec novely
AZZZ SR	k bodu 48. §34 odsek 9 Návrh: §34 odsek 9 nahradiť novým znením: “Prevádzkovateľ základnej služby je povinný podrobiť sa auditu kybernetickej bezpečnosti a predložiť záverečnú správu o výsledkoch auditu úradu najneskôr do štyroch rokov od uplynutia lehoty podľa odseku 5.” Odôvodnenie: Návrh, ktorého cieľom je predĺženie lehôt pre prevádzkovateľov základnej služby o jeden rok. Časová náročnosť, ekonomické dopady a komplikujúca sa spolupráca so subdodávateľmi prác a služieb pri plnení úloh vyplývajúcich zo Zákona o KB súvisiaca s opatreniami pri riešení aktuálnej epidemiologickej situácie, sú pre prevádzkovateľov základných služieb narastajúcim problémom.	Z	N	neodôvodnená pripomienka nad rámec novely

AZZZ SR	k Bodu 11. § 5 Opraviť číslovanie, nový doplnený odsek by mal mať č.3. Odôvodnenie: Výhrada k textu: Pravdepodobne chyba v číslovaní. Terajšie znenie § 5 má dva odseky, t.j. nový, doplnený odsek by mal mať č. 3.	O	A	
Dopravný úrad	k novelizačnému bodu 10 Navrhujeme v § 5 odsek 1 doplniť písmenom ae), ktoré znie: „ae) plní úlohy príslušného orgánu a vykonáva koordináciu a monitorovanie podľa osobitného predpisu.10ac)“. Poznámka pod čiarou k odkazu 10ac znie: „10ac) Bod 1.7. prílohy vykonávacieho nariadenia Komisie (EÚ) 2015/1998 z 5. novembra 2015, ktorým sa stanovujú podrobné opatrenia na vykonávanie spoločných základných noriem bezpečnostnej ochrany letectva (Ú. v. EÚ L 299, 14.11.2015) v platnom znení.“. Odôvodnenie Príloha vykonávacieho nariadenia Komisie (EÚ) 2015/1998 z 5. novembra 2015, ktorým sa stanovujú podrobné opatrenia na vykonávanie spoločných základných noriem bezpečnostnej ochrany letectva v platnom znení sa, vykonávacím nariadením Komisie (EÚ) 2019/1583 z 25. septembra 2019, ktorým sa mení vykonávacie nariadenie (EÚ) 2015/1998, ktorým sa stanovujú podrobné opatrenia na vykonávanie spoločných základných noriem bezpečnostnej ochrany letectva, pokiaľ ide o opatrenia kybernetickej bezpečnosti, dopĺňa bodom 1.7., ktorý upravuje oblasť identifikácie a ochrany kritických systémov informačných a komunikačných technológií v civilnom letectve a údajov pred kybernetickými hrozbami. Vykonávacie nariadenie (EÚ) 2019/1583 nadobúda účinnosť dňa 31. decembra 2021; dátum nadobudnutia účinnosti bol posunutý z pôvodného 31. decembra 2020 na 31. decembra 2021, a to vykonávacím nariadením	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	Komisie (EÚ) 2020/910 z 30. júna 2020, ktorým sa menia vykonávacie nariadenia (EÚ) 2015/1998, (EÚ) 2019/103 a (EÚ) 2019/1583, pokiaľ ide o opätovné určenie leteckých spoločností, prevádzkovateľov a subjektov vykonávajúcich kontroly bezpečnostnej ochrany nákladu a poštových zásielok z tretích krajín, ako aj o odklad určitých regulačných požiadaviek v oblasti kybernetickej bezpečnosti, previerok osôb, noriem zariadení systémov detekcie výbušnín a zariadení na stopovú detekciu výbušnín v dôsledku pandémie COVID-19. Podľa bodu 4 preambuly vykonávacieho nariadenia (EÚ) 2019/1583 transpozíciou uvedených noriem (základné normy bezpečnostnej ochrany letectva) do vykonávacích právnych predpisov EÚ v oblasti bezpečnostnej ochrany letectva sa zabezpečí, aby príslušné orgány stanovili a vykonávali postupy, ktoré podľa potreby prakticky a včas umožňujú výmenu dôležitých informácií s cieľom pomôcť iným vnútroštátnym orgánom a agentúram, prevádzkovateľom letísk, leteckým dopravcom a ďalším dotknutým subjektom pri vykonávaní účinného posúdenia bezpečnostných rizík v súvislosti s ich činnosťami, a podporili tak dané subjekty pri vykonávaní účinných posúdení bezpečnostných rizík týkajúcich sa okrem iného kybernetickej bezpečnosti a pri vykonávaní opatrení na riešenie kybernetických hrozieb. Podľa bodu 1.7.1. vykonávacieho nariadenia (EÚ) 2015/1998 v znení vykonávacieho nariadenia (EÚ) 2019/1583 príslušný orgán zabezpečí, aby prevádzkovatelia letísk, leteckí dopravcovia a subjekty vymedzené vo vnútroštátnom programe bezpečnostnej ochrany civilného letectva identifikovali a chránili svoje kritické systémy informačných a komunikačných technológií a svoje údaje pred kybernetickými útokmi, ktoré by mohli mať vplyv na bezpečnostnú ochranu civilného letectva. Podľa bodu 1.7.4.			
--	---	--	--	--

	vykonávacieho nariadenia (EÚ) 2015/1998 v znení vykonávacieho nariadenia (EÚ) 2019/1583 ak sú konkrétny orgán alebo konkrétna agentúra zodpovedné za opatrenia súvisiace s kybernetickými hrozbami v rámci jedného členského štátu, daný orgán alebo agentúru možno poveriť koordináciou a/alebo monitorovaním ustanovení v tomto nariadení súvisiacich s kybernetickým priestorom. Podľa bodu 1.7.5. vykonávacieho nariadenia (EÚ) 2015/1998 v znení vykonávacieho nariadenia (EÚ) 2019/1583 ak sa na prevádzkovateľov letísk, leteckých dopravcov a subjekty vymedzené vo vnútroštátnom programe bezpečnostnej ochrany civilného letectva vzťahujú osobitné požiadavky na kybernetickú bezpečnosť vyplývajúce z iných právnych predpisov EÚ alebo členských štátov, príslušný orgán môže nahradiť súlad s požiadavkami tohto nariadenia súladom s prvkami obsiahnutými v iných právnych predpisoch EÚ alebo členských štátov. Príslušný orgán zosúladí svoj postup s akýmikoľvek inými dotknutými príslušnými orgánmi s cieľom zabezpečiť koordinované alebo kompatibilné režimy dohľadu. Podľa prílohy I materiálu k návrhu na určenie zodpovednosti ministerstiev, ostatných ústredných orgánov štátnej správy a niektorých orgánov verejnej moci za aplikáciu a prijatie opatrení na vnútroštátnej úrovni k nariadeniam Európskej únie a rozhodnutiam Európskej únie, schváleného uznesením vlády Slovenskej republiky č. 4 z 15. januára 2020, gestorom zodpovedným za aplikáciu a prijatie opatrení na vnútroštátnej úrovni vo vzťahu k vykonávaciemu nariadeniu (EÚ) 2019/1583 je, spoločne s Ministerstvom dopravy a výstavby Slovenskej republiky a Dopravným úradom, určený aj Národný bezpečnostný úrad, a to na základe pripomienky vznesenej Národným bezpečnostným úradom v rámci medzirezortného pripomienkového konania k návrhu tohto			
--	--	--	--	--

	materiálu. Na základe vyššie uvedeného preto Dopravný úrad navrhuje, aby v podmienkach Slovenskej republiky bol príslušným orgánom na účely bodu 1.7. vykonávacieho nariadenia (EÚ) 2015/1998 v platnom znení a orgánom vykonávajúcim koordináciu a monitorovanie ustanovení vykonávacieho nariadenia (EÚ) 2015/1998 v platnom znení súvisiacich s kybernetickým priestorom Národný bezpečnostný úrad. Zároveň odporúčame v úvodnej vete novelizačného bodu 10 slová „písmenami y) až ac)“ nahradiť slovami „písmenami y) až ad)“. Uvedenú pripomienku považujeme za zásadnú.			
Dopravný úrad	k novelizačnému bodu 49 Odporúčame navrhované slová „prevádzkovateľ letiska“ nahradiť slovami „prevádzkovatelia letísk“ z dôvodu jednotného použitia množného čísla v stĺpci „Prevádzkovateľ služieb“ prílohy č. 1 k zákonu č. 69/2018 Z. z. v znení neskorších predpisov. Uvedenú pripomienku považujeme za obyčajnú.	O	N	predkladateľom zvolená technika splna požiadavky Legislatívnych pravidiel
Dopravný úrad	Pripomienka všeobecná Podľa tabuľky zhody vypracovanej k návrhu zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov príloha č. 1 k zákonu č. 69/2018 Z. z. v znení neskorších predpisov predstavuje transpozíciu prílohy II smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. Prevádzkovatelia služieb uvedení v podsektore „Letecká doprava“, sektora „Doprava“ sú totožní s typmi subjektov uvedenými v prílohe II smernice (EÚ) 2016/1148 (odvetvie „Doprava“ pododvetvie „Letecká doprava“), a to pokiaľ ide o leteckých dopravcov, riadiace orgány letiska (prevádzkovateľov	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

letísk), letiská, subjekty prevádzkujúce pomocné zariadenia nachádzajúce sa na letiskách a prevádzkovateľov poskytujúcich služby riadenia letovej prevádzky (ATC); správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené, nie sú ako typ subjektu na účely článku 4 bodu 4 smernice 2016/1148 uvedení v prílohe II tejto smernice. Sektorové a prierezové kritéria na určenie prvkov kritickej infraštruktúry a zoznam prvkov kritickej infraštruktúry a ich zaradenie do sektorov kritickej infraštruktúry určuje uznesenie vlády Slovenskej republiky č. 347/2018. Služba riadenia letovej prevádzky (ATC) je, podľa definície pojmu letové prevádzkové služby uvedenej v čl. 2 ods. 11 nariadenia Európskeho parlamentu a Rady (ES) č. 549/2004 z 10. marca 2004, ktorým sa stanovuje rámec na vytvorenie jednotného európskeho neba (rámcové nariadenie) v platnom znení, zaradená medzi letové prevádzkové služby. Podľa čl. 2 ods. 4 nariadenia (ES) č. 549/2004 v platnom znení letecké navigačné služby znamenajú letové prevádzkové služby, spojovacie, navigačné a vyhľadávacie služby (resp. komunikačné, navigačné a prehľadové služby), meteorologické služby pre leteckú navigáciu a letecké informačné služby. Poskytovateľ leteckej navigačnej služby je definovaný v čl. 2 ods. 5 nariadenia (ES) č. 549/2004 v platnom znení ako akýkoľvek verejný alebo súkromný subjekt poskytujúci letecké navigačné služby pre všeobecnú letovú prevádzku. V podmienkach Slovenskej republiky letecké navigačné služby poskytujú Letové prevádzkové služby Slovenskej republiky, š. p., Ministerstvo obrany Slovenskej republiky (Vzdušné sily Slovenskej republiky) a Slovenský hydrometeorologický ústav (útvár leteckej meteorologickej služby).			
---	--	--	--

	V nadväznosti na vyššie uvedené poukazujeme súčasne na ustanovenie ATM/ANS.OR.D.010 písm. d) vykonávacieho nariadenia Komisie (EÚ) 2017/373 z 1. marca 2017, ktorým sa stanovujú spoločné požiadavky na poskytovateľov manažmentu letovej prevádzky/leteckých navigačných služieb a na ostatné funkcie siete manažmentu letovej prevádzky, ktorým sa zrušuje nariadenie (ES) č. 482/2008, vykonávacie nariadenia (EÚ) č. 1034/2011, (EÚ) č. 1035/2011 a (EÚ) 2016/1377 a ktorým sa mení nariadenie (EÚ) č. 677/2011 v platnom znení, podľa ktorého poskytovatelia leteckých navigačných služieb a poskytovatelia, ktorí zabezpečujú manažment toku letovej prevádzky, a manažér siete prijímú opatrenia potrebné na to, aby chránili svoje systémy, používané súčasti systému a údaje a zabránili tomu, aby bola sieť vystavená bezpečnostným informačným a kybernetickým hrozbám, ktoré môžu nezákonne narušať poskytovanie ich služieb. V podmienkach Slovenskej republiky sa citované ustanovenie vzťahuje na poskytovateľov leteckých navigačných služieb a poskytovateľov, ktorí zabezpečujú manažment toku letovej prevádzky; úlohy manažéra siete plní, v súlade s vykonávacím rozhodnutím Komisie (EÚ) 2019/709 zo 6. mája 2019 o vymenovaní manažéra siete pre funkcie siete manažmentu letovej prevádzky (ATM) v rámci jednotného európskeho neba, Eurocontrol. Uvedenú pripomienku považujeme za obyčajnú.			
eustream	Čl. I. bod 31, §24 ods. 7 Ustanovenie zavádza nový pojem „zaistenie kybernetickej bezpečnosti“, ktorý nie je v zákone definovaný. Zároveň z logiky veci vyplýva, že moment, ku ktorému je možné vzťahovať zasielanie informácií, je stav, kedy dôjde k narušeniu kybernetickej	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text

	bezpečnosti, a to kybernetickým bezpečnostným incidentom. Máme za to, že povinnosť zasielania informácií pri riešení závažného kybernetického bezpečnostného incidentu je tak v dostatočnej miere upravená v súčasnom znení zákona. Uvedené ustanovenie môže navyše vyvolávať dodatočné náklady na strane prevádzkovateľov základnej služby a zároveň neprimerane zasahovať do súkromného vlastníctva a narušovať dôvernosť informácií. Zároveň návrh neposkytuje záruky, že takýto povinný krok môže napomôcť vyriešeniu závažného kybernetického incidentu alebo k znemožneniu páchania trestnej činnosti v oblasti kybernetickej bezpečnosti. Návrh: Vypustiť uvedené ustanovenie. Alternatívne: „(7) Na hlásenie závažných kybernetických bezpečnostných incidentov je prevádzkovateľ základnej služby určený rozhodnutím úradu povinný zasielať automatizovaným spôsobom a vo vzájomne dohodnutom rozsahu informácie z elektronických komunikačných sietí a informačných systémov, ktoré sú nevyhnutné v rámci riešenia závažného kybernetického incidentu alebo objasnenia trestného činu.			tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
eustream	Čl. I. bod 10., §5 ods. 1 písm. y) V uvedenom ustanovení sa používajú nedefinované pojmy „škodlivý obsah“ a „škodlivá aktivita“ vo vzťahu k pojmu „blokovanie“, ktorý má byť použitý v ďalšom texte zákona, pričom v tomto prípade z textu vyplýva, že má ísť o osobitný prípad rozhodnutia o blokovaní vydaného NBÚ v rámci riešenia opatrení o blokovaní podľa osobitných predpisov. Z uvedeného dôvodu navrhujeme pojem „blokovanie“ jednotne zadefinovať v rámci § 3 „Vymedzenie základných pojmov“, prípadne v navrhovanom novom ust. § 27a „Blokovanie“. Návrh ustanovenia: V § 5 sa odsek 1 dopĺňa	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	písmenami y) až ac), ktoré znejú: „y) v rámci riešenia opatrení o blokovani podľa osobitných predpisov10aa) vydáva rozhodnutie o blokovani a zabezpečuje vykonanie tohto rozhodnutia,"			
eustream	Čl. I. bod 33, §27a ods. 1 Z §5 ods. 1 písm. y) vyplýva, že zámerom NBÚ je vykonávať blokovanie len pre prípady resp. v rámci riešenia opatrení o blokovani podľa osobitných predpisov. Navrhované ustanovenia v §27a však naznačujú širokú definíciu „blokovanja“ vo vzťahu k akémukoľvek kybernetickému bezpečnostnému incidentu a zároveň k riešeniu opatrení o blokovani podľa osobitných predpisov. Navrhujeme preto zosúladiť rozsah novej kompetencie NBÚ podľa § 27a s ust. §5 ods. 1 písm. y) a súčasne, keďže pre účely riešenia kybernetických bezpečnostných incidentov považujeme súčasnú kompetenciu NBÚ podľa §5 ods. 1 písm. q) za dostatočnú, navrhujeme vypustiť §27a ods. 1 a celý §27a primerane upraviť len pre prípady riešenia opatrení o blokovani podľa osobitných predpisov.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
GPSR	14. Nad rámec predloženého návrhu – Z: Nad rámec predloženého návrhu si dovoľujeme upozorniť na nevyhnutnosť legislatívne upraviť podmienky týkajúce sa ustanovenia § 63 ods. 17 zákona č. 351/2011 Z. z. o elektronických komunikáciách, ktoré bolo zavedené do citovaného právneho predpisu práve zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti. Citované ustanovenie zákona č. 351/2011 Z. z. odkazuje na zákon o kybernetickej bezpečnosti, ktorý však podrobnejšie neupravuje prístup k údajom podliehajúcim telekomunikačnému tajomstvu. Uvádzané účely v zákone č. 351/2011 Z. z. súvisia s bezpečnostnými incidentmi. Prístup k	Z	ČA	text upravený po dohode s gestorm

údajom, ktoré sú predmetom telekomunikačného tajomstva, predstavuje zásah do základných práv a slobôd. Zásahy do základných práv a slobôd musia byť v demokratickej spoločnosti predvídateľné, primerané a nevyhnutné. Je nepochybné, že tieto právne princípy /vyplývajúce aj z medzinárodných zmlúv, ktorými je Slovenská republika viazaná a z judikatúry európskych súdov/, musia byť aplikované aj na prístup k predmetným údajom. Otázka uchovávania údajov, ale aj prístupu k nim, bola tiež predmetom rozhodovacej činnosti Ústavného súdu Slovenskej republiky. Zákon o kybernetickej bezpečnosti by preto mal obsahovať podmienky pre uplatnenie § 63 ods. 17 zákona č. 351/2011 Z. z. Poukazujeme na to, že v prípade trestného konania je možnosť prístupu k údajom, ktoré sú predmetom telekomunikačného tajomstva, výrazne obmedzená a takéto údaje nemožno získať vo vzťahu ku každému trestnému činu, ale len vo vzťahu ku konkrétnym trestným činom vymedzeným v § 116 ods. 1 Trestného poriadku (a pri splnení ďalších zákonných podmienok). V porovnaní s takouto striktnou právnou úpravou je v zjavnom nepomere s princípmi primeranosti a nevyhnutnosti povinnosť podľa § 63 ods. 17 zákona č. 351/2011 Z. z. na sprístupnenie telekomunikačného tajomstva, ktorá sa týka každého (nielen závažného) bezpečnostného kybernetického incidentu. Nepochybujeme, že v praxi môže nastať situácia, v ktorej bude potrebné bezodkladné sprístupnenie uvedených údajov (napríklad bezprostredná teroristická hrozba, ohlásenie útoku na vysokopostavených štátnych predstaviteľov, veľmi intenzívny útok na kritickú infraštruktúru a rôzne iné), respektíve taká situácia, v ktorej nebude možné, respektíve vzhľadom na závažnosť a bezprostrednosť hrozby nebude primerané požadovať získanie predchádzajúceho súhlasu súdu. Avšak aj v takýchto prípadoch			
---	--	--	--

	považujeme za nevyhnutné, aby súd ako nestranný a nezávislý orgán spätne preskúmal (po odstránení/odvrátení hrozby) zákonnosť sprístupnenia takýchto citlivých údajov. Prístup k takýmto údajom bez súdnej (alebo inej nezávislej) kontroly by mohol byť v rozpore s ústavnými princípmi, prípadne môže byť v rozpore s Chartou základných práv a slobôd Európskej únie a ďalšími medzinárodnými zmluvami v oblasti ľudských práv, ktorými je Slovenská republika viazaná. Okrem toho, ako bolo už aj vyššie uvedené, dochádza ku kumulácii viacerých oprávnení pre Národný bezpečnostný úrad (certifikácia, CSIRT, blokovanie a ďalšie), pričom takejto kumulácii oprávnení by mali zodpovedať aj dostatočné kontrolné mechanizmy. Táto pripomienka je zásadná.			
GPSR	10. K čl. I bodu 33 (§ 27a) - Z: Návrhom neboli ustanovené jasné pravidlá ani podmienky alebo aspoň princípy pre rozhodnutie o blokovaní a o spôsobe blokovania, čo pri monopolizácii možnosti reštrikčného správania Národného bezpečnostného úradu nepovažujeme za vyvážené. Prevádzkovateľ základnej služby je pri tom aj naďalej (bez ohľadu na rozhodnutie o blokovaní) zodpovedný za funkčnosť a bezpečnosť základnej služby. Upozorňujeme na to, že Policajný zbor aktuálne nedisponuje oprávnením vydávať ani žiadať o vydanie rozhodnutia o blokovaní podľa zákona č. 171/1993 Z. z. o Policajnom zbore, ktoré predpokladá navrhované znenie § 27a ods. 2 zákona o kybernetickej bezpečnosti (v poznámke pod čiarou k odkazu 28a sa odkazuje na zákon č. 171/1993 Z. z. o Policajnom zbore) v spojení s odsekom 4. Aj keď sa v texte návrhu zákona uvádza „žiadost“, z dôvodovej správy sa zdá, že o blokovaní by mali mať možnosť rozhodovať aj iné orgány, vrátane Policajného zboru. V tomto smere bude zrejme	Z	A	

	potrebné precizovať dôvodovú správu, respektíve doplniť príslušné kompetencie Policajného zboru aj do zákona č. 171/1993 Z. z. V navrhovanom znení odseku 6 navrhujeme vypustiť pojem „preukázateľne“. Právny pojem „doručenie“ považujeme za dostatočný a zrejmy. Z navrhovaného ustanovenia nevyplýva, ako sa bude postupovať v prípade, ak dôsledky incidentu sú na území Slovenskej republiky, avšak subjekt, ktorý prevádzkuje infraštruktúru, sa nachádza v cudzine. Považujeme za potrebné precizovať vzťah inštitútu blokovania k trestnému konaniu. Príklady uvádzané v dôvodovej správe budú bežne viesť k začatiu trestného stíhania a k vykonávaniu úkonov trestného konania (vrátane takých úkonov trestného konania, ktoré sa realizujú utajeným spôsobom), o ktorých nemá Národný bezpečnostný úrad vedomosť. V takom prípade by vykonanie blokovania mohlo ohroziť úkony trestného konania, či zmariť získanie dôkazov. Tento aspekt navrhovaná úprava nerieši. Rovnako nie je riešená povinnosť komunikácie s orgánmi činnými v trestnom konaní pred realizáciou blokovania. Ak je to možné, bude nevyhnutné ešte pred realizáciou blokovania zabezpečiť dôkazy pre trestné konanie zákonným spôsobom. Rozhodnutie úradu sa pritom považuje za konečné. Navrhujeme v návrhu zákona výslovne uviesť možnosť preskúmania rozhodnutia Národného bezpečnostného úradu o blokovaní a o spôsobe blokovania súdom. Táto pripomienka je zásadná.			
GPSR	3. K čl. I bodu 10 (poznámka pod čiarou 10aa) – O: Navrhované znenie odkazuje v poznámke pod čiarou 10aa na právny predpis, ktorý je v legislatívnom procese od 4. septembra 2019 vedenom na SLOV-LEXe pod č. LP/2019/496 (návrh zákona o dohľade v oblasti ochrany spotrebiteľa a o zmene a doplnení	O	A	

	niektorých zákonov). Navrhujeme v takýchto prípadoch uvádzať navrhované znenie zákona, na ktorý sa odkazuje, aj v sprievodných dokumentoch a/alebo uviesť link na príslušný legislatívny proces, aby bolo možné tento návrh v aktuálnej podobe bez väčších ťažkostí vyhľadať a preskúmať, napríklad aj v kontexte možných rozpočtových nárokov na potrebu doplnenia, či úprav informačných systémov verejnej správy. Takéto doplnenie sprievodných materiálov verejne prístupných na portáli SLOV-LEX by nepochybne privítali nielen povinne pripomienkujúce subjekty, ale aj široká verejnosť, tak odborná ako aj laická.			
GPSR	5. K čl. I bodu 11 (§ 5 ods. 4) – Z: Navrhované znenie oprávnenia Národného bezpečnostného úradu považujeme za veľmi široké. Nereflektuje na osobitosti a účel trestného konania, respektíve na prípady, kedy môže dôjsť ku konkurencii verejných záujmov na postihu trestných činov vs. verejný záujem na plnení úloh podľa zákona o kybernetickej bezpečnosti. Takto by v podstate mohli byť z prebiehajúceho trestného konania vyžiadané kompletne údaje (aj kópia spisu, výsluchy, výsledky ITP, respektíve čokoľvek, čo nie je prístupné iným subjektom mimo orgánov činných v trestnom konaní a súdu) a mohli by viesť k zmareniu účelu trestného konania (čisto teoreticky nemožno vylúčiť situáciu, že by bola v trestnom konaní dokumentovaná kybernetická aktivita, či útok, ktorý by sa mohol týkať aj samotného Národného bezpečnostného úradu). Je potrebné nastaviť mechanizmus, aby rozsah požadovaných údajov vo vzťahu k trestnému konaniu bol definovaný a odôvodnený a ich poskytnutie podliehalo napríklad súhlasu prokurátora v prípravnom konaní a sudcu v konaní pred súdom. Samozrejme je možné, že bude	Z	A	Text preformulovaný tak, aby splňal predpoklady uvedené v pripomienkach.

	nevyhnutné napríklad v rámci blokovania poskytnúť údaje známe polícii pre Národný bezpečnostný úrad pre účely plnenia úloh úradu podľa zákona o kybernetickej bezpečnosti (určite nie však v rozsahu celého spisu a pod.) Zastávame názor, že uvedené by malo byť prediskutované a pravidlom ustanovený rozsah údajov, ktoré môžu byť požadované), pričom Národný bezpečnostný úrad by mal mať tiež povinnosť viesť evidenciu osôb, ktoré boli s údajmi oboznámené a zákaz poskytnúť ich inému subjektu. Taktiež by mal mať povinnosť zálohovať údaje súvisiace s kybernetickým prostredím a porušeniami jeho pravidiel, aby naopak orgány činné v trestnom konaní a súdy mohli efektívne viesť vyšetrovanie na základe zákonným spôsobom získaných dôkazov. Táto pripomienka je zásadná.			
GPSR	9. K čl. I bodu 32 .§ 27 ods. 1 písm. e). – Z: Navrhujeme doplniť oprávnenie Národného bezpečnostného úradu rozhodnutím zakázať alebo obmedziť prevádzkovateľovi základnej služby používať konkrétny produkt, proces alebo službu, ak je to potrebné na zaistenie kybernetickej bezpečnosti, alebo z dôvodov bezpečnostného záujmu Slovenskej republiky. Následným vykonaním tohto rozhodnutia nastáva vysoké riziko znefunkčnenia základnej služby. Navrhujeme ustanoviť povinnosť štátu zabezpečiť pomoc a podporu finančnú i technickú a technologickú prevádzkovateľovi základnej služby za účelom čo najrýchlejšieho dosiahnutia obnovy funkcionality znefunkčnenej základnej služby v dôsledku rozhodnutia Národného bezpečnostného úradu. Žiadame upraviť postup dotknutého subjektu (prevádzkovateľa základnej služby), ak sa týmto zákazom znefunkční základná služba. Nie je zrejmé, v akom režime sa zabezpečí obnovenie základnej služby,	Z	A	text preformulovaný aj s ohľadom na iné vznesené pripomienky

	ako sa bude realizovať verejné obstarávanie nevyhnutného nového hardvéru, prípadne vykonanie prác potrebných na nevyhnutnú úpravu/zmenu informačného systému. Táto pripomienka je zásadná.			
GPSR	8. K čl. I bodu 31 (§ 24 ods. 7) – Z: Navrhuje sa pravidlo, podľa ktorého bude prevádzkovateľ základnej služby určený rozhodnutím Národného bezpečnostného úradu povinný na hlásenie kybernetických bezpečnostných incidentov alebo na zaistenie kybernetickej bezpečnosti zasielať Národnému bezpečnostnému úradu automatizovaným spôsobom a v rozsahu ustanovenom v štandarde určené systémové informácie zo sietí a informačných systémov. Navrhovaná povinnosť môže byť problematická z dvoch dôvodov – neobmedzuje rozsah informácií, ktoré možno požadovať a súčasne nepredpokladá alternatívu, že bezpečnostný incident môže znemožniť zasielanie hlásenia automatizovaným spôsobom v ustanovenej forme a rozsahu (podobná výhrada sa týka aj bodu 38). Čo sa týka rozsahu údajov – aj keď ustanovenie obsahuje konštrukciu „v rozsahu ustanovenom v štandarde úradu“ tento rozsah nemôže byť absolútny, musí byť obmedzený ustanoveným legitímnym účelom zasielania údajov. Pri stanovení takéhoto rozsahu by úrad mal byť obmedzený tak, aby napríklad nebolo možné požadovať taký rozsah údajov, ktorý by obsahoval prístupové údaje, heslá a podobne. Z uvedeného vyplýva, že automatizovaný spôsob zasielania hlásení bude potrebné zaviesť v rámci všetkých informačných systémov prevádzkovateľov základnej služby, vrátane Generálnej prokuratúry Slovenskej republiky, čo si bude vyžadovať zatiaľ neurčiteľné finančné prostriedky, keďže rozsah (jeho štandard) bude úradom určený až dodatočne. V dôsledku toho nebude vedieť prevádzkovateľ	Z	A	text preformulovaný aj s ohľadom na iné vznesené pripomienky

	základnej služby odhadnúť, naplánovať a uplatniť navýšenie rozpočtových nákladov. Táto pripomienka je zásadná.			
GPSR	6. K čl. I bodu 14 (§ 9 ods. 2) – O: Navrhujeme upraviť vzťah medzi vládnu jednotkou CSIRT a národnou jednotkou CSIRT, respektíve Národným centrom kybernetickej bezpečnosti SK-CERT, prípadne aj k ďalším jednotkám CSIRT, prípadne ho vysvetliť aspoň v dôvodovej správe.	O	A	dovodova sprava upravena
GPSR	11. K čl. I bodu 39 .§ 31 ods. 5 písm. c). – O: Navrhujeme za slová „v rozpore s § 27 ods. 1“ pripojiť slová „písm. e)“, keďže použitie produktu, služby alebo postupu môže byť len v rozpore s týmto konkrétnym ustanovením, nie v prípade ostatných situácií uvedených v § 27 ods. 1 písm. a) až d).	O	A	
GPSR	2. K čl. I bodu 5 .§ 3 písm. b). – Z: Od novelizácie zákona č. 351/2011 Z. z. o elektronických komunikáciách zákonom č. 69/2018 Z. z. sú uvedené právne predpisy vo vzájomnej súvislosti. Z tohto dôvodu z vecného hľadiska nepovažujeme za vhodné, aby každý z citovaných predpisov obsahoval samostatnú, a najmä odlišnú, definíciu pojmu „elektronická komunikačná sieť“. V tej súvislosti poukazujeme na to, že pre členské štáty EÚ je záväzná definícia pojmu „elektronická komunikačná sieť“ ustanovená v čl. 2 písm. a) smernice Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica) (Ú. v. ES L 108, 24.4.2002, s. 33 – 50). Podľa čl. 2 písm. a) uvedenej smernice: „a) "elektronická komunikačná sieť" znamená prenosové systémy a kde je to potrebné zariadenie na prepájanie alebo smerovanie a iné prostriedky, ktoré umožňujú	Z	A	

	prenos signálov po drôte, rádiovými, optickými alebo inými elektromagnetickými prostriedkami, vrátane družicových sietí, pevných (s prepínaním okruhov a paketov vrátane internetu) a mobilných pozemských sietí, elektrických káblových systémov v rozsahu, v ktorom sú používané na prenos signálov, siete používané pre rozhlasové a televízne vysielanie a siete káblovej televízie, bez ohľadu na typ prenášanej informácie;“. Táto pripomienka je zásadná.			
GPSR	12. K čl. I bodu 40 – O: Odporúčame slová „označujú ako písmená 10 až 16“ nahradiť slovami „označujú ako odseky 10 až 16“ (oprava zrejmej nesprávnosti).	O	A	
GPSR	13. K čl. I bodom 40 a 42 § 31 ods. 6 až 9 a § 31a ods. 1 a 2. - O: Odporúčame upraviť ustanovenia tak, aby boli v súlade s bodom 62.3 prílohy č. 1 k Legislatívnym pravidlám vlády Slovenskej republiky (legislatívno-technická pripomienka). Podľa bodu 62.3 prílohy č. 1 k Legislatívnym pravidlám vlády Slovenskej republiky „V texte právneho predpisu sa nariadenia Európskej únie alebo rozhodnutia Európskej únie necitujú, ale použije sa odkaz na osobitný predpis a v príslušnej poznámke pod čiarou sa uvedie ich názov a publikačný zdroj. To neplatí, ak implementáciu nariadenia Európskej únie alebo rozhodnutia Európskej únie nie je možné vykonať iným spôsobom.“.	O	A	
GPSR	7. K čl. I bodu 21 (§ 17 ods. 8) – O: Podľa navrhovaného znenia § 17 ods. 8 „Úrad rozhodne o výmaze do 30 dní.“. Z hľadiska právnej istoty by mal byť jednoznačne ustanovený deň alebo pravidlo, podľa ktorého sa určí deň, od	O	N	text vypustený

	ktorého sa začne počítať lehota 30 dní, respektíve 60 dní, zrejme v nadväznosti na navrhované znenie § 17 ods. 7.			
GPSR	4. K čl. I bodom 10 a 33 .§ 5 ods. 1 písm. y) a § 27a ods. 1. – Z: Podľa navrhovaného znenia by mal byť Národný bezpečnostný úrad (ďalej len „úrad“) oprávnený vydávať rozhodnutie o blokovaní, o spôsobe blokovaní a zároveň má byť úrad oprávnený zabezpečiť aj vykonanie tohto rozhodnutia - čo v rukách úradu koncentruje veľkú právomoc. Navrhujeme zvážiť odčlenenie rozhodovania o blokovaní a o spôsobe blokovaní od výkonu blokovaní medzi dve od seba nezávislé inštitúcie, aby nebolo možné prostredníctvom vplyvu na jedinou inštitúciu zneužiť jej koncentrované právomoci na politické, či iné nedemokratické ciele, respektíve, aby v prípade akýchkoľvek nedostatkov v postupe alebo rozhodnutí jedného úradu mohla na nedostatky primerane vecne zareagovať iná na úrade nezávislá inštitúcia. Poznamenávame, že pri navrhovanom zákone o dohľade v oblasti ochrany spotrebiteľa (materiál č. LP/2019/496) sa v časti upravujúcej „orgány dohľadu“ neustanovuje Národný bezpečnostný úrad ako orgán dohľadu (§ 2). Pre výkon blokovaní (§ 11), či vykonanie akejkoľvek inej reštrikcie je potrebné vykonať procesné úkony, ako je vyhotovenie zápisnice, výzva na odstránenie, respektíve požiadanie súdu o vydanie príkazu, ktorým sa prikáže poskytovateľovi služieb informačnej spoločnosti alebo registračnej autorite pre doménu najvyššej úrovne .sk vykonať taxatívne vymenované reštrikcie, kde sa hovorí výlučne o zablokovaní online rozhrania pre niektoré alebo pre všetky úkony alebo služby - v relácii „dohliadaný subjekt - orgán dohľadu“. Táto pripomienka je zásadná.	Z	ČA	text je preformulovaný, rozdelné do dvoch samostatných ustanovení. je doplnená DS. Blokovanie je riešenie ultima ratio (subsidiarita represie). Na základe požiadavky (MHSR) z minulého roka došlo k formulovaniu nástroja aj ako výkonu rozhodnutia pre iné orgány verejnej moci (zásah je potrebné vykonať s odbornou zručnosťou a odborným spôsobom). Návrh zákona bol predmetom PPK a aktuálna platforma predstavuje možnosť vyjadriť sa formulovať konkrétne požiadavky a výhrady širokému spektru subjektov (účel MPK). Zákon obsahuje určenie zodpovednosti (úrad aj iný orgán- žiadateľ), opravný prostriedok (preskúmateľnosť súdom), splnomocňovacie ustanovenie na podrobnosti a spôsob blokovaní (novelizačný bod 45) a rovnako dáva možnosť dotknutým orgánom vykonať legislatívne zmeny vo svojich právnych predpisoch tak, aby sa efektívny, účelný a účinný spôsobom dosiahla náprava a zamedzení škodlivých aktivít v našom kybernetickom priestore.

				Ustanovenie nebráni iným orgánom vo výkone svojich úloh, ustanovenie svojim cieľom napomáha ich efektívnej činnosti a nikoho nenúti, aby úrad žiadal o výkon takéhoto rozhodnutia.
GPSR	1. K čl. I bodu 3 (poznámka pod čiarou k odkazu 7) – Z: Považujeme za potrebné doplniť dôvodovú správu, nakoľko nie je zrejmé, ktorý novelizačný bod predstavuje zmenu normatívnej úpravy, dôsledkom ktorej je vypustenie odkazu na zákon 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. Doposiaľ sa zákon o kybernetickej bezpečnosti nevzťahoval na právne vzťahy upravené zákonom č. 166/2003 Z. z. Z predkladacej správy, ani z dôvodovej správy nemožno zistiť dôvody, pre ktoré by sa mal zákon o kybernetickej bezpečnosti vzťahovať na právne vzťahy upravené zákonom č. 166/2003 Z. z. Táto pripomienka je zásadná.	Z	A	
MDaVSR	Čl. I bod 1. § 2 ods. 2 písmeno d) V Čl. I bod 1. § 2 ods. 2 písmeno d) žiadame zosúladiť pojem siet' s definíciou elektronickej komunikačnej siete (legislatívna skratka „siet“) v § 3 písm. b). Túto pripomienku považujeme za zásadnú. Odôvodnenie: Legislatívna skratka „siet“ je zavedená až pri definícii elektronickej komunikačnej siete a nie je zrejmé, či predkladateľ má na mysli v § 2 ods. 2 písmeno d) elektronickú komunikačnú sieť.	Z	A	

MDaVSR	Čl. I bod 23. V Čl. I bod 23. odporúčame slová „dvanástich“ nahradiť číslovkou „12“.	O	A	
MDaVSR	Čl. I bod 28. V Čl. I bod 28. odporúčame slová „písmeno a) znie“ nahradiť slovami „sa vkladá nové písmeno a) ktoré znie“.	O	A	
MDaVSR	Čl. I bod 4 § 3 písmeno a) V Čl. I bod 4 § 3 písmeno a) odporúčame vypustiť slovo „používanie“ pretože predmetné slovo je synonymom už k uvedeným činnostiam.	O	A	
MDaVSR	Čl. I bod 50. V Čl. I bod 50. odporúčame slovo „ktorý“ nahradiť slovom „ktoré“.	O	A	
MDaVSR	V Čl. I bod 50. V Čl. I bod 50. žiadame slová „poskytovateľ dátových, hlasových a internetových služieb – služieb pripojenia do internetu“ vypustiť. Túto pripomienku považujeme za zásadnú. Odôvodnenie: Navrhované doplnenie je nelogické. V príslušnom stĺpci sú uvádzaní prevádzkovatelia a nie služby. Súčasne pojem „internetové služby“ legislatíva elektronických komunikácií nedefinuje a nie je zrejmé, čo má predkladateľ na mysli.	Z	A	
MDaVSR	Čl. I bod 51. V Čl. I bod 51. žiadame slová „služby vysokorýchlostného prenosu dát a hlasu v pevnej a mobilnej elektronickej komunikačnej sieti“ vypustiť. Túto pripomienku považujeme za zásadnú. Odôvodnenie: Navrhované doplnenie je nelogické. V príslušnom stĺpci sú uvádzaní prevádzkovatelia a nie služby. Pokiaľ má predkladateľ úmysel	Z	A	

	pokryť prevádzkovateľov vysokorychlostného prenosu dát, títo sú už pokrytí v platnom znení prílohy č. 1 v sektore „4. Elektronické komunikácie“.			
MDaVSR	Čl. I bod 52. V Čl. I bod 52. v prílohe č. 1 v sektore „10. Verejná správa“ v podsektore „Utajované skutočnosti“ v stĺpci „Prevádzkovateľ služieb“ žiadame vypustiť riadok „správca a prevádzkovateľ verejnej regulovanej služby, ktorú poskytuje globálny satelitný navigačný systém zriadený v rámci programu Galileo, alebo správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú naň napojené“. Túto pripomienku považujeme za zásadnú. Odôvodnenie: Ide o uzavretý systém, ktorého správcom a prevádzkovateľom je Európska agentúra pre globálne navigačné satelitné systémy (GSA). Súčasne na základe definície siete podľa § 3 písm. b) nie sú na tento systém priamo napojení prevádzkovatelia elektronických komunikačných sietí.	Z	A	
MDaVSR	Čl. I bod 7 § 3 písmeno u) V Čl. I bod 7 § 3 písmeno u) odporúčame slová „overenie plnenia povinností“ vypustiť, keďže zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov zahŕňa aj overenie plnenia povinností.	O	N	ide o definíciu auditu tak, aby spĺňala požadované atribúty.
MDaVSR	Čl. I úvodná veta V Čl. I úvodná veta odporúčame za slovami „v znení“ vložiť slová „zákona č. 373/2018 Z. z. a zákona č. 134/2020 Z. z.“.	O	A	
MDaVSR	Čl. I za bod 49. V Čl. I za bod 49. odporúčame vložiť nový bod 50., ktorý znie: „V	O	A	

	prílohe č. 1, v sektore „2. Doprava“, podsektore „Železničná doprava“, v stĺpci „Prevádzkovateľ služieb“ sa za slová „ktoré zabezpečujú len trakciu“ vkladajú slová „to neplatí pre podniky zabezpečujúce trakciu pre trolejbusovú a električkovú dráhu,“.			
MDaVSR	Čl. IV úvodná veta V Čl. IV úvodná veta odporúčame za slovami „č. 62/2020 Z. z.“ slovo „a“ nahradiť čiarkou a za slová „č. 119/2020 Z. z.“ vložiť slová „a zákona č. 242/2020 Z. z.“.	O	A	
MDaVSR	Čl. IV v poznámke pod čiarou V Čl. IV v poznámke pod čiarou odporúčame slovo „46h“ nahradiť slovom „46i“.	O	A	
MDaVSR	Čl. V V Čl. V odporúčame doplniť dátum účinnosti predmetného návrhu zákona.	O	A	
MDaVSR	doložke vybraných vplyvov V doložke vybraných vplyvov v časti 9. „Vplyv navrhovaného materiálu“, v odseku „Vplyv na rozpočet verejnej správy“ predkladateľ uvádza „Pozitívny vplyv na rozpočet verejnej správy“. Odporúčame predkladateľovi presnejšie kvantifikovať o akú úsporu ide a zároveň odporúčame zahrnúť do tejto kalkulácie vplyv na rozpočet verejnej správy z pôvodného MPK k zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov.	O	ČA	
MDaVSR	dôvodovej správe, časť B. Osobitná časť V dôvodovej správe, časť B. Osobitná časť, k bodom 49 až 53 odporúčame doplniť odôvodnenie bodu 51.	O	A	

MDaVSR	Predkladacej správe Znenie Predkladacej správy odporúčame zosúladiť s Legislatívnymi pravidlami vlády Slovenskej republiky. Odporúčame vypustiť zhrnutie vybraných vplyvov, keďže uvedené je obsahom Všeobecnej časti dôvodovej správy.	O	A	
MFSR	K čl. I K bodu 7 (§ 3) 1. Do vymedzenia základných pojmov v § 3 odporúčame doplniť definíciu pojmu „automatizovaný spôsob“, pretože nie je definovaný z hľadiska vecného ani z hľadiska technického. 2. V písmene t) odporúčame slová „alebo údržbu“ nahradiť čiarkou a slovami „údržbu alebo zrušenie“ z dôvodu popísania celého životného cyklu procesu.	O	N	doplnené do DS aj do príslušného ustanovenia.
MFSR	K čl. I K bodu 14 (§ 9 ods. 2) a bodu 18 (§ 13 ods. 6) 1. Navrhovaným ustanovením (§ 9 ods. 2) sa upúšťa od povinnosti zriadiť a prevádzkovať vlastnú akreditovanú jednotku CSIRT a zakladá sa povinnosť využívať Národnú jednotku CSIRT. Povinné využívanie Národnej jednotky CSIRT bez alternatívy môže spôsobiť organizačné problémy, pretože niektoré ústredné orgány sú v súčasnosti v procese vytvárania vlastnej akreditovanej jednotky CSIRT podľa doteraz platného zákona. Žiadame ponechať možnosť ústredným orgánov zriadiť a prevádzkovať vlastné jednotky CSIRT, a to ponechaním pôvodnej formulácie s pripojením slov „alebo môže využívať Národnú jednotku CSIRT“. 2. V súvislosti s pripomienkou v bode 1 žiadame vypustiť novelizačný bod 18 (§ 13 ods. 6).	Z	A	
MFSR	K čl. I K bodu 27 (§ 20 ods. 3) 1. Odporúčame zvážiť vypustenie tohto novelizačného bodu. Upozorňujeme, že navrhované znenie je nekompatibilné s § 5 až 7	O	N	

	vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. 2. V písmene g) odporúčame vypustiť slová „hodnotenia zraniteľností a“, pretože hodnotenia zraniteľností sú súčasťou riadenia rizík, ktoré sú uvedené v písmene b).			
MFSR	K čl. I K bodu 19 (§ 17 ods. 1) 1. Slová „odo dňa, keď k prekročeniu došlo“ žiadame nahradiť slovami „odo dňa, keď prekročenie zistil“, tak ako je to uvedené v platnom znení zákona, pretože navrhované znenie je časovo a procesne nerealizovateľné.	Z	A	text primerane preformulovaný
MFSR	K čl. I K bodu 28 .§ 20 ods. 4 písm. a). 1. Určenie manažéra kybernetickej bezpečnosti je nová rola pre prevádzkovateľa základnej služby, doteraz organizačne neupravená (na úrovni zamestnanca alebo organizačného útvaru). Takáto rola bude mať podľa povinných požiadaviek na ňu kladených za následok potrebu organizačných opatrení, systemizačných opatrení a infraštruktúrnych zmien v internej komunikácii prevádzkovateľa základnej služby. Vzhľadom na skutočnosť, že na túto úpravu sa nevzťahuje žiadne prechodné ustanovenie a ani v doložke vplyvov nie je odhadovaný vplyv tohto opatrenia na rozpočet verejnej správy, možno predpokladať problémy pri implementácii predmetného ustanovenia. Odporúčame ustanoviť prechodné obdobie. Zároveň je potrebné upraviť v doložke vplyvov vplyvy na rozpočet verejnej správy, pretože sa táto úprava týka všetkých orgánov verejnej moci, ktoré sú prevádzkovateľmi základnej služby. 2. Odporúčame špecifikovať, aké znalostné štandardy sa vyžadujú od manažéra kybernetickej bezpečnosti (napríklad odkazom na príslušný právny	O	N	Nejde o novú funkciu, manažér KB je ustanovený vo vyhláške č. 362/2018 ZZ.

	predpis, ktorý tieto znalostné štandardy upravuje). V tejto súvislosti upozorňujeme na § 5 písm. a) štvrtý bod vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, kde sa uvádza, že manažér kybernetickej bezpečnosti musí spĺňať „znalostné štandardy na funkciu manažéra kybernetickej bezpečnosti podľa osobitného predpisu“ (bez odkazu na príslušný právny predpis).			
MFSR	Všeobecne 1. V doložke vybraných vplyvov (ďalej len „doložka vplyvov“) sa uvádza, že návrh má pozitívny vplyv na rozpočet verejnej správy. V analýze vplyvov na rozpočet verejnej správy, na zamestnanosť vo verejnej správe a financovanie návrhu (ďalej len „analýza vplyvov“) však tieto vplyvy nie sú kvantifikované. Pozitívny vplyv bude mať podľa predkladateľa výber pokút podľa sadzieb ustanovených návrhom zákona a výber správnych poplatkov za konanie súvisiace s certifikáciou kybernetickej bezpečnosti. V analýze vplyvov sa uvádza, že negatívne vplyvy na rozpočet verejnej správy sa nepredpokladajú. V bode 2.1.1. Financovanie návrhu sa konštatuje, že v súčasnosti neboli zaregistrované negatívne vplyvy na rozpočet verejnej správy, na zamestnanosť vo verejnej správe, ako aj na samotné financovanie návrhu. Zároveň sa tiež uvádza, že financovanie predmetných výdavkov bude zabezpečené v rámci limitov rozpočtu verejnej správy na príslušné rozpočtové roky. V bode 2.2.4. Výpočty vplyvov na verejné financie sa uvádza, že návrh môže mať eventúálne v konečnom dôsledku aj znížené nároky na rozpočet orgánov verejnej moci, ktoré nebudú musieť plniť úlohy	Z	ČA	Po vzájomnej dohode predkladateľ do doložky vybraných vplyvov bodu 10. Poznámky doplnil konštatovanie, že „Realizácia úloh vyplývajúcich z novely zákona o kybernetickej bezpečnosti bude zabezpečená v rámci schválených limitov výdavkov dotknutých subjektov rozpočtu verejnej správy a zároveň si nevyžiada dodatočné zdroje zo štátneho rozpočtu na osobné výdavky a počet zamestnancov v dotknutých kapitolách ŠR a teda aj v kapitole NBÚ.“ Rozpor bol odstránený.

	jednotky CSIRT. Upozorňujeme, že pri príprave návrhu rozpočtu verejnej správy na roky 2021 až 2023 kapitola Národného bezpečnostného úradu v rámci priorit žiadala zvýšené výdavky v sume 680 tis. eur na roky 2021 až 2023 každoročne na udržateľnosť projektu „Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe“. Prostriedky majú byť určené na dobudovanie a zvýšenie kapacít infraštruktúr Národného centra kybernetickej bezpečnosti SK-CERT, ako aj na dobudovanie špecializovaných pracovísk pre komplexné riešenie riadenia incidentov podľa legislatívne vymedzených kompetencií a zákonných povinností jednotiek CSIRT. Aj iné rezorty (napríklad Ministerstvo zahraničných vecí a európskych záležitostí SR, Ministerstvo investícií, regionálneho rozvoja a informatizácie SR, Slovenská informačná služba) požadovali pri príprave návrhu rozpočtu verejnej správy na roky 2021 až 2023 navýšenie výdavkov na kybernetickú bezpečnosť, pričom sa odvolávali na zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. V nadväznosti na uvedené návrh môže zakladať negatívny vplyv na rozpočet verejnej správy, a preto žiadame predložiť finančnú kvantifikáciu podľa jednotlivých subjektov verejnej správy a zdrojového krytia a tiež uviesť potencionálnu úsporu výdavkov (vrátane počtu zamestnancov) vyplývajúcu zo zrušenia povinnosti zriaďovať a prevádzkovať vlastnú akreditovanú jednotku CSIRT podľa dotknutých kapitol štátneho rozpočtu.			
MFSR	K čl. I K bodu 21 (§ 17ods. 7 a 8) 1. Žiadame odsek 7 vypustiť ako nadbytočný, prípadne odsek 8 preformulovať takto: „(8) Úrad rozhodne o výmaze do 30 dní po doručení súhlasného stanoviska od ústredného orgánu	Z	N	Text vypustený. Rozpor odstránený.

	zodpovedného za sektor, v ktorom je prevádzkovateľ služby vedený.“. Prevádzkovateľ je zodpovedný za kontrolu, či prekročil kritériá, t. j. či došlo k nahláseniu do zoznamu (vtedy Národný bezpečnostný úrad nežiada hodnoverný dôkaz o tom, že prekročil kritériá). Ak prevádzkovateľ zistí, že kritéria na zaradenie do zoznamu už nespĺňa, tak požiada Národný bezpečnostný úrad o výmaz zo zoznamu a ten ho zo zoznamu vymaže.			
MFSR	K čl. I K bodu 19 (§ 17 ods. 1) 2. Na základe zákonnej požiadavky uvedenej v § 17 ods. 1 odporúčame dopracovať identifikačné kritériá prevádzkovanej služby vo vyhláske Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby) pre sektor Bankovníctvo, prevádzkovateľ služieb „správcovia, prevádzkovatelia a osoby zabezpečujúce činnosti Štátnej pokladnice podľa zákona č. 291/2002 Z. z. o Štátnej pokladnici a o zmene a doplnení niektorých zákonov v znení neskorších predpisov“, pretože inak bude táto zákonná požiadavka pre dotknutých prevádzkovateľov služieb nevykonateľná.	O	A	
MFSR	K čl. I K bodu 21 (§ 17ods. 7 a 8) 2. V prípade ponechania § 17 ods. 7 a 8 v navrhovanom znení upozorňujeme na skutočnosť, že splnenie tejto zákonnej požiadavky bude vykonateľné pre všetky prevádzkované služby za predpokladu, že sa upraví vyhláska Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby), tak aby boli popísané identifikačné kritériá pre všetky prevádzkované služby okrem tých, ktoré sú zaradené medzi prvky kritickej infraštruktúry.	O	N	text vypustený

MFSR	Všeobecne 2. Žiadame doložku vplyvov doplniť tak, že pred presunom plnenia úloh medzi Národnou jednotkou CSIRT a jednotkami jednotlivých orgánov verejnej moci bude spracované porovnanie alternatív z pohľadu nákladovej efektívnosti. Návrh ruší povinnosť plniť úlohu jednotky CSIRT jednotlivými orgánmi verejnej moci s možnosťou presunu kompetencií na Národnú jednotku CSIRT. Podľa doložky vplyvov nie je v súčasnosti možné určiť pozitívny vplyv alebo negatívny vplyv na rozpočet verejnej správy. Žiadame, aby bola pred jednotlivými rozhodnutiami o spôsobe výkonu služieb porovnaná ekonomická efektívnosť oboch alternatív.	Z	ČA	Po vzájomnej dohode predkladateľ do doložky vybraných vplyvov doplnil, že konštatovanie, že ekonomické porovnanie relevantných alternatív bude spracované v budúcnosti, pred presunom plnenia úloh, nie plošne pri predložení návrhu.
MFSR	K čl. I K bodu 14 (§ 9 ods. 2) a bodu 18 (§ 13 ods. 6) 3. V § 9 ods. 2 zároveň odporúčame za slová „to neplatí pre podsektor Obrana a podsektor Informačné systémy verejnej správy“ doplniť slová „v sektore 10. Verejná správa“. V bode 52 prílohy č. 1 sa názov sektora „10. Verejná správa“ priamo uvádza pri vypustení podsektora Spravodajské služby, a preto odporúčame uvedené zosúladiť.	O	N	
MFSR	Všeobecne 3. V doložke vybraných vplyvov žiadame uviesť spôsob určenia výšky správneho poplatku 1 000 eur za podanie žiadosti o akreditáciu a certifikáciu kybernetickej bezpečnosti a doplniť očakávané pozitívne vplyvy na rozpočet verejnej správy. Z predloženého materiálu nie je zrejmé, akým spôsobom bola určená výška správneho poplatku 1 000 eur za podanie žiadosti o akreditáciu CSIRT a podanie žiadosti o certifikáciu produktu, služby a procesu. Je potrebné doplniť, či ide o expertný odhad, sumu určenú na základe skúseností z iných krajín alebo podobne. Zároveň je	Z	A	Pozitívny vplyv na rozpočet verejnej správy nebude vyčíslený, keďže reálny počet žiadostí nie je možné predikovať. Suma predstavuje reálny náklad. MF SR akceptovalo nemožnosť vyčíslenia pozitívneho vplyvu na rozpočet verejnej správy.

	vhodné doplniť očakávané počty žiadostí, aby sa dal kvantifikovať pozitívny vplyv na rozpočet verejnej správy.			
MFSR	Všeobecne 4. Odporúčame, aby návrh reflektoval dokument s názvom „Súbor spoľahlivých a komplexných opatrení pre koordinovaný prístup EÚ k bezpečným sieťam 5G“, ktorý vypracovala Európska komisia - Generálne riaditeľstvo pre komunikačné siete, obsah a technológie (DG CONNECT). Siete 5G budú v budúcnosti tvoriť základ digitálnej infraštruktúry Slovenska. Zákon upravujúci oblasť kybernetickej bezpečnosti by nemal v súčasnosti ignorovať kľúčové otázky bezpečnosti tejto infraštruktúry, pričom najlepšia prax v tejto oblasti sa nachádza vo vyššie citovanom dokumente Európskej komisie. Možno sa domnievať, že nedostatky v tejto oblasti môžu viesť k problémom s využívaním fondov EÚ určených na digitalizáciu a spomaliť ich implementáciu.	O	A	
MFSR	Všeobecne 5. Upozorňujeme, že problematika riešená v návrhu zákona je aj obsahom vykonávacích právnych predpisov, pričom predložený materiál neobsahuje návrh zmien týchto vykonávacích právnych predpisov. Ide najmä o vyhlášku Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení a vyhlášku Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby). Návrh zákona upravuje zavedenie bezpečnostných požiadaviek pre všetky informačné systémy verejnej správy (ďalej iba „ISVS“) podľa zákona č. 69/2018 Z. z. o kybernetickej	O	A	vykonavacie predpisy budú novelizované

	bezpečnosti a o zmene a doplnení niektorých zákonov. Odporúčame návrh zákona prepracovať tak, že ISVS sa budú rozdeľovať na základe identifikačných kritérií ustanovených vo vyhláške Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby). ISVS, ktoré nespĺnia uvedené kritériá, sa budú zabezpečovať podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a ISVS, ktoré spĺnia uvedené kritériá sa budú zabezpečovať podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe, resp. na základe vyhlášky č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy. V tejto súvislosti odporúčame vypustenie § 3 písm. k) druhého bodu a § 17 ods. 3 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti z dôvodu, aby sa nemuseli všetky ISVS zabezpečovať na rovnakej úrovni ako kritická infraštruktúra. ISVS, ktoré neobsahujú citlivé informácie ani nespĺňajú žiadne identifikačné kritériá, by museli byť na základe zákona o kybernetickej bezpečnosti chránené rovnako, ako kritická infraštruktúra, čo je v rozpore s dobrou praxou, kedy vynaložené prostriedky na ochranu nemajú byť vyššie ako možné straty. Zároveň sa na ISVS vzťahujú bezpečnostné opatrenia podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe.			
MFSR	Všeobecne 6. Návrh je potrebné zosúladiť s prílohou č. 1 Legislatívnych pravidiel vlády SR (ďalej len „príloha LPV“) [napríklad v čl. I úvodnej vete slová „neskorších predpisov“ nahradiť slovami „zákona č. 373/2018 Z. z. a zákona č. 134/2020 Z. z.“ v súlade s	O	A	

bodom 28.1 prílohy LPV, v bode 3 slová „vypúšťa citácia:“ nahradiť slovami „vypúšťajú citácie“, v bode 10 § 5 ods. 1 písm. y) slová „osobitných predpisov10aa“ nahradiť slovami „§ 27a“ a vypustiť poznámku pod čiarou k odkazu 10aa ako nadbytočnú, v bode 20 slová „2, 3 a 4“ nahradiť slovami „2 až 4“, v bode 23 slovo „dvanástich“ nahradiť číslom „12“ v súlade s bodom 6 prílohy LPV, v bode 24 § 19 ods. 2 na konci vypustiť slovo „zákona“ a na konci novelizačného bodu pripojiť vetu: „Poznámka pod čiarou k odkazu 23 sa vypúšťa.“, v bode 28 úvodnú vetu preformulovať takto: „V § 20 ods. 4 sa vkladá nové písmeno a), ktoré znie:“, v bode 33 poznámke pod čiarou k odkazu 28a vypustiť poslednú citáciu, v bode 35 na konci pripojiť vetu: „Poznámka pod čiarou k odkazu 31 sa vypúšťa.“, v bode 36 § 29 ods. 4 vypustiť slová „podľa osobitného predpisu“ ako nadbytočné a v poznámke pod čiarou k odkazu 31d slová „zákona č. 513/1991 Zb.“ nahradiť slovami „Obchodného zákonníka“, v bode 39 úvodnej vete slová „ods. 5“ nahradiť slovami „odsek 5“ v súlade s bodom 30.3 prílohy LPV, v bode 40 poslednej vete slovo „písmená“ nahradiť slovom „odseky“, v bode 42 § 31a ods. 2 úvodnej vete slovo „tento“ vypustiť ako nadbytočné, v bode 50 slovo „ktorý“ nahradiť slovami „ktoré“, v čl. II, ktorým sa navrhuje rozšíriť Sadzobník správnych poplatkov o novú časť XXV. s názvom Kybernetická bezpečnosť odporúčame namiesto novej časti XXV. zvážiť možnosť zaradenia nových správnych poplatkov pod časť XX. Dôveryhodné služby za položku 268 ako novú položku 268a, prehodiť poradie novelizačných článkov III a IV, aby bolo zachované chronologické poradie novelizovaných zákonov, v čl. III bode 1 v poznámke pod čiarou k odkazu 21 uviesť konkrétne ustanovenie zákona č. 69/2018 Z. z. a na konci novelizačného bodu pripojiť vetu: „Poznámka pod čiarou k			
--	--	--	--

	odkazu 20 sa vypúšťa.“, v súvislosti s vypustením § 21 až 23 v bode 4 je potrebné upraviť vnútorné odkazy v § 29 ods. 1 písm. a) a § 33 ods. 5 platného zákona, v bode 5 na konci pripojiť vetu: „Doterajšie písmená j) a k) sa označujú ako písmená i) a j), v čl. IV úvodnej vete vypustiť slová „mení a“, pretože návrhom sa platné znenie zákona iba dopĺňa, v čl. V doplniť chýbajúci dátum nadobudnutia účinnosti návrhu zákona].			
MFSR	K čl. III (novela zákona č. 95.2019 Z. z.) K bodu 2 (§ 19) Odporúčame § 19 zo zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe nevypúšťať, ale zosúladiť jeho znenie so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti. Napríklad podľa § 19 ods. 1 písm. b) zákona č. 95/2019 Z. z. sa požaduje, aby riadiaca, výkonná a kontrolná zložka systému riadenia bezpečnosti boli navzájom personálne a kompetenčne oddelené, pričom zákon č. 69/2018 Z. z. neobsahuje takúto požiadavku. Znenie oboch zákonov by malo byť zosúladené, pričom upozorňujeme, že v niektorých štátnych inštitúciách nie je možné oddeliť tieto zložky bez navýšenia stavu zamestnancov. K bodu 3 /§ 20 ods. 1 písm. c)/ V písmene c) odporúčame za slovo „realizáciu“ vložiť slovo „relevantných“. Pri nadobúdaní alebo vytváraní informačného systému verejnej správy môžu byť niektoré bezpečnostné požiadavky irelevantné v rozsahu, v akom sú uvedené v osobitnom predpise. K bodu 4 (§ 21 až 23) Ustanovenia § 21 až 23 odporúčame nevypúšťať, ale upraviť ich tak, aby boli súladné s vyhláškou č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy. Táto pripomienka súvisí so všeobecnou pripomienkou, ktorou navrhujeme rozdelenie bezpečnostných	O	A	text preformulovaný aj s ohľadom na iné vznesené pripomienky

	požiadaviek pre informačné systémy verejnej správy podľa toho, či spĺňajú alebo nespĺňajú identifikačné kritériá ustanovené v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti.			
MFSR	Nad rámec návrhu Odporúčame do čl. I vložiť nový novelizačný bod v tomto znení: „.... § 28 sa dopĺňa odsekom 4, ktorý znie: „(4) Postupom podľa odseku 1 nie je dotknutý výkon kontroly a auditu podľa osobitného predpisu.x)“.“ Poznámka pod čiarou k odkazu x) znie: „x) Napríklad zákon č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.“ Ministerstvo financií SR a Úrad vládneho auditu, ako auditujúce orgány podľa § 2 písm. k) zákona č. 357/2015 Z. z. o finančnej kontrole a audite vykonávajú vládny audit, ktorého cieľom je podľa § 10 ods. 2 citovaného zákona, okrem iného, aj overenie a hodnotenie bezpečnosti a funkčnosti informačných systémov, primeranosť a úplnosť informácií, ktoré informačný systém obsahuje. Doplnením navrhovaného ustanovenia sa precizujú kompetencie jednotlivých kontrolných orgánov.	O	A	
MFSR	K čl. I K bodu 25 .§ 19 ods. 6 písm. e). Odporúčame vypustiť slová „alebo Policajnému zboru“, pretože postačuje oznámenie orgánu činnému v trestnom konaní.	O	A	
MFSR	K čl. I K bodu 1 .§ 2 ods. 2 písm. d). Upozorňujeme, že doterajšie platné znenie písmena d) zahŕňa aj ochranu infraštruktúry finančného sektora, preto odporúčame do dôvodovej správy doplniť dôvod vypustenia jej ochrany.	O	A	
MFSR	K čl. I K bodu 24 (§ 19 ods. 2)	O	N	

	V odseku 2 odporúčame nahradiť slovo „prevádzkovateľa“ slovami „týkajúcich sa prevádzkovanej“. Prevádzkovateľ základnej služby môže využívať siete a informačné systémy tretích strán, ktoré nie sú naviazané na základnú službu a teda nie je dôvod, aby spĺňali rovnaké bezpečnostné požiadavky.			
MFSR	K čl. I K bodu 33 (§ 27a) V odseku 8 žiadame doplniť celý postup alebo odkaz na právne predpisy, na základe ktorých bude poškodená strana požadovať náhradu škody.	Z	A	Text preformulovaný. Zodpovednosť za náhradu škody je jednak formulovaná (pri rozhodnutiach úradu) v § 12 ods. 5 platného znenia a následne za rozhodnutie na základe vykonateľného rozhodnutia iného orgánu verejnej moci zodpovedá konkrétny orgán verejnej moci podľa predpisov, na základe ktorých rozhodnutie vydal. Pre lepšiu prehľadnosť textu úrad doplnil konštrukciu zodpovednosti aj do ustanovenia o blokovaní.
MFSR	K čl. I K bodu 32 .§ 27 ods. 1 písm. e). Znenie písmena e) žiadame preformulovať takto: „e) rozhodnutím zakázať alebo obmedziť prevádzkovateľovi základnej služby používať konkrétny produkt, proces alebo službu, ak je produkt, proces alebo služba preukázateľne zdrojom bezpečnostného incidentu a zároveň je to potrebné na zaistenie kybernetickej bezpečnosti alebo z dôvodov bezpečnostného záujmu Slovenskej republiky a ak to nebude mať negatívny vplyv na poskytovanie samotnej základnej služby.“. Podľa definície navrhovanej v bode 7 /§ 3 písm. r)/ je produktom „prvok alebo skupina prvkov siete alebo informačného systému“. Nie je zrejmé, čo nastane, ak je produktom	Z	N	text preformulovaný aj s ohľadom na iné vznesené pripomienky. Vysvetlené. Rozpor odstránený.

	poskytovaná základná služba a zakázaním sa prestane poskytovať. Upozorňujeme, že môžu vzniknúť škody voči zmluvným používateľom (tretím stranám). Zakázaním používania produktu, ktorý je prevádzkovateľom základnej služby alebo prevádzkovateľom kritickej infraštruktúry môže dôjsť k znefunkčneniu poskytovania služby štátu. Návrh nerieši, kto znáša následky „vypnutia“ služby (Národný bezpečnostný úrad ako orgán, ktorý rozhodol o zakázaní služby alebo prevádzkovateľ). Upravená je iba časť problematiky v bode 33 (§ 27a ods. 8). Táto pripomienka bola uplatnená už pri tvorbe pôvodného zákona o kybernetickej bezpečnosti a Národný bezpečnostný úrad ju neakceptoval.			
MFSR	K čl. I K bodu 22 (§ 18 ods. 4) Žiadame slová „odo dňa prekročenia“ nahradiť slovami „odo dňa, keď prekročenie zistil“, tak ako je to uvedené v platnom znení zákona, pretože prevádzkovateľ nevie, kedy prekročil kritériá. Prevádzkovateľ by musel robiť neustále analýzu dát, čo je nerealizovateľné.	Z	A	
MHSR	K navrhovanému § 27a - odseku 7 Ak osoba nevykoná blokovanie podľa určenia úradu, tak ho vykoná úrad alebo to zabezpečí úrad cez tretí subjekt, s čím sa nestotožňujeme a žiadame odsek 7 vypustiť alebo upraviť. Odôvodnenie: Úrad prekračuje svoje právomoci, pričom celá zodpovednosť zostáva na prevádzkovateľovi systému alebo poskytovanej základnej služby podľa osobitných predpisov alebo zmluvy. Závažnosť a dôsledky spôsobené odstavením služby môže posúdiť len kompetentný orgán/prevádzkovateľ a nie úrad. Podobne ako v predchádzajúcom odseku sa okrem orgánu verejnej moci uvádza aj iná osoba, ktorá nie je definovaná. V zmysle znenia by	Z	N	Zabezpečiť riadny spôsob blokovania, tak, aby sa škodlivá aktivita alebo obsah nemohli šíriť ďalej je základným predpokladom úspešného blokovania. Bez toho by mohlo dôjsť k špekulatívnym spôsobom vyhýbania sa a k nedostatočnému zamedzeniu takejto aktivity.

	mohlo ísť o akúkoľvek osobu.			
MHSR	K čl. I bod 10 Navrhujeme nahradiť znenie § 5 ods. 1 písm. y) znením: „y) spolupracuje s inými subjektmi pri blokovaní škodlivého obsahu alebo škodlivej aktivity v kybernetickom priestore Slovenskej republiky alebo škodlivého obsahu alebo škodlivej aktivity smerujúcej do kybernetického priestoru Slovenskej republiky alebo z kybernetického priestoru Slovenskej republiky (ďalej len „blokovanie“) v rozsahu podľa § 27a,“. Odôvodnenie: V čl. I v novelizačnom bode 10 sa navrhuje doplnenie písmena y) do § 5 ods. 1 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Znenie tohto ustanovenia vrátane poznámky pod čiarou ku vkladnému odkazu 10aa) vychádza z návrhu zákona o dohľade v oblasti ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov, ktorý bol predložený do legislatívneho procesu v priebehu roka 2019, avšak nebol schválený. Uvedený návrh právneho predpisu sa pripravoval v gescii Ministerstva hospodárstva SR, ktoré po prehodnotení aktuálnej legislatívy v oblasti ochrany spotrebiteľa dospelo k záveru o začlenení tohto návrhu do pripravovaného nového zákona o ochrane spotrebiteľa, v ktorom sa spoja hmotnoprávne ustanovenia a procesnoprávne ustanovenia upravujúce základné inštitúty ochrany spotrebiteľa, čím sa dosiahne prehľadnejšia úprava spotrebiteľského práva v súlade s Programovým vyhlásením vlády SR na obdobie rokov 2020-2024. Návrh zákona o ochrane spotrebiteľa je v štádiu prípravy. Podľa bodu 22.11 Legislatívnych pravidiel vlády SR nemožno v poznámke pod čiarou uvádzať predpisy, ktoré nie sú platné. Okrem obsahu poznámky pod čiarou však máme výhrady aj	O	ČA	

	k samotnému zneniu návrhu písmena y), v ktorom sa uvádza len „opatrenie o blokovaní“, zatiaľ čo v návrhu § 27a, ktoré bližšie upravuje blokovanie, sa už ako podklad pre rozhodnutie NBÚ spomína akékoľvek vykonateľné rozhodnutie iného subjektu podľa osobitného predpisu. Návrh zákona o dohľade v oblasti ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov zamýšľal blokovanie online rozhrania v dvoch podobách – vo forme predbežného opatrenia o blokovaní, ale tiež vo forme sankcie za porušenie povinnosti uloženej meritórnym rozhodnutím. Tento koncept bude pravdepodobne premietnutý aj do pripravovaného nového zákona o ochrane spotrebiteľa. Ponechanie navrhovaného reštriktívneho znenia návrhu § 5 ods. 1 písm. y) by preto do budúcnosti mohlo vyvolávať aplikačné problémy. Pro futuro je návrh § 27a a s ním priamo súvisiaci § 5 ods. 1 písm. y) (mechanizmus spolupráce vo veciach blokovania) potrebným ustanovením pre zabezpečenie výkonu blokovania online rozhrania na účely ochrany spotrebiteľa (v súlade s čl. 9 ods. 4 písm. g) nariadenia (EÚ) 2017/2394 v platnom znení), ale aj na účely zabezpečenia ochrany vnútorného trhu pred nebezpečnými výrobkami (v súlade s čl. 14 ods. 4 písm. k) nariadenia (EÚ) 2019/1020). Úprava blokovania v zákone o kybernetickej bezpečnosti je preto z nášho pohľadu potrebná a vítaná. Máme však za to, že úprava režimu blokovania a výkonu blokovania na základe žiadosti iného subjektu by mali byť v zákone o kybernetickej bezpečnosti upravené dostatočne konkrétne z dôvodov právnej istoty, ale zároveň tak, aby boli tieto ustanovenia použiteľné tiež pre potreby výkonu blokovania z iných dôvodov, ako je ochrana spotrebiteľa.			
--	--	--	--	--

MHSR	K doložke vybraných vplyvov Odporúčame predkladateľovi, aby dopracoval časť 5. "Alternatívne riešenia" a doplnil zapracovanie pripomienok do časti 13. "Stanovisko komisie pre posudzovanie vybraných vplyvov z PPK" Odôvodnenie: V zmysle obsahových požiadaviek doložky v časti II. Jednotnej metodiky podľa bodu 5. je v rámci alternatívnych riešení potrebné uviesť minimálne nulový variant, t. j. analýzu súčasného stavu. V časti 13. je predkladateľ po doručení stanoviska komisie v rámci PPK povinný doplniť toto stanovisko do doložky, pričom uvedie, ako boli prípadné pripomienky komisie zapracované.	O	N	
MHSR	K Doložke vplyvov Podľa bodov 30-31 predmetného návrhu zákona, kde sa pojednáva spôsob hlásenia kybernetickej bezpečnosti incidentu, môže pre podnikateľov vzniknúť administratívna záťaž, z uvedeného dôvodu tieto skutočnosti odporúčame popísať a vyčíslieť v Analýze vplyvov na PP - negatívny vplyv na PP. - V bode 40 predmetného návrhu sa uvádza sadzba pokuty za nesplnenie zákonnej povinnosti, tzv. priestupky, čo je možné hodnotiť ako potenciálny negatívny vplyv na podnikateľov, z uvedeného dôvodu tieto skutočnosti odporúčame popísať a vyčíslieť v Analýze vplyvov na PP - negatívny vplyv na PP. Odôvodnenie: Podľa Jednotnej metodiky na posudzovanie vybraných vplyvov vzniknú negatívne vplyvy na podnikateľov, ktoré je potrebné vyznačiť a popísať, resp. aj vyčíslieť, aj keď sú len potenciálne. Odporúčame predkladateľovi materiál doplniť Doložku a Analýzu vplyvov pre ich úplnosť, že nepôjde len o pozitívne, ale aj negatívne vplyvy na podnikateľské prostredie.	O	ČA	upravena dovodova sprava
MHSR	k bodu 2 V § 2 v odkaze 6) v poznámke pod čiarou sa vypúšťa zákon č.	O	N	predpis vypustený bez nahradu

	275/2006 Z. z. o informačných systémoch verejnej správy (ISVS). Uvedený neplatný osobitný predpis navrhujeme v písmene e) nahradiť konkrétnym právnym predpisom, napr.: novým zákonom č. 95/2020 Z. z. o IKT, resp. iným právnym predpisom. Odôvodnenie: V poznámke pod čiarou sa vypúšťa zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy (ISVS). Po tejto úprave nie je jasné, o ktorý všeobecne záväzný právny predpis sa jedná a tým pádom, ktoré informačné aktíva do tejto výnimky spadajú. Je viacero zákonov, resp. nariadení EÚ/EK ktoré predpisujú, resp. by mohli predpisovať vyššiu úroveň bezpečnosti týchto informačných aktív systémov (IS), vrátane IS v pôsobnosti alebo dohľade rezortov MV SR, MF SR, MZ SR ... a ďalších.			
MHSR	bod 10 V § 5 sa odsek 1 dopĺňa písmenom y), kde žiadame definovať neznáme pojmy „škodlivý obsah“ alebo „škodlivá aktivita. Odôvodnenie: Textácia „v rámci riešenia opatrení o blokovaní podľa osobitných predpisov 10aa) vydáva rozhodnutie o blokovaní škodlivého obsahu alebo škodlivej aktivity (ďalej len „blokované“) a zabezpečuje vykonanie tohto rozhodnutia.“ obsahuje nedefinované výrazy „škodlivý obsah“ alebo „škodlivá aktivita, pričom sa pod tento pojem dajú subsumovať aj rôzne aktivity, ktoré nemusia mať podstatný význam a na druhej strane aj to, že ich posúdenie úradom môže byť v takom prípade len subjektívne.	Z	A	
MHSR	K navrhovanému § 27a - odseku 6 V druhej časti odseku 6 môže úrad, okrem orgánu verejnej moci, požiadať o spoluprácu aj inú osobu, ktorá je povinná žiadosti vyhovieť, pričom rozhodnutie úradu je konečné, s čím zásadne nesúhlasíme. Odôvodnenie: Úrad, okrem toho, že prekračuje rámec	Z	N	Žiadny štátny orgán nemôže konať podľa ľubovôle. Blokované je nástroj riešenia kybernetického bezpečnostného incidentu. Je dôležité si uvedomiť a rovnako tak vnímať, že nelegálne a

	svojej pôsobnosti vydaním rozhodnutia o blokovani, ukladá povinnosť bezodkladnej spolupráce aj tretím osobám, pričom rozhodnutie úradu je konečné. To znamená, že pri ukladaní pokuty sa neriadi príslušnými ustanoveniami správneho poriadku. Navyše tretia osoba nie je definovaná, čím môže ísť o akúkoľvek osobu určenú podľa ľubovôle úradu, čo považujeme za neprípustné.			škodlivé konanie sa postupne presúva z fyzického sveta do toho kybernetického a v rámci škodlivých aktivít je blokovanie, pozastavenie takejto aktivity jediným nástrojom ako zamedziť paáchaniu škôd nepredvíteľných rozmerov (úlohy OČTK a MO nie sú dotknuté). Spolupráva s inými osobami je nevyhnutná pre riadne zabezpečenie tejto činnosti.
MHSR	bod 14 V náhrade textu v § 9 ods. 2 navrhujeme namiesto slov "využíva Národnú jednotku CSIRT" použiť slová "môže využívať Národnú jednotku CSIRT..." Odôvodnenie V prípade, že ústredný orgán definovaný v § 4 ods.2 písmena b) má alebo si zriadi vlastnú jednotku typu CSIRT/CERT, tak nie je dôvod, aby povinne využíval Národnú jednotku CSIRT. V tomto zmysle je potrebné znenie textu upraviť.	O	A	pripomienka do ucelu akceptovana
MHSR	K čl. I bod 33 V poznámke pod čiarou k odkazu 28a) v § 27a ods. 4 navrhujeme vypustiť odkaz na zákon č. 747/2004 Z. z. v znení neskorších predpisov a na zákon č. .../2020 Z. z. o dohľade v oblasti ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov. Odôvodnenie: Vypustenie zákona č. .../2020 Z. z. o dohľade v oblasti ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov navrhujeme s odvolaním sa na bod 22.11 Legislatívnych pravidiel vlády SR, keďže ide o predpis, ktorý nie je platný. Súčasne navrhujeme aj vypustenie odkazu na zákon č. 747/2004 Z. z. v znení	O	A	

	neskorších predpisov z dôvodu, že Národná banka Slovenska nie je v súčasnosti oprávnená rozhodovať o blokovaní. Udelenie tohto oprávnenia pre Národnú banku Slovenska bolo predmetom osobitného novelizačného článku návrhu zákona o dohľade v oblasti ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov. Pro futuro medzi potenciálnych žiadateľov o blokovanie budú patriť tiež orgány dohľadu v oblasti ochrany spotrebiteľa vrátane NBS. Poznámka pod čiarou k odkazu 28a) obsahuje len demonštratívny výpočet právnych predpisov, pričom oprávnenie príslušných subjektov vydať rozhodnutie o blokovaní musí vychádzať z osobitného predpisu, preto máme za to, že nezahrnutie orgánov dohľadu v oblasti ochrany spotrebiteľa do poznámky pod čiarou k odkazu 28a) nebude znamenať nemožnosť aplikácie § 27a v navrhovanom znení či potrebu opätovnej novelizácie zákona č. 69/2018 Z. z.			
MHSR	K § 27a Blokovanie - odsek 1 Žiadame § 27a odsek 1) zosúladiť s odsekom 1 v § 5 nasledovne: 1) Úrad rozhoduje o blokovaní podľa osobitného predpisu 10aa), spôsobe blokovania a zabezpečuje blokovanie pri riešení kybernetického bezpečnostného incidentu“. Odôvodnenie: Znenie v § 27a odsek 1 nekorešponduje so znením v § 5 ods. 1 písm. y) a preto je potrebné ho zosúladiť. Máme za to, že „rozhodnutie o blokovaní“ môže úrad vydávať len pre IS a siete prevádzkované vo svojej pôsobnosti. Ustanovením úrad získa právomoc rozhodovať o blokovaní a o spôsobe blokovania a vykonávať blokovanie v rámci riešenia kybernetického bezpečnostného incidentu a to ex offio alebo na základe žiadosti iných subjektov, a to bez súhlasu vecne príslušného súdu (ako je to pri blokovaní napr. podľa zákona č.	Z	N	text preformulovaný aj s ohľadom na iné vznesené pripomienky. Blokovanie rozdelené do dvoch samostatných ustanovení. Inštitút blokovania v podobe, akom je predložený, bol predmetom rozsiahlej diskusie aj so zástupcami MHSR v rámci úprav zákona o ochrane o spotrebiteľov v roku 2019. Konštrukcia v odseku 1 predstavuje blokovanie ako nástroj pri riešení závažných kybernetických bezpečnostných incidentoch. § 12 ods. 5 platného znenia je uvedené, že hlásenie kybernetického

	171/2005 Z. z. o hazardných hrách). Náklady na blokovanie a zodpovednosť za škodu súvisiacu s vykonaním blokovania znáša žiadateľ, ak bolo blokovanie vykonané na základe žiadosti, ale v prípade vykonania blokovania NBÚ ex offio tieto náklady a túto zodpovednosť zákon neustanovuje. V tejto súvislosti je potrebné poukázať na §11 návrhu zákona o dohľade v oblasti ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov, ktorý v ods. 8 odkazuje na výkon blokovania podľa osobitného predpisu a to na zákon č. 69/2018 Z. z. nový §27a Blokovanie. Toto ustanovenie je však natoľko všeobecné, že je možné pod jeho výkon subsumovať akúkoľvek aktivitu, nielen aktivitu súvisiacu s ochranou spotrebiteľa. Otázkou je možné zneužitie postavenia úradu, ktorý bude mať nekontrolovateľný nástroj na obmedzovanie podnikania a blokovania doteraz slobodného prístupu na internet (k štátom vybraným internetovým doménam), nakoľko práva dotknutých subjektov sú ochraňované súdnym vstupom, kedy práve súd má byť garantom toho, že nebude blokována internetová doména a teda obmedzená podnikateľská činnosť subjektu, kde na takýto zásah nie sú splnené podmienky.		bezpečného incidentu nikomu nie je na škodu a za prípadnú škodu zodpovedá úrad. Konštatovanie o obsancii zodpovednosti nie je namieste. Následne, v odseku 2 predkladaného znenia sa umožňuje, aby každý, kto má v osobitných právnych predpisoch na účely ochrany práv a právom chránených záujmov uvedenú možnosť blokovať, obmedziť alebo pozastaviť nelegálnu činnosť prebiehajúcu v kybernetickom priestore môže na základe svojho vlastného rozhodnutia požiadať úrad o vykonanie príslušnej aktivity na sieti. Úrad na základe takéhoto rozhodnutia vykoná takéto rozhodnutie odborným spôsobom. za škodu v tomto prípade zodpovedá ten, kto takéto rozhodnutie vydal. V tomto smere navrhované ustanovenie o blokovaní obsahu aj možnosť vopred prerokovať s úradom spôsob a primeranosť takéhoto rozhodnutia. Nejde v žiadnom prípade o "nekontrolovateľný spôsob" výkonu činností. každé rozhodnutie úradu je jednak preskúmateľné súdom a rovnako tak úrad podlieha kontrolej činnosti výboru NRSR.
--	--	--	---

MHSR	 bodu 36 a k doložke vplyvov na podnikateľské prostredie Žiadame do doložky vplyvov uviesť negatívny vplyv na rozpočet verejnej správy a kvantifikovať výšku nákladov na audity, ktoré musia podľa zákona prevádzkovatelia základných služieb vykonať. Taktiež žiadame túto informáciu doplniť do predkladacej správy a dôvodovej správy. Zároveň žiadame doplniť vplyv na podnikateľské prostredie, nakoľko sa v predchádzajúcom bode uvádza, že výkon auditu v oblasti kybernetickej bezpečnosti je podnikaním podľa osobitného predpisu. Zo znenia jasne vyplýva, že právna úprava má vplyv na podnikateľské prostredie, pričom v predkladacej správe a v doložke sa uvádza opak, že nemá žiadny vplyv. Odôvodnenie: Podľa nového odseku 4 v § 29, ktorý znie: “Právnická osoba, vykonáva audit kybernetickej bezpečnosti prostredníctvom certifikovaného audítora kybernetickej bezpečnosti alebo certifikovaných audítorov kybernetickej bezpečnosti. Zabezpečovanie auditu kybernetickej bezpečnosti je podnikaním podľa osobitného predpisu31d). Ak audit kybernetickej bezpečnosti realizuje audítor kybernetickej bezpečnosti prostredníctvom právnickej osoby, zodpovedá za škodu spôsobenú pri výkone auditu kybernetickej bezpečnosti táto právnická osoba.“ audítora kybernetickej bezpečnosti certifikuje úrad, pričom činnosť audítora je podnikateľskou činnosťou. Certifikácia všetkých IS a služieb verejnej správy je povinná a je možné ju vykonať len cez audítora určeného úradom za ustanovené poplatky, a to periodicky, čiže pravidelne v rozsahu 2 rokov a nepravidelne pri každej zmene. Keďže sa v rozsahu verejnej správy jedná o všetky základné služby podľa tohto zákona (zákon č. 69/2018 Z. z o KB, vrátane zákona č. 305/2013 Z. z. o eGovernmente), ide o finančné prostriedky veľkého rozsahu, ktoré budú smerované zo štátneho rozpočtu do súkromného sektoru.	Z	N	Vašu pripomienku nie je možné akceptovať, keďže sa nezavádza žiadny nový inštitút. Povinnosť vykonať audity je daná už od vzniku zákona, takmer dva roky. K tomu je platná a účinná vyhláška (436/2019 ZZ). V návrhu zákona bola v tomto duchu aj predkladaná doložka. Pri tejto úprave ide o legislatívno právnu úpravu, ktorej potreba vznikla praxou.
------	---	---	---	---

	Zároveň poukazujeme na to, že výška celkových nákladov na takúto zákazku nebola doteraz nikde kvantifikovaná. Zo strany úradu sa jedná o sprostredkovanie štátnej zákazky značného finančného rozsahu pre vybrané subjekty.			
MHSR	K navrhovanému § 27a odseku 2 Žiadame formuláciu v § 27a odseku 2) zosúladiť so znením § 5 ods. 1 písm. y) nasledovne: 1) Úrad rozhoduje o spôsobe blokovania a zabezpečuje blokovanie aj na základe žiadosti subjektov podľa osobitných predpisov 28a) (ďalej len „žiadateľ o blokovanie“). Odôvodnenie: Znenie odseku 2 v § 27a nekorešponduje so znením v § 5 ods. 1 písm. y) a je preto potrebné ho zosúladiť. Blokovanie vykonáva tretí subjekt a úrad toto blokovanie bude zabezpečovať, tak ako je uvedené v § 5 ods. 1 písm. y).	Z	A	
MHSR	bod 31 Žiadame v § 24 v doplnenom odseku 7 vypustiť povinnosť zasielania systémových údajov prevádzkovateľa základnej služby úradu v ním ustanovenom rozsahu zo sietí a informačných systémov v prípade, keď sa nejedná o riešenie závažného kybernetického incidentu a zároveň nie sú tieto údaje k riešeniu nevyhnutné. Odôvodnenie: Hromadný zber citlivých systémových údajov od všetkých prevádzkovateľov základných služieb nie je dôvodný a môže narušiť samotnú bezpečnosť citlivých údajov a prevádzku informačných systémov. Zároveň je tým narušený zásadný bezpečnostný princíp „need to know“. Tieto citlivé neverejné informácie sú/majú byť obsahom bezpečnostných projektov, havarijných plánov a obnovy a vnútorných smerníc jednotlivých inštitúcií. Zároveň nie je známy úradom ustanovený ich rozsah, čo znamená, že je to čokoľvek. Úrad však, v prípade oprávnenia, môže	Z	N	text preformulovaný aj s ohľadom na iné vznesené pripomienky

	do nich aj tak nahliadať v prípade výkonu auditu alebo riešenia konkrétneho závažného kybernetického incidentu, ak bol o to požiadaný. Ich hromadný zber mimo príslušného pracoviska je preto neodôvodnený, ako aj rizikový pre konkrétnych prevádzkovateľov a služby nimi prevádzkované.			
MHSR	bodu 32 Žiadame v § 27 v doplnenom odseku 1 vypustiť zákaz používania konkrétneho produktu, procesu alebo služby. Odôvodnenie: Uvedeným rozhodnutím by mohlo byť ohrozené poskytovanie základných služieb verejnej správy, ako aj účelové obmedzenie používania vybraných produktov a služieb prikázané zo strany úradu, v dôsledku čoho by mohli vzniknúť nenahraditeľné materiálne a finančné straty, vrátane strát na životoch a zdraví obyvateľstva. Vyraďenie služby alebo komponentu môže zároveň spôsobiť ochromenie ďalších súvisiacich služieb na tomto prvku závislých, vrátane informačných systémov nespádajúcich pod tento zákon. Zodpovednosť za príslušný sektor je v prípade ohrozenia plne na gestorovi sektoru a prevádzkovateľovi základnej služby, pričom úrad pri dôvodnom zistení môže odporúčať spomenuté obmedzenie. Úrad má na obmedzenie rizikového komponentu alebo služby aj inú možnosť, a to možnosť eliminovať komponent alebo službu na úrovni doménovej štruktúry, nakoľko má v gescii sektor č. 3 digitálnej infraštruktúry, ktorý zahŕňa výmenné uzly internetu, služby systému doménových mien na internete, vrátane správy domén najvyššej úrovne podľa prílohy č. 1 k zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti. Z uvedeného dôvodu považujeme doplnenie odseku v uvedenom znení za zásadne nevhodné a neadekvátne.	Z	N	text preformulovaný aj s ohľadom na iné vznesené pripomienky

MHSR	K navrhovanému §27a - odseku 8 Žiadame znenie v § 27a odsek 8) upraviť tak, aby úrad znášal zodpovednosť v prípade ním vydaného rozhodnutia o spôsobe blokovania. Odôvodnenie: Ak úrad vydal rozhodnutie o spôsobe blokovania, ktoré je zároveň konečné, žiadame ošetriť prípad neúčinného, neadekvátneho/chybného spôsobu blokovania zo strany úradu (časovo, rozsahom a pod.). Úrad má v prípade tohto precedensu niešť zodpovedať za škody spôsobené chybným spôsobom a zabezpečením blokovania a nie prenášať túto zodpovednosť na žiadateľa, ktorý to nemohol ovplyvniť.	Z	ČA	Vami navrhovaný právny predpoklad je upravený v § 12 ods. 5 platného znenia. Text je primerane preformulovaný.
MIRRI SR	K Čl. I bod 33. vlastného materiálu Bod 33. konkrétne navrhovaný § 27a Blokovanie ods. 1 navrhujeme preformulovať nasledovne: "Úrad rozhoduje o blokovaní a spôsobe blokovania a v nevyhnutných prípadoch aj sám vykonáva blokovanie v prípade riešenia bezpečnostného incidentu, pri ktorom škodlivá aktivita alebo škodlivý obsah môže mať negatívny vplyv na kybernetickú bezpečnosť. Blokovanie sa uskutočňuje na dobú nevyhnutne potrebnú k odstráneniu škodlivej aktivity alebo škodlivého obsahu." ODÔVODNENIE: Blokovanie zo strany úradu má byť až sekundárne. Z pohľadu efektívnosti a účelu blokowania, je nutné požadovať blokovanie o zodpovedného subjektu a blokovanie zo strany úradu mať ako krajnú možnosť. Nutnosť obmedziť blokovanie len na najkrajnejšiu možnú mieru. Chýba mi tu aj otázka doby blokowania. Napr. na nevyhnutnú dobu, kedy dôjde k odstráneniu škodlivej aktivity alebo škodlivého obsahu	Z	N	Vysvetlené. Rozpor odstránený.
MIRRI SR	K Čl. I bod 33. vlastného materiálu Bod 33. konkrétne navrhovaný § 27a Blokovanie ods. 2 navrhujeme preformulovať nasledovne: "Úrad rozhoduje o blokovaní, spôsobe	Z	N	Vysvetlené. Rozpor odstránený.

	blokovania a v nevyhnutných prípadoch vykonáva blokovanie aj na základe žiadosti subjektov podľa osobitných predpisov28a) (ďalej len „žiadateľ o blokovanie“). ODÔVODNENIE: V prípade žiadosti je nutné tiež rozhodnúť o dôvode blokovania.			
MIRRI SR	K Čl. I bod 33. vlastného materiálu Bod 33. konkrétne navrhovaný § 27a Blokovanie ods. 8 navrhujeme preformulovať nasledovne: "Ak vydáva úrad rozhodnutie o blokovaní podľa odseku 1, náklady na blokovanie a zodpovednosť za škodu súvisiacu s vykonaním blokovania znáša úrad. Ak vydáva úrad rozhodnutie o blokovaní na základe žiadosti podľa odseku 2, náklady na blokovanie a zodpovednosť za škodu súvisiacu s vykonaním blokovania znáša žiadateľ o blokovanie. " ODÔVODNENIE: Explicitne uvedená zodpovednosť za blokovanie. Vzhľadom na povahu inštitúty a možný zásah do práv fyzických a právnických osôb, je nutné zadefinovať zodpovednosť pre všetky prípady blokovania.	Z	A	
MIRRI SR	K Čl. I bod 33. vlastného materiálu Inštitút blokovania predstavuje pomerne značný zásah do práv fyzických a právnických osôb. Z tohto dôvodu a z uplatňovania princípu právneho štátu je nutné stanoviť presné situácie, kedy je možné blokovanie použiť. V rámci odôvodnenia sa uvádza podvodná stránka, resp. riešenie formy sociálneho inžinierstva phishingu. Tieto incidenty si vyžadujú z pohľadu riešenia kybernetického bezpečnostného incidentu promptné riešenie, čo z pohľadu doručovania rozhodnutia o blokovaní splnené nebude. Aplikčná prax práve naopak ukazuje, že poskytovatelia rôznych služieb pružne reagujú na nahlásenie podvodného obsahu. Je nutné zaviesť zoznam spôsobov blokovania. Rozpísať jednotlivé pravidlá.	Z	A	

	Čo znamená účinnosť, účelnosť a primeranosť blokovania. Je potrebné zaviesť princíp nevyhnutnosti. Úrad by musel vyhodnotiť, či neexistuje aj iné riešenie ako je samotné blokovanie. Ak existuje iný prostriedok, mal by byť použitý a blokovanie by malo predstavovať krajný prostriedok nevyhnutný k zamedzeniu negatívnych dôsledkov. Navrhujeme prijatie vykonávacieho právneho predpisu, ktorý by bližšie stanovoval minimálne proces blokovania vrátane rámcového zadenfinovania pravidiel, spôsoby blokovania, dobu blokovania. Taktiež chýba legálna definícia škodlivej aktivity a škodlivého obsahu.			
MIRRI SR	K Čl. I bod 33 vlastného materiálu Navrhujeme úpravu § 27a ods 6. v zmysle odôvodnenia. ODÔVODNENIE: V zmysle tohto ustanovenia rozhodnutie NBÚ o blokovaní je konečné. Takto definované ustanovenie neumožňuje pre subjekty žiadnu možnosť právnej ochrany v podobe možnosti podania vyjadrenia, vysvetlenia, námietok, prípadne vykonania bezodkladnej účinnej nápravy tak, aby blokovanie nemuselo byť vykonané. Je tiež potrebné zvážiť možné dopady pre tie subjekty, ktorých sa blokovanie týka.	Z	A	
MIRRI SR	K Čl. I bod 33 vlastného materiálu Navrhujeme úpravu § 27a, ktorý ustanovuje novú rozhodovaciu právomoc NBÚ vo veci blokovania pri riešení kybernetického bezpečnostného incidentu. ODÔVODNENIE: Ide o kompetenciu, ktorá zasahuje do činnosti nielen orgánov verejnej moci, ale aj osôb, ktoré sú „prevádzkovateľmi infraštruktúr“, na ktorých sa má blokovanie vykonať. V návrhu absentuje vymedzenie pojmu „prevádzkovateľ infraštruktúry“. Taktiež chýba jednoznačné vymedzenie osobnej pôsobnosti a teda, kto má byť dotknutou	O	N	problematika vyjasnená v zasadných pripomienkach

	osobou, ktorej sa má blokovanie týkať.			
MIRRI SR	K Čl. I bod 10. vlastného materiálu Navrhujeme vypustiť poznámku pod čiarou ktorá znie: „10aa) § 11 zákona č. .../2020 Z. z. o dohľade v oblasti ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov. § 35ea zákona č. 747/2004 Z. z. o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení zákona č. .../2020 Z. z.“ ODÔVODNENIE: Poznámka pod čiarou odkazuje na právne predpisy, ktoré v čase novelizácie predmetného predpisu neexistujú a nie je známy ani obsah odkazovaných ustanovení. V rámci novelizácie predmetného právneho aktu sa zavádza inštitút „blokovanja“. Navrhované ustanovenie definuje pôsobnosť úradu v tejto oblasti a obmedzuje použitie tohto inštitútu na okruh vzťahov, ktoré sú definované v osobitnom predpise, ktorého obsah nie je známy. Nie je teda možné určiť dosah tohto ustanovenia. Z uvedeného dôvodu navrhujeme toto ustanovenie vynechať.	Z	A	
MIRRI SR	K Čl. I bod 46. vlastného materiálu Nesúhlasíme s navrhovaným znením § 32 ods. 2 a navrhujeme ponechať pôvodné znenie ustanovenia § 32 ods. 2, a teda „Ústredný orgán sa v spolupráci s úradom splnomocňuje na vydanie všeobecne záväzného právneho predpisu, ktorým ustanovia sektorové bezpečnostné opatrenia v rozsahu svojej pôsobnosti podľa prílohy č. 1 a v súlade s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti.“ Odôvodnenie: Nie je štandardné, aby sa na vydanie všeobecne záväzných právnych predpisov, ktoré upravujú konkrétny sektor, za ktorý zodpovedá konkrétny orgán verejnej moci vyžadoval súhlas od iného orgánu verejnej moci. Z navrhovaného ustanovenia nie je zrejmé, za akých podmienok bude NBÚ súhlasiť,	Z	A	

	resp. nesúhlasiť s vydaním všeobecne záväzných právnych predpisov. Taktiež je otázne či sa súhlas týka len splnomocnenia na vydanie všeobecne záväzného právneho predpisu, a teda NBÚ už nebude skúmať znenie daného všeobecne záväzného predpisu alebo sa súhlas viaže na samotné vydanie všeobecne záväzného predpisu v tom zmysle, že NBÚ bude skúmať znenie všeobecne záväzného predpisu a až následne udelí súhlas na jeho vydanie.			
MIRRI SR	K Čl. I bod 47. vlastného materiálu Nesúhlasíme s navrhovaným znením § 33 ods. 1. Navrhujeme zmeniť znenie § 33 ods. 1 a to nasledovne: „Na konanie úradu podľa § 13 ods. 7, § 16 ods. 2 a 3, sa nevzťahuje správny poriadok. Na konanie úradu podľa § 17 ods. 6, § 21 ods. 4, § 27 a § 27a sa vzťahuje správny poriadok, pričom rozklad nie je prípustný.“ ODÔVODNENIE:Navrhované znenie § 33 ods. 1 vylučuje aplikáciu správneho poriadku na konanie NBÚ v konkrétnej rozhodovacej činnosti. Navrhované znenie § 33 ods. 1 rozširuje vylúčenie správneho poriadku na celý § 17 a § 21. Dôvod prečo došlo k rozšíreniu vylúčenia správneho poriadku z § 17 ods. 6 a § 21 ods. 4 na celé znenie § 17 a § 21 nie je nijakým spôsobom odôvodnený a len znižuje použitie právnych nástrojov zo strany prevádzkovateľov základných služieb, ktorí by chceli využiť opravné prostriedky v zmysle správneho poriadku. Zatiaľ čo v prípade § 17 ods. 6 (oznámenie o zaradení služby do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb oznám) a § 21 ods. 4 (oznámenie o zaradení služby do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb) NBÚ nevydáva rozhodnutie, v prípade uloženia povinnosti zasielať automatizovaným spôsobom systémové	Z	N	Pripomienka je v časti nad rámec novely. V časti, v ktorej žiadate o aplikovanie Správneho poriadku na inštitút blokovania nie je možné vyhovieť z dôvodov jasne uvedených v rámci vyhodnotenia novelizačného bodu o blokovani. Rozhodnutie je preskúmateľné súdom a musí byť odôvodnené. Pri vykonávaní blokovania na žiadosť orgánu verejnej moci na základe vykonateľného rozhodnutia nie je právne možné aplikovať Vami navrhovaný postup. Vysvetlené. Rozpor odstránený.

	informácie (§ 24 ods. 7) a taktiež o zákaze produktu, procesu alebo služby (§ 27 ods. 1 písm. e) už rozhodnutie vydáva. Pretože v rozhodovacej činnosti NBÚ v konkrétnych konaniach podľa § 17 ods. 6, § 21 ods. 4, § 27 a § 27a dochádza k výraznému zásahu do práv jednotlivých subjektov a sú im ukladané povinnosti, je potrebné, aby mohli tieto subjekty využiť opravné prostriedky v zmysle správneho poriadku, okrem rozkladu.			
MIRRI SR	K Čl. III. bod 2. vlastného materiálu Nesúhlasíme s vypustením § 19 zákona č. 95/2019 o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. ODÔVODNENIE: Vypustenie § 19 spôsobí nevykonateľnosť ostatných ustanovení zákona č. 95/2019 o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, ktoré vyžadujú riešenie kybernetickej bezpečnosti informačných technológií verejnej správy a sú spolu organizačne previazané, vrátane vymedzenia zodpovedností. Vypustenie predmetných ustanovení taktiež spôsobí právnu neistotu v oblasti bezpečnosti informačných technológií verejnej správy a nepriaznivo ovplyvní bezpečnosť informačných systémov verejnej správy, ktoré nie sú základnými službami v zmysle 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Zákon o kybernetickej bezpečnosti ani príslušná sektorová vyhláška nemôže stanoviť zrušené povinnosti správcov informačných systémov verejnej správy.	Z	A	
MIRRI SR	K Čl. III bod 1. vlastného materiálu S úpravou uvedeného ustanovenia zásadne nesúhlasíme. ODÔVODNENIE: V navrhovanej úprave sa navrhuje, aby všetci správcovia postupovali pri prijatí a realizovaní bezpečnostných	Z	A	

	opatrení v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Nie všetci správcovia v zmysle zákona č. 95/2019 o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov sú automaticky aj prevádzkovateľmi základných služieb. Je potrebné aby spĺňali tri kumulatívne kritéria v zmysle smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, ktorými sú: subjekt poskytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností; poskytovanie tejto služby je závislé od sietí a informačných systémov a incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby. Posledné kritérium, a teda incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby je v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov vyjadrený v § 18 a príslušnej vyhláške NBÚ č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby). Pokiaľ sa nebude skúmať či správca naplnil aj dopadové kritéria, nemožno hovoriť o prevádzkovateľovi základnej služby.			
MIRRI SR	K Čl. I. bod 14. vlastného materiálu S uvedenou formuláciou nesúhlasíme a navrhujeme § 9 ods. 2 ponechať v pôvodnom znení. ODÔVODNENIE: Navrhovanou právnou úpravou ústredné orgány prichádzajúci o právo zriadenia vlastnej jednotky CSIRT alebo použitia iných akreditovaných jednotiek CSIRT. Súčasná právna úprava už umožňuje využitie Národnej jednotky CSIRT. Ponechanie súčasného znenia skôr	Z	A	

	pomáha znižovať zaťaženie jednotlivých jednotiek CSIRT (najmä národnej jednotky CSIRT) a dáva priestor pre ústredný orgán, aby si zvolil, akým spôsobom chce zabezpečovať povinnosti v zmysle tejto právnej úpravy.			
MIRRI SR	K Čl. I ods. 31 vlastnému materiálu S uvedenou formuláciou nesúhlasíme. ODÔVODNENIE: Ustanovenie zavádza povinnosť prevádzkovateľa základnej služby zasielať automatizovaným spôsobom určené systémové informácie zo sietí a informačných systémov na základe rozhodnutia úradu. Zavedením tejto povinnosti sa zabezpečuje prenos všetkých relevantných informácií nevyhnutných pre rýchle, efektívne riešenie zistených kybernetických bezpečnostných incidentov. Je potrebné špecifikovať o aké systémové informácie pôjde, nakoľko takto naformulované znenie znie veľmi extenzívne.	O	N	pripomienka nesplna požiadavky legislatívnych pravidiel
MIRRI SR	K Čl. I. bod 18. vlastného materiálu So zmenou daného ustanovenia nesúhlasíme. ODÔVODNENIE: Súvisí s pripomienkou k Čl. I. bod 17.	Z	A	
MIRRI SR	K Čl. I bod 17. vlastného materiálu So zmenou daného ustanovenia nesúhlasíme. ODÔVODNENIE: Z formulácie ustanovenia nie je jasné, či sa danou zmenou rozšíri okruh žiadateľov o akreditáciu, napríklad o súkromné subjekty. V súčasnom znení žiadateľom môže byť len ústredný orgán štátnej správy. Predmetná úprava môže viesť k prechodu personálnej kapacity už existujúcich akreditovaných jednotiek do súkromných jednotiek CSIRT, čím možno očakávať väčšie finančné zaťaženie na zabezpečovanie úloh podľa tohto zákona.	Z	A	

MIRRI SR	K Čl. III bod 3. vlastného materiálu So zmenou uvedeného bodu zásadne nesúhlasíme. ODÔVODNENIE: Nakoľko nesúhlasíme s vypustením § 21 až 23, nesúhlasíme s tým, aby správcovia mali povinnosť zabezpečiť pre informačný systém verejnej správy vypracovanie bezpečnostnej dokumentácie a prijatie a realizáciu bezpečnostných opatrení podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Nie všetci správcovia v zmysle zákona č. 95/2019 o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov sú automaticky aj prevádzkovateľmi základných služieb, a preto im nemožno ukladať povinnosť na základe zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov ak sa na nich tento právny predpis nevzťahuje.	Z	A	
MIRRI SR	K Čl. III bod 4. vlastného materiálu So zmenou uvedenou v tomto bode zásadne nesúhlasíme. ODOVODNENIE: Vypustenie § 21 až 23 spôsobí nevykonateľnosť ostatných ustanovení zákona č. 95/2019 o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, ktoré vyžadujú riešenie kybernetickej bezpečnosti informačných technológií verejnej správy a sú spolu organizačne previazané, vrátane vymedzenia zodpovedností. Vypustenie predmetných ustanovení taktiež spôsobí právnu neistotu v oblasti bezpečnosti informačných technológií verejnej správy a nepriaznivo ovplyvní bezpečnosť informačných systémov verejnej správy, ktoré nie sú základnými službami. V dôvodovej správe k návrhu zákona sa uvádza, že ak budú potrebné prísnejšie opatrenia, budú upravené v sektorovej vyhláške podľa § 32 ods. 2. Lenže sektorová vyhláška sa	Z	A	

	bude týkať len základných služieb a prevádzkovateľov základných služieb zo sektoru Verejná správa a podsektoru Informačné systémy verejnej správy (podľa prílohy č. 1). V tomto prípade ide o základné služby podľa § 3 písm. k) bod prvý zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Podľa jednotného informačného systému kybernetickej bezpečnosti boli v sektore Verejná správa a podsektore Informačné systémy verejnej správy (podľa prílohy č. 1) zaradené 4 základné služby. Avšak vyše 1300 informačných systémov verejnej správy nie je zaradených do zoznamu základných služieb ako základná služba podľa § 3 písm. k) prvého bodu podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov ale ako základná služba podľa § 3 písm. k) druhého bodu podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Takáto sektorová vyhláška by sa nevzťahovala na všetky informačné systémy verejnej správy, a teda bezpečnosť informačných systémov verejnej správy nebude dostatočne upravená. Taktiež, sektorovou vyhláškou nie je možné stanoviť zrušené povinnosti a kompetencie orgánu vedenia orgánov riadenia a správcov informačných systémov verejnej správy.			
MIRRI SR	K Čl. III bod 5. vlastného materiálu So zmenou uvedenou v tomto bode zásadne nesúhlasíme. ODÔVODNENIE: Zrušenie § 31 písm. i) zákona č. 95/2019 o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov zrušenie vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.	Z	A	

	Ak dôjde k zrušeniu § 31 písm. i), Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky stráca kompetenciu pri vydávaní všeobecne záväzných predpisov, ktoré by upravovali bezpečnosť informačných systémov verejnej správy, ktoré nie sú základnou službou v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.			
MIRRI SR	K Čl. I bod 21. vlastného materiálu Uvedený bod navrhujeme preformulovať nasledovne "§ 17 sa dopĺňa odsekmi 7 a 8, ktoré znejú: (8) Úrad rozhodne o výmaze do 30 dní. Ak nemožno vzhľadom na povahu vecí rozhodnúť v lehote podľa predchádzajúcej vety, môže ju úrad predĺžiť najviac o 30 dní. O predĺžení lehoty s uvedením dôvodov je úrad povinný upovedomiť prevádzkovateľa základnej služby, ktorý žiada o výmaz.“ ODÔVODNENIE: Navrhujeme skrátiť pôvodne navrhovanú lehotu na predĺženie rozhodovania NBÚ z pôvodných 60 dní na 30 dní, aby nedochádzalo k zbytočne dlhému rozhodovaniu o výmaze.	O	N	text preformulovaný aj s ohľadom na iné vznesené pripomienky
MIRRI SR	K Čl. I. bod 16. vlastného materiálu Uvedený bod navrhujeme preformulovať nasledovne: "V § 10 odsek 1 znie: (1) Za bezpečnosť sietí a informačných systémov, ktoré nie sú základnou službou a za procesy riešenia kybernetických bezpečnostných incidentov, iný orgán štátnej správy a ústredný orgán v rozsahu svojej pôsobnosti zodpovedajú tým, že môžu prijať a dodržiavať vhodné a primerané bezpečnostné opatrenia podľa § 20.“ ODÔVODNENIE: Iným orgánom štátnej správy a ústredným orgánom nemožno ukladať povinnosť plniť bezpečnostné opatrenia v zmysle § 20. Bezpečnostné opatrenia v zmysle § 20 sú povinní realizovať prevádzkovatelia základných služieb a nie subjekty, ktoré	Z	N	Ponechaný pôvodný text. Rozpor odstránený.

	neboli zaradené registra prevádzkovateľov základných služieb.			
MIRRI SR	K Čl. I bod 22. vlastného materiálu Uvedený bod navrhujeme preformulovať nasledovne: "V § 18 odsek 4 znie: Ak prevádzkovateľ služby podľa prílohy č. 1 prekročí špecifické sektorové kritériá, ak sú určené, oznámi to úradu do 30 dní odo dňa prekročenia, v rozsahu podľa § 17 ods. 5, ak zároveň prekročí dopadové kritériá.“ ODÔVODNENIE: Neexistuje žiaden dôvod, prečo by mal subjekt nahlasovať naplnenie sektorových kritérií, ak nespĺňa dopadové kritériá. V zmysle § 2 vyhlášky NBÚ č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby) platí, že: „prevádzkovaná služba spĺňa identifikačné kritériá základnej služby, ak spĺňa aspoň jedno dopadové kritérium a aspoň jedno špecifické sektorové kritérium, ak je uvedené v prílohe č. 1.“ Taktiež v zmysle smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, musí prevádzkovateľ základnej služby spĺňať tri kumulatívne kritériá, ktorými sú: subjekt poskytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností; poskytovanie tejto služby je závislé od sietí a informačných systémov a incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby. Posledné kritérium, a teda incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby je v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov vyjadrený v § 18 a príslušnej vyhláške NBÚ č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby). Nevyžadovanie	Z	N	Text vypustený. Rozpor odstránený.

	naplnenia dopadového kritéria je jednak v rozpore s vyhláškou č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby), ale najmä v rozpore so smernicou NIS.			
MIRRI SR	K Čl. I ods. 28 vlastnému materiálu Uvedený bod navrhujeme preformulovať nasledovne: "V § 20 ods. 4 písmeno a) znie: a) určenie manažéra kybernetickej bezpečnosti, ktorý je svojím zaradením v organizačnej štruktúre prevádzkovateľa základnej služby nezávislý od riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti pre prevádzkovateľa základnej služby ..." ODÔVODNENIE: Navrhované ustanovenie neprimerane zaťažuje viaceré subjekty spadajúce pod prevádzkovateľov základnej služby. Je nutné určiť, ktorí prevádzkovatelia základnej služby túto povinnosť musia spĺňať a ktorí nie. Napr. pre obec môže takáto povinnosť znamenať neprimerané finančné zaťaženie.	Z	ČA	Text je preformulovaný aj s ohľadom na ostatné vznesené pripomienky. Uvedená konštrukcia zaradenia takejto povinnosti priamo do zákona bola úradu odporúčaná stálou pracovnou komisiou pre technické predpisy v čase prípravy a schvaľovania vyhlášky o bezpečnostných opatreniach. V rámci mpk boli vysporiadané otázky presne tohto charakteru. Organizačné zaradenie funkcie manažéra kybernetickej bezpečnosti nepredstavuje žiadne objektívne znemožnenie riešenia situácií popísaných vo Vašej pripomienke. Ide o formálne určenie funkcie, nie o konkrétne zaradenie konkrétnej osoby. Rovnako je z povahy Vašich vznesených pripomienok dôležité uviesť, že povinnosť určiť manažéra kybernetickej bezpečnosti nie je vyžadovaná pre všetkých PZS. Vo vyhláške č. 362/2018 ZZ sa uvádza, že funkcia určenia manažéra kybernetickej bezpečnosti je povinná pre kategórie sietí a

				informačných systémov III, čo prakticky znamená, že sa týka PZS so složitejšími IS a tými najcitlivejšími údajmi a pre subjekty (ako napríklad malé obce) nie je povinná, ale len odporúčaná. Vysvetlené. rozpor odstránený.
MIRRI SR	K Čl. I bod 32. vlastného materiálu Uvedený bod navrhujeme preformulovať nasledovne: "V § 27 sa odsek 1 dopĺňa písmenom e), ktoré znie: e) rozhodnutím zakázať alebo obmedziť prevádzkovateľovi základnej služby používať konkrétny produkt, proces alebo službu, ak je to potrebné na zaistenie kybernetickej bezpečnosti, alebo z dôvodov bezpečnostného záujmu Slovenskej republiky, ak sa hodnoverným spôsobom možno domnievať, že zákaz alebo obmedzenie konkrétneho produktu, procesu alebo služby zaistí kybernetickú bezpečnosť alebo bezpečnostný záujem Slovenskej republiky. " ODÔVODNENIE: Navrhované ustanovenie zasahuje do voľného pohybu tovaru a služieb podľa čl. 26 ods. 2 Zmluvy o fungovaní Európskej únie (ďalej len „ZoFEU“) vnútorný trh zahŕňa oblasť bez vnútorných hraníc, v ktorej je zaručený voľný pohyb tovaru, osôb, služieb a kapitálu v súlade s ustanoveniami zmlúv. V zmysle ZoFEU je možné obmedziť tento slobodný pohyb v prípade napr. verejnou bezpečnosťou, ale dané obmedzenia musia byť účelné a nesmú byť možnosťou diskriminácie konkrétnych výrobcov, resp. poskytovateľov služieb. Navrhované ustanovenie umožňuje široko koncipované uplatnenie, napr. zakázanie tovaru a služby, ktoré nespôsobili závažný kybernetický bezpečnostný incident, ani nie sú v príčinnej súvislosti so závažným kybernetickým bezpečnostným	Z	ČA	Text preformulovaný tak, aby splňal predpoklady uvedené v pripomienkach. Uvedené ustanovenie predstavuje implementáciu ToolBox a na základe vykonanej analýzy rizík s ohľadom na záujmy štátu umožňuje zakázať, alebo obmedziť používanie určitého výrobku. Momentálne v našej legislatíve neexistuje právny nástroj na výkon takejto činnosti, čo znemožňuje legálnou cestou vyhnúť sa rizikovým dodávateľom, resp. výrobcom. Vysvetlené. Rozpor odstránený.

	incidentom. Z tohto dôvodu navrhujeme zúženie uplatnenia navrhovaného ustanovenia.			
MIRRI SR	K Čl. I bod 45. vlastnému materiálu Uvedený bod navrhujeme preformulovať nasledovne: "V § 32 ods. 1 sa za písmeno f) vkladá nové písmeno g), ktoré znie: g) postupy na manipulovanie s digitálnymi stopami v rámci riešenia kybernetického bezpečnostného incidentu." ODÔVODNENIE: Aplikčná prax ukázala, že je nutné zadefinovať rámcové pravidlá pre prácu s digitálnymi stopami pri riešení kybernetických bezpečnostných incidentov. Rámcovo je nutné zadefinovať pravidlá a postupy pre identifikáciu zariadení s potencionálnymi digitálnymi stopami, spôsob zaistenia, vyťaženia a uchovania digitálnych stôp v zmysle medzinárodných štandardov, napr.: • ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence • ISO/IEC 27040:2015 — Information technology — Security techniques — Storage security • ISO/IEC 27041:2015 — Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method • ISO/IEC 27050:2016+ — Information technology — Security techniques — Electronic discovery	O	N	problematika vyjasnená v zasadných pripomienkach
MIRRI SR	K Čl. I bod 21. vlastného materiálu Uvedený bod navrhujeme preformulovať nasledovne: "§ 17 sa dopĺňa odsekmi 7 a 8, ktoré znejú: (7) Ak prevádzkovateľ služby podľa § 3 písm. l) bod 1 a § 3 písm. l) bod 2 hodnoverným spôsobom preukáže, že nedošlo k prekročeniu identifikačných kritérií prevádzkovej služby podľa § 18, môže požiadať úrad o výmaz." ODÔVODNENIE: V navrhovanom znení môže žiadosť o	Z	N	Text vypustený. Rozpor odstránený.

	výmaz urobiť len prevádzkovateľ služby v sektore podľa prílohy č. 1. V tomto prípade ide v zmysle platného a účinného znenia zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov o základné služby podľa § 3 písm. k) prvého bodu. Avšak navrhované ustanovenie sa netýka základných služieb podľa § 3 písm. k) druhého bodu zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých (základná služba ako informačný systém verejnej správy). Predmetné ustanovenie je diskriminačné a znevýhodňuje prevádzkovateľov základných služieb podľa § 3 písm. k) druhého bodu v zmysle platného a účinného znenia zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.			
MIRRI SR	K Čl. I bod 11. vlastného materiálu Uvedený bod navrhujeme preformulovať nasledovne: "§ 5 sa dopĺňa odsekom 4 ktorý znie: (4) Úrad je oprávnený požadovať od prevádzkovateľov základnej služby, orgánov verejnej moci a právnických osôb poskytnutie súčinnosti, alebo informácií, ktoré sú potrebné na plnenie úloh podľa tohto zákona v nevyhnutnej miere." ODÔVODNENIE: S navrhovaným ustanovením zásadne nesúhlasíme. Je potrebné vymedziť aké informácie budú požadované. Môže ísť aj o osobné údaje, kde v tomto prípade pre ich spracúvanie chýba právny základ. Obsah poskytnutej súčinnosti môže byť v rozpore s režimom bankového tajomstva, telekomunikačného tajomstva. Považujeme za vhodné podotknúť že orgán verejnej moci je širší pojem ako ústredný orgán.	Z	ČA	Text preformulovaný tak, aby spĺňal predpoklady uvedené v pripomienke aj s ohľadom na ostatné vznesené pripomienky k uvedenému bodu. Rozpor odstránený.
MIRRI SR	K Čl. I bod 25. vlastného materiálu Uvedený bod navrhujeme preformulovať nasledovne: "V § 19 ods. 6 písmeno e) znie: e) bezodkladne oznámiť orgánu činnému v	Z	N	Text vypustený. Rozpor odstránený.

	trestnom konaní alebo Policajnému zboru skutočnosti nasvedčujúce tomu, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o nich hodnoverným spôsobom dozvie." ODÔVODNENIE: Povinnosť nahlasovať skutočnosti nasvedčujúce tomu, že bol spáchaný trestný čin bolo potrebné obmedziť na prípady, kedy má povinný subjekt potvrdené hodnoverným spôsobom ich autenticnosť.			
MIRRI SR	K Čl. I bod 29. vlastného materiálu Uvedený bod navrhujeme preformulovať nasledovne: "V § 22 odseky 4 a 5 znejú: (4) Ak poskytovateľ digitálnej služby využíva na poskytovanie svojej digitálnej služby tretiu stranu alebo dodávateľa, na výkon činností, ktoré priamo súvisia s poskytovaním digitálnej služby (ďalej len „dodávateľ činností“), je povinný uzatvoriť s treťou stranou alebo dodávateľom činností zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby, keď poskytovateľ digitálnej služby využíva na poskytovanie svojej digitálnej služby prevádzkovateľa základnej služby alebo dodávateľa činností. ODÔVODNENIE: Navrhujeme nahradiť slová „prevádzkovateľ základnej služby“ slovným spojením „tretia strana“, v spojitosti s bodom 24 návrhu novely zákona. Poskytovateľ dátovej služby (ďalej len „PDS“) a prevádzkovateľ základnej služby (ďalej len „PZS“) sú povinní riadiť sa zákonom o kybernetickej bezpečnosti, preto podobne ako v bode 24 návrhu nebude nutnosť zmluvy medzi PZS vs. PZS, obdobne by tomu malo byť vo vzťahu PDS vs. PZS. Naším návrhom nebude dotknutá povinnosť zmluvy medzi PDS a treťou stranou.	O	N	Úprava je zvolená s ohľadom na lepšie pochopenie textu.
MIRRI SR	K Čl. I bod 5. vlastného materiálu Uvedený bod navrhujeme preformulovať nasledovne: "V § 3 sa za	Z	A	

písmeno a) vkladá nové písmeno b), ktoré znie: b) elektronickou komunikačnou sieťou prenosové systémy, ktoré môžu ale nemusia byť založené na trvalej infraštruktúre alebo centralizovanej administratívnej kapacite, prípadne prepájacie alebo smerovacie zariadenie a iné prostriedky vrátane neaktívnych prvkov siete, ktoré umožňujú prenos signálov po vedení, rádiovými, optickými alebo inými elektromagnetickými prostriedkami, vrátane družicových sietí, pevných (s prepájaním okruhov a paketov vrátane internetu) a mobilných sietí, elektrických káblových systémov v rozsahu, v ktorom sa používajú na prenos signálov, sietí používaných na rozhlasové a televízne vysielanie a sietí káblovej televízie bez ohľadu na typ prenášaných informácií (ďalej len „sieť“), „. ODÔVODNENIE: Preberaná definícia odkazuje na smernicu Európskeho parlamentu a Rady č. 2002/21/ES, ktorá však v danej časti stratí účinnosť 21.12.2020, nakoľko EÚ prijala novelizačnú smernicu v podobe Smernice Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií (EKEK) a Slovenská republika ju bude musieť do vyššie uvedeného dátumu implementovať (pozri článok 125 EKEK). Nie je preto vhodné, aby zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov odkazoval na zrušenú definíciu neúčinného právneho predpisu. V zmysle článku 2 bodu 1 EKEK je elektronická komunikačná sieť definovaná ako: „elektronická komunikačná sieť“ je prenosové systémy, ktoré môžu ale nemusia byť založené na trvalej infraštruktúre alebo centralizovanej administratívnej kapacite, prípadne prepájacie alebo smerovacie zariadenie a iné prostriedky vrátane neaktívnych prvkov siete, ktoré umožňujú prenos signálov po vedení, rádiovými, optickými alebo inými elektromagnetickými			
---	--	--	--

	prostriedkami, vrátane družicových sietí, pevných (s prepájaním okruhov a paketov vrátane internetu) a mobilných sietí, elektrických káblových systémov v rozsahu, v ktorom sa používajú na prenos signálov, sietí používaných na rozhlasové a televízne vysielanie a sietí káblovej televízie bez ohľadu na typ prenášaných informácií“ Definícia je oproti pôvodnej značne širšia a jej zakotvenie by bolo v súlade s legislatívou EÚ.			
MIRRI SR	K Čl. IV vlastnému materiálu Uvedený bod navrhujeme v druhom odseku preformulovať nasledovne: "V § 64 ods. 1 sa vkladá druhá veta „Za týmto účelom je podnik povinný prijať bezpečnostné opatrenia podľa osobitného predpisu46h)“. Poznámka pod čiarou k odkazu 46h znie: „46h) § 20 zákona č. 69/2018 Z. z.“. ODÔVODNENIE: Novelizované ustanovenie sa týka všeobecnej klauzuly bezpečnosti a integrity verejnej siete alebo služby a v novelizovanom znení znie nasledovne: „Podnik, ktorý poskytuje verejné siete alebo verejné služby, je povinný prijať zodpovedajúce technické a organizačné opatrenia a bezpečnostné opatrenia podľa osobitného predpisu na ochranu bezpečnosti svojich sietí a služieb, ktoré s ohľadom na stav techniky musia zabezpečiť úroveň bezpečnosti, ktorá je primeraná existujúcemu riziku. Opatrenia sa prijímajú najmä s cieľom predchádzať bezpečnostným incidentom a minimalizovať vplyv bezpečnostných incidentov na užívateľov a vzájomne prepojené siete.“ Ide v podstate o zbytočnú slovnú vsuvku, ktorá zneprehľadňuje dané ustanovenie, nakoľko na jednom mieste hovorí o bezpečnostných opatreniach a na druhom, že ich cieľom je ochrana bezpečnosti sietí a služieb. Nakoľko ide o implementáciu Smernice Európskeho parlamentu a Rady2002/58/ES z 12. júla 2002, týkajúca	O	ČA	

	sa spracovávanie osobných údajov a ochrana súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), zakotvenie požiadavky bezpečnostných opatrení v implementačnom ustanovení môže naraziť aj na súladnosť s právom EÚ. Článok 4 smernice o súkromí a elektronických komunikáciách v originálnom znení znie: „The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.“ Navyše, aj nariadenie GDPR v článku 32 analogicky ustanovuje, že „Prevádzkovateľ a sprostredkovateľ prijímajú so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku...“ Novelizované ustanovenie tak zneprehľadňuje požiadavky na podniky a v jednom paragrafovom znení mieša zákonné požiadavky zvláštnou terminológiou. Rozumieme však cieľu zákonodarcu ustanoviť výslovný odkaz na bezpečnostné opatrenia v zmysle § 20 zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Z tohto dôvodu navrhujeme samostatné zakotvenie danej povinnosti, ktorá sa nebude miešať s požiadavkami smernice o súkromí a elektronických komunikáciách na bezpečnosť verejných sietí a služieb.			
--	---	--	--	--

MIRRI SR	K vlastnému materiálu Čl. V Uvedený článok navrhujeme preformulovať nasledovne: "Tento zákon nadobúda účinnosť 1. januára 2021" ODÔVODNENIE: Navrhujeme zjednotenie textácie Čl. V s ostatnými časťami návrhu zákona a predloženými materiálmi vo vzťahu k navrhovanej účinnosti.	O	A	
MIRRI SR	K vlastnému materiálu V súvislosti s navrhovanou zmenou § 3 písm. k) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov kde navrhujeme vypustiť bod 2. je potrebné vykonať zmenu aj v § 17. Z § 17 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov navrhujeme vypustiť odsek 3. ODÔVODNENIE: V súvislosti so zrušením § 3 písm. k) druhého bodu bude zaradzovanie informačných systémov verejnej správy do zoznamu základných služieb a ich správcov do registra prevádzkovateľov základných služieb realizované na základe § 17 ods. 2.	Z	A	
MIRRI SR	K Čl. I bod 33. vlastného materiálu Všeobecne k bodu 33. ktorým sa za § 27 vkladá § 27a: Uvedený koncept z nášho pohľadu zavádza nový precedens do legislatívneho rámca v oblasti informatizácie vrátane kybernetickej bezpečnosti s možnými dopadmi na subjekty pôsobiace v digitálnej ekonomike Slovenska, ktoré je nutné náležite vyhodnotiť. Dnes je opisovaná prax možná len cez rozhodnutie súdu. A priori uvedený koncept neodmietame, mal by byť však dostatočne spracovaný, garantujúci právnu istotu a mala by mu predchádzať spoločenská debata dotknutých subjektov trhu a regulátora, inak môže negatívne ovplyvniť čoraz viac podnikov fungujúcich v online priestore a	Z	A	

	rovnako aj spotrebiteľov. Debata by mala prebehnúť aj na úrovni Komisie pre správu národnej domény .sk pri MIRRI SR, nakoľko uvedený koncept bude mať osobitný dopad na prácu správcu národnej domény. SK a registrátorov.			
MIRRI SR	K vlastnému materiálu Z § 3 písm. k) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov navrhujeme vypustiť bod 2. ODÔVODNENIE: Prevádzkovateľ základnej služby musí v zmysle smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii spĺňať 3 kumulatívne kritériá, ktorými sú: subjekt poskytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností; poskytovanie tejto služby je závislé od sietí a informačných systémov a incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby. Posledné kritérium, a teda incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby je v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov vyjadrený v § 18 a príslušnej vyhláške NBÚ č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovanvej služby (kritériá základnej služby). Vyhláška NBÚ č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovanvej služby (kritériá základnej služby) sa však aplikuje len na základné služby podľa § 3 písm. k) prvého bodu ale nie na základné služby podľa § 3 písm. k) druhého bodu. Avšak vyše 1300 informačných systémov verejnej správy nie je zaradených do zoznamu základných služieb ako základná služba podľa § 3 písm. k) prvého bodu podľa zákona č. 69/2018 Z. z. o kybernetickej	Z	A	

	bezpečnosti a o zmene a doplnení niektorých zákonov ale ako základná služba podľa § 3 písm. k) druhého bodu podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Pokiaľ sa nebude skúmať či prevádzkovateľ základnej služby naplnil dopadové kritéria, nemožno hovoriť o prevádzkovateľovi základnej služby. Nevyžadovanie naplnenia dopadového kritéria je v rozpore so smernicou NIS.			
MKSR	K čl. I bod 39 1. V úvodnej vete odporúčame slovo „ods.“ nahradiť slovom „odsek“. Odôvodnenie: Legislatívna technika. 2. V navrhovanom § 31 ods. 5 písm. a) odporúčame vypustiť čiarku za slovom „súčinnosť“ a na konci doplniť čiarku. Odôvodnenie: Legislatívna technika. 3. V navrhovanom § 31 ods. 5 písm. b) odporúčame bodku na konci nahradiť čiarkou. Odôvodnenie: Legislatívna technika.	O	A	
MKSR	K prílohe č. 1 zákona č. 69.2018 Z. z. Upozorňujeme, že v právne záväznom texte v prílohe č. 1 k zákonu č. 69/2018 Z. z. je potrebné vykonať redakčnú opravu súvisiacu s nevykonaním zmeny ustanovenej v čl. XIII zákona č. 134/2020 Z. z., ktorým sa mení a dopĺňa zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony, podľa ktorého sa slová „Úrad podpredsedu vlády pre investície a informatizáciu“ vo všetkých tvaroch v celom texte zákona okrem § 34 ods. 10 nahrádzajú slovami „Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky“ v príslušnom tvare. Odôvodnenie: Legislatívno-technická pripomienka.	O	A	

MKSR	K čl. IV Upozorňujeme, že zákon č. 351/2011 Z. z. bol novelizovaný aj zákonom č. 242/2020 Z. z. Odporúčame upraviť. Odôvodnenie: Legislatívna technika.	O	A	
MKSR	K čl. III bod 1 V navrhovanej poznámke pod čiarou k odkazu 21 odporúčame slovo „zákon“ nahradiť slovom „Zákon“ a pripojiť slová „v znení neskorších predpisov“. Odôvodnenie: Legislatívna technika.	O	A	
MKSR	K čl. I Za novelizačný bod 6 navrhujeme vložiť nový novelizačný bod 7, ktorý znie: „7. V § 3 písmeno l) znie: „l) základnou službou služba, ktorá je zaradená v zozname základných služieb a 1. závisí od sietí alebo informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1, alebo 2. je prvkom kritickej infraštruktúry, 9)“. Doterajšie novelizačné body 7 až 53 navrhujeme primerane prečíslovať. Odôvodnenie: Oprava závažnej významovej chyby v texte zákona, ktorá je umocnená navrhovanými novelizačnými doplneniami (najmä navrhovaným písmenom s) doplneným do § 3).	Z	A	
MKSR	K čl. I Za novooznačený novelizačný bod 54 navrhujeme vložiť novelizačný bod 55, ktorý znie: „55. V prílohe č. 1 v sektore „10. Verejná správa“, v stĺpci „Prevádzkovateľ služieb“ sa slová „správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona č. 275/2006 Z. z. podporujúci služby verejnej správy, služby vo verejnom záujme a verejné služby“ nahrádzajú slovami „správcovia	Z	A	

	a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti orgánu riadenia podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov podporujúcich služby verejnej správy, služby vo verejnom záujme a verejné služby“.. Odôvodnenie: Oprava textu prílohy č. 1 súvisiaca s navrhovaným novelizačným bodom 7.			
MOSR	K Čl. I bod 52 V Čl. I návrhu zákona žiadame za bod 52 doplniť nový bod 53, ktorý znie: „V prílohe č. 1 sa v sektore „10. Verejná správa“ podsektore „Obrana“ v stĺpci „Ústredný orgán“ slová „Ministerstvo obrany Slovenskej republiky“ nahrádzajú slovami „Vojenské spravodajstvo“.. Túto pripomienku Ministerstvo obrany Slovenskej republiky považuje za zásadnú. Odôvodnenie: Vojenské spravodajstvo v rámci svojej pôsobnosti spravuje a prevádzkuje spravodajské systémy a informačné systémy, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky, zodpovedá za zabezpečenie kybernetickej bezpečnosti v rozsahu svojej pôsobnosti a plní úlohy jednotky CSIRT pre podsektor „Obrana“ podľa § 15 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Vzhľadom na tieto skutočnosti žiadame, aby bolo ako ústredný orgán vykonávajúci pôsobnosť v oblasti kybernetickej bezpečnosti v rámci sektoru „10. Verejná správa“ podsektoru „Obrana“ určené Vojenské spravodajstvo.	Z	N	Odôvodnenie je súčasťou vyhodnotenia predchádzajúcich pripomienok.
MOSR	K Čl. I bod 10 V Čl. I bod 10 návrhu zákona sú v navrhovanom § 5 ods. 1 písm. y) použité pojmy „škodlivý obsah“ a „škodlivá aktivita“, ktoré však v	Z	ČA	Text preformulovaný tak, aby spĺňal predpoklady uvedené v pripomienkach.

	návrhu zákona nie sú vymedzené. Preto žiadame, aby boli do návrhu zákona doplnené legálne definície pojmov „škodlivý obsah“ a „škodlivá aktivita“. Túto pripomienku Ministerstvo obrany Slovenskej republiky považuje za zásadnú. Odôvodnenie: V súlade s čl. 6 ods. 2 Legislatívnych pravidiel vlády Slovenskej republiky musí byť zákon terminologicky správny, presný, jednotný a všeobecne zrozumiteľný. Možno v ňom používať len správne a v právnom poriadku ustálené pojmy a správnu právnu terminológiu. Nový pojem treba v právnom predpise právne vymedziť. Keďže navrhované pojmy „škodlivý obsah“ a „škodlivá aktivita“ nie sú v návrhu zákona vymedzené, môžu tieto pojmy subsumovať akúkoľvek škodlivú aktivitu v kybernetickom priestore, a to bez ohľadu na jej závažnosť. Vzhľadom na to, že sa s blokovaním „škodlivého obsahu“ alebo „škodlivej aktivity“ viaže možný zásah do elektronického obsahu a obsahu elektronickej komunikácie, môže blokovanie znamenať zásah do slobody prejavu a slobody podnikania, teda zásah do základných ľudských a občianskych práv garantovaných Ústavou Slovenskej republiky. Platná legislatíva pritom umožňuje vykonávať rozhodnutia tohto charakteru vzhľadom na ich závažnosť predovšetkým na základe príkazu súdu, vydávaného na základe žiadosti oprávneného subjektu (napr. podľa zákona č. 171/2005 Z. z. o hazardných hrách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov). Vzhľadom na uvedené skutočnosti preto žiadame, aby boli do návrhu zákona doplnené legálne definície pojmov „škodlivý obsah“ a „škodlivá aktivita“.			Doplnená dôvodová správa.
MOSR	K Čl. I bod 11 V Čl. I bod 11 návrhu zákona žiadame na konci poslednej vety	Z	A	Text preformulovaný tak, aby spĺňal predpoklady uvedené v pripomienkach.

	navrhovaného § 5 ods. 4 bodku nahradiť bodkočiarkou, za ktorú žiadame doplniť nasledovný text: „informácie sa poskytujú len za podmienky, že ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu) alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb konajúcich v jej prospech alebo k ohrozeniu medzinárodnej spravodajskej spolupráce.“. Poznámka pod čiarou k odkazu x znie: „x) Zákon Národnej rady Slovenskej republiky č. 198/1994 Z. z. v znení neskorších predpisov. Zákon Národnej rady Slovenskej republiky č. 46/1993 Z. z. v znení neskorších predpisov.“. Túto pripomienku Ministerstvo obrany Slovenskej republiky považuje za zásadnú. Odôvodnenie: Doplnenie uvedeného textu požadujeme z dôvodu zabezpečenia plnenia úloh Vojenského spravodajstva, vymedzených zákonom Národnej rady Slovenskej republiky č. 198/1994 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov, a taktiež z dôvodu ochrany zdrojov, prostriedkov, totožnosti osôb konajúcich v jej prospech alebo aby nedošlo k ohrozeniu medzinárodnej spravodajskej spolupráce. Obdobné ustanovenia obsahuje aj v súčasnosti platné znenie § 9 ods. 1 písm. b) a § 10 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.			
MOSR	K Čl. I bod 31 V Čl. I bod 31 návrhu zákona žiadame na konci poslednej vety navrhovaného § 24 ods. 7 bodku nahradiť bodkočiarkou, za ktorú žiadame doplniť nasledovný text: „to sa nevzťahuje na siete a informačné systémy, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky.“ Túto pripomienku Ministerstvo obrany Slovenskej republiky považuje za zásadnú. Odôvodnenie: Vzhľadom	Z	A	text preformulovaný aj s ohľadom na iné vznesené pripomienky

	na skutočnosť, že za zaistenie kybernetickej bezpečnosti sietí a informačných systémov, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky, zodpovedá príslušný ústredný orgán v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, a vzhľadom na to, že v rámci daného podsektora „Obrana“ je pre účely detekcie a reakcie na kybernetické bezpečnostné incidenty zriadená podľa § 15 predmetného zákona jednotka CSIRT, považujeme povinnosť prevádzkovateľa základnej služby určeného rozhodnutím úradu zasielať automatizovaným spôsobom systémové informácie zo sietí a informačných systémov úradu za neopodstatnenú.			
MOSR	K Čl. I bod 32 V Čl. I bod 32 návrhu zákona odporúčame v navrhovanom § 27 ods. 1 písm. e) precizovať a rozpracovať mechanizmus vydávania rozhodnutí úradu, a to najmä vo vzťahu k lehotám, prechodnému obdobiu v prípade zákazu používať konkrétnu technológiu a finančným škodám spôsobených prevádzkovateľovi rozhodnutím úradu. Tento mechanizmus by mal zároveň zohľadňovať analýzu rizík. Odôvodnenie: Rozhodnutím úradu, ktorým sa prevádzkovateľovi základnej služby zakazuje alebo obmedzuje používanie konkrétneho produktu, procesu alebo služby, by mohlo byť ohrozené poskytovanie základných služieb, v dôsledku čoho by mohli vzniknúť materiálne a finančné straty. Vyradenie služby alebo komponentu môže zároveň spôsobiť ochromenie ďalších súvisiacich služieb závislých na tomto prvku, vrátane informačných systémov nespádajúcich pod zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení	O	A	text preformulovaný aj s ohľadom na iné vznesené pripomienky

	neskorších predpisov. Zároveň upozorňujeme na garantovaný slobodný pohyb tovaru v rámci jednotného trhu EÚ a na možné medzinárodné dopady zákazu používania konkrétnej technológie.			
MOSR	K Čl. I bod 33 V Čl. I bod 33 návrhu zákona sa v navrhovanom znení § 27a ods. 4 používa slovné spojenie „vykonateľné rozhodnutie žiadateľa o blokovanie“, ktoré v návrhu zákona nie je bližšie definované. Preto odporúčame, aby bola do návrhu zákona doplnená legálna definícia tohto právneho pojmu. Odôvodnenie: V navrhovanom znení § 27a ods. 1 a 2 sa uvádza, že Národný bezpečnostný úrad rozhoduje o blokovaní buď z vlastnej iniciatívy alebo na základe žiadosti, ktorú mu doručí žiadateľ o blokovanie. V navrhovanom znení § 27a ods. 4 sa však používa slovné spojenie „vykonateľné rozhodnutie žiadateľa o blokovanie“, z ktorého implicitne vyplýva, že okrem Národného bezpečnostného úradu môže o blokovaní rozhodovať aj samotný žiadateľ o blokovanie. Zo znenia návrhu zákona však nie je zrejmé, že by predkladateľ sám založil žiadateľovi o blokovanie právomoc takéto rozhodnutie vydať alebo že by aspoň odkazoval na osobitný predpis, ktorý žiadateľovi o blokovanie takúto právomoc zakladal. Okrem toho môže za týchto podmienok vo veciach rozhodovania o blokovaní dôjsť ku kompetenčným konfliktom medzi Národným bezpečnostným úradom a žiadateľmi o blokovanie. Preto považujeme za vhodné odstrániť rozpor medzi ustanovením navrhovaného § 27a ods. 4 s ostatnými ustanoveniami navrhovaného § 27a.	O	A	bližšie vysvetlené v DS
MOSR	K Čl. I bod 33 V Čl. I bod 33 návrhu zákona žiadame navrhované znenie § 27a ods. 1 a 2 preformulovať nasledovným spôsobom: „(1) Úrad rozhoduje o	Z	ČA	Text primerane upravený. Úrad rozhoduje o blokovaní podľa zákona o KB pri riešení KBI a o spôsobe

	blokovaní podľa osobitného predpisu10aa), spôsobe blokovanja a zabezpečuje blokovanie pri riešení kybernetického bezpečnostného incidentu. (2) Úrad rozhoduje o spôsobe blokovanja a zabezpečuje blokovanie aj na základe žiadosti subjektov podľa osobitných predpisov28a) (ďalej len „žiadateľ o blokovanie“).“. V navrhovanom znení § 27a ods. 7 ďalej žiadame vypustiť slová „inak blokovanie vykoná úrad“. Túto pripomienku Ministerstvo obrany Slovenskej republiky považuje za zásadnú. Odôvodnenie: V Čl. I bod 10. návrhu zákona sa § 5 ods. 1 dopĺňa novým písmenom y), podľa ktorého Národný bezpečnostný úrad zabezpečuje vykonanie rozhodnutia o blokovaní škodlivého obsahu alebo škodlivej aktivity. Podľa navrhovaného znenia § 27a ods. 1 a 2 však sám Národný bezpečnostný úrad vykonáva blokovanie, čo nekorešponduje so znením vyššie spomenutého návrhu § 5 ods. 1 písm. y). Zo znenia ďalších odsekov navrhovaného § 27a vyplýva, že Národný bezpečnostný úrad má vydávať rozhodnutie o blokovaní, ale samotné blokovanie má vykonávať iný subjekt, ako napr. podľa § 27a ods. 6 („Rozhodnutie úradu o blokovaní úrad preukázateľne doručí osobe, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať, a ktorá je povinná vykonať blokovanie.“) alebo podľa § 27a ods. 7 („Osoba, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať, je povinná na základe rozhodnutia úradu o blokovaní zamedziť prevádzku spôsobom podľa rozhodnutia úradu o blokovaní.“). Vzhľadom na vyššie uvedené nezrovnalosti vyjadrujeme nesúhlas s tým, aby blokovanie vykonával Národný bezpečnostný úrad, a to aj z dôvodu, že v danom prípade by išlo o zásah Národného bezpečnostného úradu do informačných systémov subjektov, na ktoré sa vzťahuje konečné rozhodnutie o blokovaní. Na základe vyššie uvedených		blokovania na základe žiadosti iného orgánu verejnej moci.
--	---	--	---

	rozporov, ktoré vyplývajú z citovaných ustanovení, je potrebné ich vzájomné zosúladenie.			
MOSR	K Čl. I bod 8 V Čl. I bod 8 návrhu zákona žiadame ponechať Vojenské spravodajstvo v § 4 písm. b) ako ústredný orgán vykonávajúci pôsobnosť v oblasti kybernetickej bezpečnosti. Túto pripomienku Ministerstvo obrany Slovenskej republiky považuje za zásadnú. Odôvodnenie: Na základe vypustenia Vojenského spravodajstva a taktiež Slovenskej informačnej služby z okruhu subjektov, ktoré sa na účely zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“) považujú za ústredný orgán podľa § 4 písm. b) zákona č. 69/2018 Z. z., a taktiež na základe vypustenia podsektoru „Spravodajské služby“ v sektore „Verejná správa“ v prílohe č. 1 zákona č. 69/2018 Z. z., nie je zrejmé postavenie Vojenského spravodajstva v rámci pôsobnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti. V súlade s dôvodovou správou k návrhu novely zákona č. 69/2018 Z. z. má k predmetnému vypusteniu dôjsť z dôvodu „odzrkadľovania ustanovenia článku 1 ods. 6 smernice NIS a súčasne táto zmena vyplynula z potrieb aplikačnej praxe, keďže sa uvedené ukázalo ako neefektívne“. Uvedené zdôvodnenie považujeme za nedostačujúce na vykonanie vyššie uvedeného zásahu do pôsobnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti prostredníctvom novelizácie zákona č. 69/2018 Z. z. bez predchádzajúcej diskusie s dotknutými subjektmi. Podľa článku 1 ods. 6 smernice NIS touto smernicou nie sú dotknuté opatrenia prijímané členskými štátmi na zabezpečenie ich základných štátnych funkcií, z čoho vyplýva, že je	Z	N	Dôvody vypustenia doplnené do DS:- Vojenské spravodajstvo v zmysle zákona č. 198/1994 Z. z. okrem iného plní úlohy zamerané aj na aktivity a ohrozenia v kybernetickom priestore (§ 2 ods. 1 písm. h). Ďalej, Vojenské spravodajstvo má v zmysle § 4a uvedeného zákona zriadené Centrum pre kybernetickú obranu, ktoré získava, sústreďuje, analyzuje a vyhodnocuje informácie dôležité na zabezpečenie kybernetickej obrany a plní úlohy aj podľa zákona o kybernetickej bezpečnosti. Centrum má prístup k jednotnému informačnému systému kybernetickej bezpečnosti, ktorý zriaďuje a prevádzkuje Národný bezpečnostný úrad. - Novelou zákona č. 69/2018 Z. z. dochádza k vypusteniu Vojenského spravodajstva ako ústredného orgánu z dôvodu, že dochádza k vypusteniu sektora „Spravodajské služby“ /analogicky teda platí aj pre Slovenskú informačnú službu/. Keďže platí, že kde nie sú identifikovaní prevádzkovatelia základnej služby, logicky nie je sektor,

	na členskom štáte, aby si sám prijal opatrenia na zabezpečenie základných štátnych funkcií, a to najmä tých, ktoré sú uvedené v čl. 1 ods. 6 smernice NIS. Predkladateľ ďalej v dôvodovej správe k návrhu novely zákona č. 69/2018 Z. z. bližšie nešpecifikuje aké konkrétne poznatky z aplikačnej praxe ho viedli k vyvodu záveru, že súčasná právna úprava je neefektívna. Preto považujeme za žiaduce uviesť v dôvodovej správe konkrétne dôvody, ktoré predkladateľa vedú k záveru, že súčasná právna úprava je neefektívna. Podľa § 4a zákona č. 198/1994 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov Vojenské spravodajstvo prostredníctvom Centra pre kybernetickú obranu Slovenskej republiky, ktoré je osobitnou organizačnou zložkou Vojenského spravodajstva, plní úlohy na úseku obrany štátu v kybernetickom priestore a kybernetickej bezpečnosti v rozsahu ustanovenom osobitným predpisom. Týmto osobitným predpisom je práve zákon č. 69/2018 Z. z., ktorý by mal upravovať tento rozsah pre Vojenské spravodajstvo. Podľa súčasnej právnej úpravy sa pritom na Vojenské spravodajstvo vzťahujú ustanovenia zákona č. 69/2018 Z. z., upravujúce „ústredné orgány“, keďže Vojenské spravodajstvo je podľa § 4 písm. b) ústredným orgánom na účely tohto zákona. Vzhľadom na vyššie uvedené skutočnosti žiadame, aby bolo Vojenské spravodajstvo v § 4 písm. b) ponechané ako ústredný orgán vykonávajúci pôsobnosť v oblasti kybernetickej bezpečnosti.			tak nie je ani ústredný orgán, ktorý by reguloval prevádzkovateľov základnej služby. Vojenské spravodajstvo nemá žiadne regulované subjekty a úlohy na úseku kybernetickej bezpečnosti vykonáva len vo vzťahu k vlastným činnostiam (okrem iného spravodajské služby). Pôsobnosť Ministerstva obrany SR vo vzťahu k prevádzkovateľom základných služieb pre informačné systémy, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky, zostávajú v plnej miere zachované (má regulované subjekty, medzi ktoré patrí aj Vojenské spravodajstvo) a teda tieto činnosti bude vykonávať Ministerstvo obrany (prostredníctvom Centra pre kybernetickú bezpečnosť).
MPSVRSR	K Čl. I bod 33 Odporúčame v Čl. I bode 33 navrhovanom § 27a doplniť spôsob a postup komunikácie s dotknutým orgánom verejnej moci, ak žiadateľ žiada o jeho blokovanie. Odôvodnenie: V Čl. I bode 33 navrhovaný § 27a predstavuje závažný zásah do činností orgánu	O	A	

	verejnej moci a možné zásadné obmedzenie výkonu verejnej moci, ktorú podľa osobitných právnych predpisov orgán verejnej moci zabezpečuje, obzvlášť v prípade, keď sa väčšina jeho výkonu vykonáva elektronicky.			
MSSR	K čl. I bod 39 Odporúčame nahradiť slovo "ods." slovom "odsek". Ide o legislatívno-technickú pripomienku.	O	A	
MSSR	K čl. I bod 40 V poslednej vete odporúčame slovo "písmená" nahradiť slovom "odseky". Ide o legislatívno-technickú pripomienku.	O	A	
MSSR	K uzneseniu vlády Slovenskej republiky V úvodnej časti, kde má byť uvedený predkladateľ, žiadame doplniť, kto je predkladateľom návrhu zákona.	O	A	
MŠVVaŠSR	Všeobecne Odporúčame návrh zákona upraviť legislatívno-technicky, napr.: - v čl. I bode 25 vypustiť slová "alebo Policajnému zboru" v súlade s legálnou definíciou "orgánu činného v trestnom konaní" podľa § 10 ods. 1 Trestného poriadku v súlade s čl. 6 ods. 3 LPV, t. j. právny pojem s vymedzeným významom sa v tomto význame používa jednotne v celom právnom poriadku, - v čl. I bode 28 úvodnej vete slová "písmeno a) znie:" nahradiť slovami "sa za úvodnú vetu vkladá nové písmeno a), ktoré znie:" v súlade s bodom 32 prílohy č. 1 k LPV a - v čl. I bode 40 slová "označujú ako písmená" nahradiť slovami "označujú ako odseky" v súlade s bodom 32 prílohy č. 1 k LPV.	O	A	

MVSR	Pripomienky všeobecného charakteru: 1. Použitá terminológia a najmä jej zmeny spôsobia rozdielne definície rovnakých alebo podobných pojmov v rôznych právnych predpisoch. Terminológia je nekonzistentná, rozporuplná a neúplná. Odporúčame preto zadefinovať v spolupráci s odborníkmi v danej oblasti a akademickou obcou odbornú terminológiu pre oblasť kybernetickej bezpečnosti. Ako optimálne navrhujeme po vzore napr. Českej republiky vydať ‘Výkladový slovník Kybernetické bezpečnosti’, ktorý bol v Českej republike vydaný v spolupráci s českou pobočkou AFCEA a pod záštitou NBÚ ČR a NÚKIB. Po ustálení odbornej terminológie potom túto následne používať vo všetkých právnych predpisoch jednotným a konzistentným spôsobom.	O	N	terminológia bola predmetom posudzovania pri tvorbe zákona, neustále sa precizuje a stáva sa akceptovanou a zaužívanou v odbornej a aj laickej praxi.
MVSR	Pripomienky ku konkrétnym novelizačným bodom: 6. V čl. I bod 8 žiadame upraviť nasledovne: „8. V § 4 písm. b) sa vypúšťa slovo „úrad“ a slová „Ministerstvo vnútra Slovenskej republiky“ a slová „Slovenská informačná služba, Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky a Vojenské spravodajstvo“ sa nahrádzajú slovami „a Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky“. Odôvodnenie: Na informačné systémy Ministerstva vnútra Slovenskej republiky (ktorého súčasťou sú aj informačné systémy využívané orgánmi činnými v trestnom konaní a kriminálnou políciou) sa nemôže aplikovať zákon o kybernetickej bezpečnosti v predkladanom znení. Predkladané znenie by umožnilo Národnému bezpečnostnému úradu nariadiť vykonanie auditu informačných systémov Ministerstva vnútra SR a uvedené by mohol nariadiť aj súkromným audítorm (na náklady Ministerstva vnútra	Z	N	Pripomienka je nad rámec novely. MVSR bolo zaradené ako ústredný orgán už do návrhu nového zákona a svoju povinnosť realizuje od roku 2018. NBÚ nevidí logické odôvodnenie predloženej pripomienky jednak aj z dôvodu, že MV je v sektore verejnej správy ústredným orgán zodpovedným za bezpečnosť sietí a informačných systémov a rovnako tak na účely zákona je audit oprávnený vykonať výlučne na to certifikovaný audítorm a nie jednotka CSIRT.

	SR). Ministerstvo vnútra SR pre účel auditov informačných systémov Ministerstva vnútra SR buduje svoj vlastný CSIRT. Túto pripomienku považujeme za zásadnú.			
MVSR	10. K bodu 12 celý doplnený nový § 5a žiadame zásadným spôsobom prepracovať, nakoľko je len čiastočnou implementáciou nariadenia (EÚ) č. 2019/881 a ďalej aj z nasledovných dôvodov. Odôvodnenie: Ustanovenie § 5a ods. 1 poveruje úrad plnením úloh podľa osobitného predpisu. V poznámke pod čiarou je odkaz na čl. 58 ods. 6 až 9 aktu o kybernetickej bezpečnosti (nariadenia (EÚ) č. 2019/881). Avšak z aktu o kybernetickej bezpečnosti vyplýva pre členský štát viacero úloh (napríklad z čl. 23 nominovať člena do siete národných styčných úradníkov), v čl. 58 ods. 2 povinnosť členského štátu notifikovať Komisii určenie vnútroštátneho certifikačného orgánu, čl. 60 oznamovacie povinnosti. Vzhľadom na skutočnosť, že nie je zabezpečené plnenie všetkých úloh z aktu o kybernetickej bezpečnosti, v podmienkach Slovenskej republiky nemožno dosiahnutie zhody s Európskym právom chápať ako úplné, aj keď ju predkladateľ ako úplnú uvádza v doložke zlučiteľnosti. Akt o kybernetickej bezpečnosti je potrebné doplniť do prílohy č. 3 návrhu zákona a adekvátne k tomu zmeniť názov prílohy. Navyše z pohľadu implementácie aktu o kybernetickej bezpečnosti upozorňujeme, že z návrhu nie je zrejmé, kto bude tým vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti zodpovedným za dozor, respektíve dohľad nad touto činnosťou v členskom štáte (čl. 58 ods. 1). Návrh v § 5 ods. 1 len uvádza, že úrad plní úlohy podľa osobitného predpisu, (v poznámke pod čiarou odkazuje iba na čl. 58 ods. 6 až 9 aktu o kybernetickej bezpečnosti).	Z	A	K časti chýbajúcim ustanoveniam: podľa § 5 ods. 1 písm. f) úrad plní notifikačné a nahlasovacie povinnosti voči príslušným orgánom EÚ. Z uvedeného je zrejmé, že plnení všetkých povinností vyplývajúcich z Aktu KB je zabezpečené už v rámci terajšej úpravy. NBú už pri príprave zákona predpokladal prijatie Aktu a v súlade s legislatívnymi pravidlami zabezpečil, aby uvedené ustanovenie pokrývalo plnenie povinností voči orgánom EÚ aj do budúcnosti. K časti nejasnosti, kto je orgánom certifikácie kybernetickej bezpečnosti doplníme dôvodovú správu.

	Uvedené je dôležité upraviť v zákone nielen z dôvodu náležitej a úplnej implementácie aktu o kybernetickej bezpečnosti, ale taktiež pre posúdenie, či sú dodržané aj iné požiadavky aktu o kybernetickej bezpečnosti, napr. požiadavka oddelenosti činností podľa článku 56 ods. 5 písm. a) a článku 56 ods. 6 od činností dohľadu podľa čl. 58. Navyše ministerstvo vnútra má ambíciu akreditovať vlastný orgán posudzovania zhody pre certifikáciu produktov IKT, služieb IKT a procesov IKT. Túto pripomienku považujeme za zásadnú.			
MVSR	11. K bodu 14 s uvedenou zmenou zásadne nesúhlasíme, nakoľko nebola vopred prerokovaná s dotknutými ústrednými orgánmi. Navrhujeme preto buď ponechať pôvodné znenie § 9 ods. 2 alebo žiadame slová „podsektor Obrana a podsektor Informačné systémy verejnej správy“ nahradiť slovami „podsektor Obrana, bezpečnosť a podsektor Informačné systémy verejnej správy“. Odôvodnenie: Niektoré vybrané rezorty vzhľadom na plnenie špecifických úloh plánujú zriadiť a prevádzkovať v budúcnosti vlastné akreditované jednotky CSIRT. Rovnako tak rezort Ministerstva vnútra SR pripravuje vybudovanie rezortnej jednotky CSIRT, ktorá bude pokrývať všetky informačné systémy prevádzkované rezortom. Novo navrhované znenie § 9 ods. 2 by znemožnilo zriaďovanie a prevádzku iných jednotiek, s čím zásadne nesúhlasíme. Túto pripomienku považujeme za zásadnú.	Z	A	Ponechaná možnosť prevádzkovať vlastnú jednotku CSIRT.
MVSR	12. K bodu 15 vzhľadom na pripomienku k novelizačnému bodu 14 a čiastočné zachovanie pôvodného znenia § 9 ods. 2 navrhujeme zachovať tento odsek minimálne v takom rozsahu, aby bolo možné kvantifikovať prevádzkové náklady Národnej jednotky CSIRT pri	O	A	

	výkone činností pre ústredný orgán.			
MVSR	13. K bodu 16 navrhujeme upraviť slovosled, nakoľko takto zaniká základná myšlienka.	O	N	
MVSR	14. K bodu 17 navrhujeme ponechať pôvodné znenie alebo nahradiť slová „ústredný orgán“ slovami „orgán verejnej moci“. Odôvodnenie: Z pohľadu ministerstva vnútra je žiaduce, aby akreditované jednotky CSIRT vznikali vždy pod záštitou ústredného orgánu alebo minimálne orgánu verejnej moci. V prípade že sa umožní akreditovať podnikateľským subjektom, a tým v princípe „outsorcovať“ bezpečnostný dohľad a riešenie bezpečnostných incidentov a udalostí, je potrebné presne zadefinovať, kedy je možné použiť takýto model a za dodržania akých podmienok. Táto možnosť, konkrétne pre rezort ministerstva vnútra, vzhľadom na citlivosť spracúvaných informácií a dosah prevádzkovaných informačných systémov na štátnu a verejnú správu a aj širokú verejnosť nie je akceptovateľná. Túto pripomienku považujeme za zásadnú.	Z	N	Ponecháva sa možnosť zriadiť a prevádzkovať vlastnú jednotku CSIRT ústredným orgánom, systém hlásenia a riešenia incidentov rovnako zostáva zachovaný. Zvyšné úpravy sú legislatívneho charakteru a reflektujú prax.
MVSR	15. K bodu 18 navrhujeme ponechať pôvodné znenie alebo nahradiť slová „ústredného orgánu, ktorý má plniť úlohy jednotky CSIRT“ slovami „orgánu verejnej moci, ktorý má plniť úlohy jednotky CSIRT“. Túto pripomienku považujeme za zásadnú.	Z	ČA	Ponecháva sa možnosť zriadiť a prevádzkovať vlastnú jednotku CSIRT ústredným orgánom, systém hlásenia a riešenia incidentov rovnako zostáva zachovaný. Zvyšné úpravy sú legislatívneho charakteru a reflektujú prax.

MVSR	16. K bodu 23 navrhujeme slovo „šiestich“ nahradiť slovom „dvadsiatich štyroch“. Odôvodnenie: Uvedené navrhujeme upraviť vo vzťahu k počtu základných služieb, ktoré prevádzkuje rezort ministerstva vnútra a tieto budú pripájané pod rezortnú jednotku CSIRT postupne v priebehu celých 24 mesiacov od navrhovanej účinnosti zákona a zároveň týmto dôjde k harmonizácii lehôt určených v zákone 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. Vzhľadom na neustále pribúdajúce hrozby v kybernetickom priestore je všeobecný konsenzus uskutočniť túto činnosť v čo najskoršom možnom termíne, je však potrebné zohľadniť špecifické postavenie rezortu ministerstva vnútra vzhľadom na počet prevádzkovaných základných služieb. Túto pripomienku považujeme za zásadnú.	Z	N	Neodôvodnená pripomienka, vo vzťahu k zabezpečovaniu bezpečnosti je lehota dvoch rokov neúmerne dlhá. Nami navrhovaná doba predstavuje dostatočný priestor na prijatie bezpečnostných opatrení.
MVSR	17. K bodu 31 navrhujeme vypustiť celý bod 31. Odôvodnenie: Jedná sa o veľmi široké oprávnenie úradu požadovať po ktoromkoľvek prevádzkovateľovi základnej služby zasielať mu ním určené systémové informácie zo sietí a informačných systémov. Úrad by na základe uvedeného mohol doslova kedykoľvek a vo vzťahu ku ktorémukoľvek prevádzkovateľovi základnej služby rozhodnúť, aby mu ním určeným spôsobom zasielal systémové informácie (logy), čo je neprijateľné a zároveň vysoko rizikové, koncentrovať takto citlivé záznamy, nevynímajúc informácie podliehajúce osobitnému režimu ochrany (napr. bankové tajomstvo, daňové tajomstvo a pod.) na jedinom štátnom orgáne podľa jeho ľubovôle, v ním určenom obsahu, rozsahu a forme. Takto	Z	N	Text návrhu zákona bol predmetom verejných konzultácií aj PPK, nie je preto pravdivé tvrdenie vo Vašej pripomienke, že text nebol dostupný na vyjadrenie sa dotknutým subjektom. Navrhované ustanovenie je nevyhnuté pre zabezpečenie plnia úloh na úseku kybernetickej bezpečnosti. Bez adekvátnych nástrojov zaistovania bezpečnosti nie je možné túto úlohu plniť efektívne a účinne.

	koncipované oprávnenie úradu by prekračovalo pôvodný účel zákona, a to spolupráca subjektov vykonávajúcich pôsobnosť v oblasti kybernetickej bezpečnosti v snahe o zachovanie požadovanej úrovne kybernetickej bezpečnosti štátu a pre neho významných (kritických) základných služieb do pozície autoritatívnej. Navyše uvedené ustanovenie nebolo predmetom konzultácií so zainteresovanými stranami, na ktoré sa zavedená povinnosť vzťahuje. Považujeme to za nevyhnutné riešiť v rámci širšej odbornej a celospoločenskej diskusie, vypracovať k nim podrobnú analýzu vplyvov, ich právne posúdenie a navrhujeme ich preto z predkladaného návrhu zákona vypustiť. Okrem toho zasielanie informácií automatizovaným spôsobom prinesie subjektom dodatočné finančné náklady na prevádzku systémov, ktoré nie sú nijakým spôsobom uvedené v doložke vplyvov na rozpočet verejnej správy ani v doložke vplyvov na podnikateľské prostredie. Túto pripomienku považujeme za zásadnú.			
MVSR	18. K bodu 32 navrhujeme vypustiť celý bod 32. Odôvodnenie: Ide o veľmi široké oprávnenie úradu zakázať alebo obmedziť ktorémukoľvek prevádzkovateľovi základnej služby používať konkrétny produkt, proces alebo službu pod vágne koncipovanou podmienkou „ak je to potrebné na zaistenie kybernetickej bezpečnosti, alebo z dôvodov bezpečnostného záujmu Slovenskej republiky“, pod čo je možné subsumovať v zásade čokoľvek. Navyše uvedené ustanovenie je pravdepodobne v rozpore s platným zákonom o verejnom obstarávaní č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov, tzv. „nediskriminačný prístup“. Bez uvedenia vopred predvídateľných	Z	ČA	Text preformulovaný tak, aby spĺňal predpoklady uvedené v pripomienkach. prax.

	podmienok a pri dodržaní zásad presne stanoveného procesu uvedené nie je možné akceptovať. Uvedené ustanovenie nebolo predmetom konzultácií so zainteresovanými stranami, na ktoré sa zavedená povinnosť vzťahuje. Považujeme za nevyhnutné riešiť v rámci širšej odbornej a celospoločenskej diskusie, vypracovať k nim podrobnú analýzu vplyvov, ich právne posúdenie a navrhujeme ich preto z predkladaného návrhu zákona vypustiť. Túto pripomienku považujeme za zásadnú.			
MVSR	19. K bodu 33 navrhujeme vypustiť celý bod 33. Odôvodnenie: Úrad si navrhuje novú úlohu/oprávnenie, a to rozhodovať o blokovaní pri riešení kybernetického bezpečnostného incidentu, pričom na základe uvedeného zákona v poznámke pod čiarou 28a – zákon Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov neumožňuje žiadať blokovanie. Predkladateľ v dôvodovej správe uvádza, že sa jedná o zhmotnenie vznesenej spoločenskej požiadavky efektívneho zamedzovania škodlivých aktivít alebo škodlivého obsahu na internete, hoci takúto spoločenskú objednávku, či požiadavku sme nezaznamenali. Uvedené preto považujeme za nevyhnutné riešiť v rámci širšej odbornej a celospoločenskej diskusie, vypracovať k nim podrobnú analýzu vplyvov, ich právne posúdenie a navrhujeme ich preto z predkladaného návrhu zákona vypustiť. Ide o ďalšie oprávnenie úradu, pri ktorom absentujú konkrétne pravidlá zamedzujúce zneužitiu, ktoré je nepredvídateľné a nie je možné sa voči nemu účinne (právne) brániť. V budúcnosti nie je možné vylúčiť zavedenie kompetencie blokovania do právneho poriadku, avšak s jasnými pravidlami, podmienkami a obmedzeniami namiesto	Z	N	Vašu pripomienku nie je možné prakticky akceptovať, resp. ani vyhodnotiť, keďže neobsahuje žiadne konkrétne formulácie ani návrhy. Ďalej, z dôvodu pochopenia textu uvádzame, že blokovanie vykonáva úrad už dnes ako riešenie závažného kybernetického incidentu. Blokovanie je riešenie ultima ratio (subsidiarita represie). Na základe plošnej požiadavky z minulého roka došlo k formulovaniu nástroja aj ako výkonu rozhodnutia pre iné orgány verejnej moci (zásah je potrebné vykonať s odbornou zručnosťou a odborným spôsobom). Návrh zákona bol predmetom PPK a aktuálna platforma predstavuje možnosť vyjadriť sa formulovať konkrétne požiadavky a výhrady širokému spektru subjektov (účel MPK). Zákon obsahuje určenie zodpovednosti

	neurčitého uvedenia „pri riešení kybernetického bezpečnostného incidentu“. Výkon rozhodnutia o blokovaní totižto môže predstavovať významný zásah do základných práv a slobôd, napr. do súkromného vlastníctva, preto by nemalo byť v kompetencii jediného štátneho orgánu v zásade bez akejkoľvek kontroly. Súčasne nie je na základe týchto ustanovení zrejмый proces, opravné prostriedky, kontrolné mechanizmy, nie je jasné, kto bude znášať náklady, ako bude úrad rozhodovať o blokovaní, na akej infraštruktúre bude vykonávať blokovanie, v akom rozsahu, aké údaje a mnohé ďalšie záležitosti. Uvedené je potrebné špecifikovať. Napr. v bode 10 návrhu sa hovorí o blokovaní škodlivého obsahu respektíve škodlivej aktivity, pričom ani jeden z týchto pojmov nebol doplnený do definícií. Túto pripomienku považujeme za zásadnú.			(úrad aj iný orgán- žiadateľ), opravný prostriedok (preskúmateľnosť súdom), splnomocňovacie ustanovenie na podrobnosti a spôsob blokovania (novelizačný bod 45) a rovnako dáva možnosť dotknutým orgánom vykonať legislatívne zmeny vo svojich právnych predpisoch tak, aby sa efektívny, účelný a účinným spôsobom dosiahla náprava a zamedzení škodlivých aktivít v našom kybernetickom priestore. Ustanovenie nebráni iným orgánom vo výkone svojich úloh, ustanovenie svojim cieľom napomáha ich efektívnej činnosti a nikoho nenúti, aby úrad žiadal o výkon takéhoto rozhodnutia.
MVSR	2. V návrhu zákona sa analýze rizík, resp. manažmentu rizík príkladá minimálny priestor, pričom ide o základný východiskový bod pri návrhu opatrení podobne ako to je v legislatíve EÚ a NATO.	O	A	
MVSR	20. K bodu 35 navrhujeme nahradiť slová „orgán posudzovania zhody podľa osobitného predpisu, 31) ktorý je akreditovaný ako orgán príslušný na posudzovanie zhody v oblasti kybernetickej bezpečnosti“ slovami „certifikovaný audítor kybernetickej bezpečnosti, 31a) ktorým je fyzická osoba a spoločník, alebo štatutárny orgán alebo zamestnanec právnickej osoby. Certifikáciu audítora kybernetickej bezpečnosti vykonáva osoba akreditovaná	O	ČA	

	podľa osobitného predpisu31b) ako orgán certifikujúci osoby31c) (Ďalej len „orgán certifikujúci osoby“) v oblasti kybernetickej bezpečnosti“.			
MVSR	21. K bodu 38 je potrebné vypustiť text „alebo zasielať automatizovaným spôsobom a v rozsahu ustanovenom v štandarde úradu určené systémové informácie zo sietí a informačných systémov podľa § 24 ods. 7.“. Odôvodnenie: V uvedenej podobe môže slúžiť k narušeniu dôvernosti systému prevádzkovateľa informačného systému, nakoľko umožňuje žiadať aj systémové údaje, ktoré majú dôverný charakter. Zároveň nie je špecifikovaný spôsob automatizovaného odosielania, na koho náklady sa takéto odosielanie bude vykonávať a po akú dobu sa budú takéto údaje a za akých podmienok uchovávať. Okrem toho zasielanie informácií automatizovaným spôsobom prinesie subjektom dodatočné finančné náklady na prevádzku systémov, ktoré nie sú nijakým spôsobom uvedené v doložke vplyvov na rozpočet verejnej správy ani v doložke vplyvov na podnikateľské prostredie. Túto pripomienku považujeme za zásadnú.	Z	N	text je preformulovaný s ohľadom na iné vznesené pripomienky a je prepracovaný tak, aby predstavoval transparentný proces.
MVSR	22. K bodu 40 navrhujeme znížiť spodnú hranicu na od 0 eur v prípadoch kedy nedošlo k závažnému správnomu deliktu a nevznikla žiadna škoda a došlo k promptnej náprave stavu a vrchnú hranicu naviazať na napr. ročný obrat v predošliých rokoch nakoľko najmä u menších subjektov môže byť pokuta v hornom rozsahu likvidačná. Všeobecne odporúčame postupovať ako pri škodách v správnom poriadku.	O	N	

MVSR	23. K bodu 42 navrhujeme prehodnotiť celý bod 31a, kedy úrad u certifikátov kybernetickej bezpečnosti vydaných inou certifikačnou autoritou vydá napr. varovanie a zároveň bude kontaktovať danú certifikačnú autoritu s požiadavkou o prehodnotenie vydaného certifikátu.	O	N	
MVSR	24. K bodu 44 navrhujeme určiť periodicitu záväzne z dôvodu plánovania výdavkov na audity v nadväznosti k štandardizácii informačných systémov a harmonizovať v súlade so zákonom 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.	O	N	uvedene v paltnej vyhlaske NBU
MVSR	25. K bodu 46 navrhujeme zachovať pôvodné znenie a prerokovať ho so všetkými rezortmi. Odôvodnenie: Uvedené navrhujeme prerokovať s orgánmi príslušnými na tvorbu právnych predpisov, nakoľko máme za to, že úrad nie je oprávnený v rámci legislatívneho procesu udeľovať súhlas s vydaním, resp. v akejkoľvek fáze legislatívneho procesu schvaľovať vykonávací právny predpis iného ústredného orgánu. Toto považujeme za rozporné s pravidlami tvorby právnych predpisov, ide o prekračovanie právomocí úradu a navrhujeme novelizačný bod vypustiť. Túto pripomienku považujeme za zásadnú.	Z	A	
MVSR	26. Nad rámec návrhu - Z dôvodu úpravy v § 63 ods. 17 zákona č. 351/2011 Z. z. o elektronickej komunikácii v znení neskorších predpisov je potrebné upraviť zákon o kybernetickej bezpečnosti	Z	A	text upravený po dohode s gestorom

	tak, aby pre účely uvedenej úpravy zákona vznikol medzirezortný kontrolný orgán k činnosti úradu v časti aplikácie § 63 ods. 17 zákona 351/2020 Z. z. o elektronických komunikáciách. Zároveň nie je definovaný spôsob nakladania s takto získanými údajmi ani za akých podmienok a po akú dobu ich možno uchovávať. Zároveň navrhujeme aby pre nakladanie s odpočúvanou komunikáciou získaných zo štátnych orgánov bol požadovaný súhlas štatutára štátneho orgánu. Pri aplikovaní uvedeného je nevyhnutné prihliadať na ustanovenia 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. Vznik medzirezortného kontrolného orgánu navrhujeme aj pre kontrolu v tejto novele navrhovaného blokovania (navrhovaný bod 33). Túto pripomienku považujeme za zásadnú.			
MVSR	3. Niektoré vybrané ustanovenia zberu informácií (bod 31 návrhu zákona), zákazu alebo obmedzenia produktu, procesu alebo služby (bod 32 návrhu zákona), blokovania (bod 33 návrhu zákona) a odňatie certifikátu kybernetickej bezpečnosti (bod 42 návrhu zákona) (§ 24 ods. 7, § 27 ods. 1 písm. a) a § 27a), ktoré neboli predmetom konzultácií so zainteresovanými stranami, považujeme za nevyhnutné riešiť v rámci širšej odbornej a celospoločenskej diskusie, vypracovať k nim podrobnú analýzu vplyvov, ich právne posúdenie a navrhujeme ich preto z predkladaného návrhu zákona vypustiť. Odôvodnenie: Uvedené je nevyhnutné najmä v záujme zabezpečenia súladného legislatívneho postupu vychádzajúc z Legislatívnych pravidiel vlády SR ako aj z Jednotnej metodiky na	Z	N	Vašu pripomienku nie je možné akceptovať, keďže neobsahuje žiadne konkrétne formulácie ani konkrétne návrhy. Pripomienka je svojim znením opakujúca sa a platí odôvodnenie úradu ku konkrétny bodom vyššie. Čo sa týka certifikácie, uvádzame, že ide o implementáciu nariadenia nariadenia (EÚ) č. 2019/881.

	posudzovanie vplyvov. Ide najmä o otázky zberu informácií (§ 24 odsek 7 návrhu), zákazu alebo obmedzenia produktu, procesu alebo služby (§ 27 ods. 1 písm. e) návrhu), blokovania (§ 27a návrhu) a odňatie certifikátu kybernetickej bezpečnosti (§ 31a) sú veľmi citlivé otázky, kde okrem hrozby zneužitia moci voči konkrétnym osobám a subjektom bez existujúceho kontrolného mechanizmu, ktorý v danom rozsahu vôbec nie je riešený, môžu SR hroziť potenciálne žaloby pre podozrenia z nekalej obchodnej súťaže, prípadne narúšajúce princíp voľného trhu presadzovaného EÚ. Okrem toho nie sú ani vopred dané a vopred predvídateľné dôvody, kvôli ktorým je úrad oprávnený produkt zakázať alebo obmedziť. V neposlednom rade otázka odnímania certifikátu kybernetickej bezpečnosti (ktorý mimochodom nie je vôbec v návrhu zadaný) vydaného inou certifikačnou autoritou, napr. aj iného štátu, je sama o sebe veľmi citlivou záležitosťou. Uvedené ustanovenia nie sú žiadnym relevantným spôsobom zdôvodnené, pričom úplne absentuje ich analýza a vplyvy na podnikateľské prostredie a iné zainteresované subjekty a neboli zvážené ani možné právne dôsledky a s nimi súvisiace problémy. Navrhujeme preto zabezpečiť širšiu a dôkladnejšiu diskusiu s odbornou verejnosťou a akademickou obcou. Uvedené časti zákona navrhujeme vypustiť a po širokej odbornej diskusii ich v rámci iných legislatívnych konaní zásadne prepracovať. Túto pripomienku považujeme za zásadnú.			
MVSR	4. Účelom Európskeho toolbox-u kybernetickej bezpečnosti 5G sietí (ďalej len „EÚ Toolbox“), kde všetky aktivity vrátane vypracovania a poskytnutia podkladov do jednotného dokumentu „Spoločné európske posúdenie rizík súvisiacich s 5G sieťami“ za Slovenskú	Z	A	

republiku zabezpečoval Národný bezpečnostný úrad (ďalej len „úrad“), je primárne stanovenie spoločného súboru opatrení na zmiernenie rizík kybernetickej bezpečnosti 5G sietí. Táto oblasť zahŕňajúca najmä strategické opatrenia nie je v návrhu zákona vôbec pokrytá. Rovnako navrhujeme dopracovať do návrhu zákona koncept tzv. hybridných hrozieb a politických rizík. Odôvodnenie: Slovenská republika je spolu s ostatnými európskymi štátmi povinná implementovať požiadavky EÚ Toolbox-u a ich implementácia práve do návrhu zákona je logickým krokom, vzhľadom na skutočnosť, že návrh zákona predstavuje jediný právny predpis, ktorý vo všeobecnej rovine a naprieč všetkými sektormi a podsektormi ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti, a teda aj požiadavky na zaistenie bezpečnosti pre sektor elektronické komunikácie, podsektor siete a služby republiky pevných a mobilných elektronických komunikácií, kam patria aj 5G siete. Navyše úrad ako jediný vyhodnocoval za Slovenskú republiku riziká spojené s ich využívaním. Nevyhnutnosť implementácie EÚ Toolbox-u do právneho poriadku Slovenskej republiky bola zvýraznená aj prijatými závermi Európskej rady na jej mimoriadnom zasadnutí 1. a 2. októbra 2020 vid'. bod 11. „Európska rada schvaľuje závery Rady z 9. júna 2020 o formovaní digitálnej budúcnosti Európy. Vyzýva EÚ a členské štáty, aby v plnej miere využívali súbor nástrojov EÚ pre kybernetickú bezpečnosť 5G prijatý 29. januára 2020, a najmä aby uplatňovali príslušné obmedzenia týkajúce sa vysokorizikových dodávateľov v prípade kľúčových aktív, ktoré sú v koordinovaných posúdeniach rizík EÚ vymedzené ako kritické a citlivé. Európska rada zdôrazňuje, že potenciálni dodávatelia technológií 5G sa musia posudzovať na základe spoločných objektívnych kritérií. Túto			
--	--	--	--

	pripomienku považujeme za zásadnú.			
MVSR	5. Mnohé ustanovenia v návrhu zákona sú nad rámec vyžadujúceho z pohľadu legislatívy EÚ a nastavením prísnejších podmienok oproti krajinám EÚ môže v konečnom dôsledku dôjsť k znevýhodneniu subjektov riešiacich túto problematiku v SR. Samotné riešenie otázky certifikátov kybernetickej bezpečnosti je pravdepodobne predčasné vzhľadom na neexistenciu európskeho certifikačného rámca.	O	N	Vaša pripomienka nemá žiadne reálne odôvodnenie. Táto problematika bola predmetom dlhých odborných diskusií pri tvorbe zákona a predložená novela nejde nad rámec predmetu platného zákona o kybernetickej bezpečnosti
MVSR	7. K bodu 7 navrhujeme vypustiť celý bod 7. Odôvodnenie: Ustanovenie § 3 zákona sa dopĺňa novými definíciami, z ktorých definície pod písm. q) až t) sú definície uvedené a prebraté z nariadenia R a EP (EÚ) č. 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/ 2013 (ďalej len „akt o kybernetickej bezpečnosti“). Keďže vyššie spomenuté nariadenie je priamo aplikovateľné, bez nutnosti prijatia vnútroštátnej transpozičnej normy, nevyžaduje transpozíciu do vnútroštátnej právnej normy, dokonca ju vôbec nepripúšťa. Vzhľadom na priamu aplikovateľnosť nariadenia a zákaz bránenia tejto priamej aplikovateľnosti preberaním znenia nariadenia do vnútroštátnych predpisov navrhujeme definície v bodoch q) až t) vypustiť a nahradiť ich odkazmi na vyššie citovaný akt o kybernetickej bezpečnosti (čl. 2 body 9 – 14 aktu o kybernetickej bezpečnosti). Túto pripomienku považujeme za zásadnú.	Z	ČA	primerane upravené .Z dôvodu zaužívanej systematiky zákona, prehľadnosti, praktickej použiteľnosti a aj významnosti impementácie nariadenia sa úrad rozhodol, že na účely tohto zákona pojmy upraví.

MVSR	8. K bodu 10 V čl. I bod 10 navrhujeme upraviť, nakoľko uvedený návrh nie je dostatočne transparentný a môže mať v kombinácii s aplikovaním § 29 ods. 6 zákona nezanedbateľný dopad na štátny rozpočet a rozpočet podnikateľského sektoru. V odkaze pod čiarou 10aa) sa odkazuje na ešte neexistujúcu právnu normu (zákona o dohľade v oblasti ochrany spotrebiteľa) a v § 5 ods. 1 dopĺňané písmeno y) by úrad v otázke blokovania škodlivého obsahu vo vzťahu k informačným systémom prevádzkovanými rezortom ministerstva vnútra mal vydať odporúčanie na blokovanie škodlivého obsahu a samotnú realizáciu je potrebné ponechať na rezortnú jednotku CSIRT.	O	N	pripomienka neobsahuje konkrétne návrhy a nie je možné sa ňou relevantne zaoberať. Problematika je vyjasnená v rámci zásadných pripomienok.
MVSR	9. K bodu 11 z uvedeného bodu nie je zrejmý rozsah súčinnosti ani konkretizácia informácií, ktoré je úrad oprávnený od uvedených subjektov požadovať. Odôvodnenie: Podľa navrhovaného znenia je úrad oprávnený požadovať od vybraných subjektov poskytnutie súčinnosti, alebo informácií, ktoré sú potrebné na plnenie úloh podľa tohto zákona, pričom návrh ide ešte ďalej, keď hovorí, že tieto subjekty sú povinné úradu požadovanú súčinnosť, alebo informácie, ktoré sú potrebné na plnenie úloh podľa tohto zákona, aj poskytnúť. Z návrhu nie je zrejmé, aké informácie môže úrad požadovať, pričom napr. v prípade, že ide o osobitné kategórie údajov (napr. osobné údaje, utajované skutočnosti, bankové, daňové tajomstvo, lekárske tajomstvo, lokalizačné údaje a pod.) tieto vychádzajúc z iných právnych noriem ani subjekty poskytovať nemôžu. Žiadame preto jasne precizovať druh požadovaných informácií ako aj určenie jasného účelu spracúvania úradom (aby bolo zrejmé čo sa s danými	Z	A	Text preformulovaný tak, aby splňal predpoklady uvedené v pripomienkach.

	informáciami následne deje). Navyše, ak má oprávneniu úradu korešpondovať povinnosť uvedených subjektov súčinnosť alebo informáciu poskytnúť, toto je v mnohých prípadoch spojené s dodatočnými finančnými nákladmi (nakol'ko ide o novú povinnosť subjektov), a preto požadujeme jej kvantifikáciu a vyčíslenie aj v doložke vybraných vplyvov na jednotlivé subjekty (na rozpočet verejnej správy ako aj na podnikateľské prostredie). Túto pripomienku považujeme za zásadnú.			
MZSR	K bodu 14 Novelizčný bod 14, konkrétne § 9 ods. 2 návrhu zákona žiadame bez náhrady vypustiť. V prípade, ak by predkladateľ tento návrh neprijal, žiadame, aby mal rezort zdravotníctva z navrhovanej úpravy výnimku ako podsektor Obrana a podsektor Informačné systémy verejnej správy. Odôvodnenie: V súčasnosti platná právna úprava zákona č. 69/2018 Z. z. umožňuje, v prípade ústredného orgánu štátnej správy, ktorým je Ministerstvo zdravotníctva Slovenskej republiky a jeho podriadeným organizáciám, využívať služby Národnej jednotky CSIRT na základe zmluvy a zároveň umožňuje aj možnosť vybudovania si vlastnej jednotky CSIRT. V kontexte vzniku pandémie COVID-19 a vykonávania potrebných úloh na území Slovenskej republiky je navrhovaná úprava pre Ministerstvo zdravotníctva Slovenskej republiky ako cieľové riešenie pre heterogénne prostredie neprijateľné.	O	A	
MZSR	bodu 6.,19,22,31,32,33,44 1. K bodu 6 (§ 3 písm. h): Ustanovenie § 3 písm. h) doplnením slov „činnosti potrebné na ochranu sietí a informačných systémov, užívateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami,“ stratilo významovú správnosť a	O	ČA	

	zrozumiteľnosť textu. Odporúčame preformulovať alebo vypustiť . 2. K bodu 19 (§ 17): Dotknutý prevádzkovateľ základnej služby nemusí zaznamenať okamih, ktorým došlo k prekročení identifikačných kritérií. Uvedené môže znamenať neaplikovateľnosť ustanovenia. Z tohto dôvodu navrhujeme ponechať pôvodné znenie alebo doplniť do textu slová „ak zistí, že prekročil identifikačné kritériá“. 3. K bodu 22 (§18 ods. 4): Dotknutý prevádzkovateľ základnej služby nemusí zaznamenať okamih, ktorým došlo k prekročeniu špecifických sektorových kritérií. Uvedené môže znamenať neaplikovateľnosť ustanovenia. Z tohto dôvodu navrhujeme ponechať pôvodné znenie alebo doplniť do textu slová „ak zistí, že prekročil špecifické sektorové kritériá“. 4. K bodu 31 (§ 24 ods. 7): Odporúčame zvážiť, či implementácia automatizovaného zasielania údajov nebude mať negatívny finančný dopad na prevádzkovateľov základných služieb. Prevádzkovatelia základných služieb nebudú zrejme schopní plniť uvedenú zákonnú povinnosť. 5. K bodu 32 (§27 ods. 1 písm. e): Odporúčame zvážiť vhodnosť takejto kompetencie úradu. Zakázať alebo obmedziť prevádzkovateľovi základnej služby používať konkrétny produkt, je zásahom do fungovania jeho činnosti. Zmena technológií môže znamenať nutnosť úplnej výmeny hardvéru, softvéru či úplné znefunkčnenie poskytovania základných služieb. 6. K bodu 33 (§27a): Absentuje vymedzenie pojmov „prevádzkovateľ infraštruktúry“, „škodlivý obsah“ a „škodlivá aktivita“. Odporúčame doplniť. 7. K bodu 44 (§32 ods. 1 písm. f): Periodicita auditu má zásadný dopad na prevádzkovateľa základných služieb. Z tohto dôvodu navrhujeme doplniť periodicitu určenia časového intervalu auditu (každé dva roky) priamo do zákona a v tom prípade zodpovedajúco upraviť aj splnomocňovacie ustanovenie § 32			
--	--	--	--	--

	zákona. 8. Nad rámec návrhu upozorňujeme na potrebu zosúladenia terminológie, použitej vo vyhláske 164/2018 Z. z., ktorou sa určujú identifikačné kritéria prevádzkovej služby (kritéria v základnej služby) so zákonom 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov a so zákonom č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov - konkrétne napr. definícia akútneho lôžka, ktorá je uvedená v Prílohe č.1 Vyhlášky 164/2018 Z. z., oblasť Zdravníctvo, Špecifické sektorové kritériá, sa v zákone nenachádza .			
MZSR	K bodu 52 (Príloha 1, riadok 10) K bodu 52 (Príloha č. 1): V zmysle § 3 písm. k.) druhého bodu zákona informačným systémom verejnej správy sú zdravotnícke zariadenia zaradené medzi poskytovateľov základnej služby v sektore verejnej správy t. j. aj tie, ktoré nespĺňajú sektorové a dopadové kritériá zdravotníckych zariadení podľa riadku (sektoru 11) Prílohy č. 1 . Z toho dôvodu navrhujeme do Prílohy č. 1 riadok 10 (verejná správa) doplniť slová „ s výnimkou zdravotníckych zariadení“. Táto pripomienka je zásadná.	Z	N	Kategorizácia je závislá na splnení identifikačných kritérií
MZVEZ SR	K čl. I bodu 32 § 27 ods. 1 písm. e) odporúčame formulovať takto: „e) rozhodnúť o zákaze alebo obmedzení prevádzkovateľa základnej služby používať konkrétny produkt, proces alebo službu, ak je to potrebné na zaistenie kybernetickej bezpečnosti, alebo z dôvodov bezpečnostného záujmu Slovenskej republiky. V prípade, ak predmetné rozhodnutie má alebo môže mať zahraničnopolitický	O	N	text preformulovaný aj s ohľadom na iné vznesené pripomienky

	dosah, bude ho úrad vopred konzultovať s Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky.“. Odôvodnenie: V zmysle novelizačného bodu 32 môže Národný bezpečnostný úrad rozhodnúť o zákaze alebo obmedzení prevádzkovateľa základnej služby používať konkrétny produkt, proces alebo službu, ak je to potrebné na zaistenie kybernetickej bezpečnosti, alebo z dôvodov bezpečnostného záujmu SR. Tieto služby môžu byť poskytované zahraničným ekonomickým subjektom pôsobiacim v Slovenskej republike, resp. nimi poskytované, a teda zásah voči nim môže mať dopad na naše zahraničnopolitické záujmy a bilaterálne vzťahy s krajinami ich pôvodu. Z tohto dôvodu odporúčame, aby Národný bezpečnostný úrad bol zaviazaný takéto rozhodnutie vopred konzultovať s Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky.			
MZVEZ SR	K čl. I bodu 32 K navrhovanému zneniu § 27 ods. 1 písm. e) odporúčame vytvoriť verejne dostupnú databázu o produktoch, procesoch a službách, ktoré majú certifikát kybernetickej bezpečnosti (vrátane produktov certifikovaných v rámci EÚ). Odôvodnenie: Takáto databáza produktov, procesov a služieb umožní z pohľadu prevádzkovateľa základnej služby ako verejného obstarávateľa nastaviť transparentné kritériá verejného obstarávania, ktoré zamedzia potencionálnym uchádzačom ponúkať zakázané produkty, procesy a služby ohrozujúce kybernetickú bezpečnosť alebo bezpečnostné záujmy SR.	O	A	všetky informácie sú zverejňované v jednotnom informačnom systéme kybernetickej bezpečnosti
MZVEZ SR	K čl. I bodu 32 K navrhovanému zneniu § 27 ods. 1 písm. e) odporúčame doplniť	O	N	uvedené bude vzhľadom na konkrétne okolnosti predmetom vydaného

	ustanovenie o prechodnom období, počas ktorého môže prevádzkovateľ základnej služby naďalej využívať zakázaný produkt, proces alebo službu. Odôvodnenie: navrhované ustanovenie umožňuje úradu zakázať využívanie niektorých produktov, procesov alebo službu, ak je to potrebné na zaistenie kybernetickej bezpečnosti SR alebo z dôvodu bezpečnostného záujmu SR. Ustanovenie v takomto znení však vystavuje prevádzkovateľa základnej služby neprimeranému riziku, že bude musieť okamžite po rozhodnutí úradu prestať používať zakázaný produkt, proces alebo službu bez pripraveného adekvátneho riešenia, čo z pohľadu prebiehajúcich alebo budúcich zmluvných vzťahov vytvára právnu neistotu a nestabilitu. Zároveň, prevádzkovateľ verejnej služby v postavení verejného obstarávateľa je nútený dodržiavať ustanovenia zákona o verejnom obstarávaní a uvedené rozhodnutie by malo vplyv na transparentnosť verejných obstarávaní z dôvodu, že úrad môže zakázať využívanie produktov, procesov alebo služieb, ktoré boli transparentne vysúťažené a splnili všetky požiadavky na bezpečnosť nastavené zo strany verejného obstarávateľa, keďže rozhodnutie úradu môže byť prijaté po ukončení procesu verejného obstarávania. Uvedená formulácia taktiež vytvára dodatočné náklady na rozpočet prevádzkovateľa základnej služby, ktorý bude musieť takýmto rozhodnutím okamžite prestať využívať zakázaný produkt, proces alebo službu pred ukončením ich životného cyklu a štandardným procesom výmeny. Eventuálne možno uvažovať o novelizácii zákona o verejnom obstarávaní, ktorá by umožnila efektívne nahradiť zakázaný produkt, proces alebo službu tak, aby zostali zachované funkcie prevádzkovateľa základnej služby a boli splnené bezpečnostné požiadavky.		rozhodnutia. Nie je možné zovšeobecniť vami požadovanú pripomienku.
--	--	--	--

MZVEZ SR	K čl. I bodu 32 K navrhovanému zneniu § 27 ods. 1 písm. e) odporúčame vytvoriť verejne dostupnú databázu rozhodnutí úradu o zákaze využívania produktov, procesov a služieb. Odôvodnenie: Takáto databáza zakázaných produktov, procesov a služieb umožní z pohľadu prevádzkovateľa základnej služby ako verejného obstarávateľa nastaviť transparentné kritériá verejného obstarávania, ktoré zamedzia potencionálnym uchádzačom ponúkať zakázané produkty, procesy a služby ohrozujúce kybernetickú bezpečnosť a lebo bezpečnostné záujmy SR.	O	A	všetky informácie sú zverejňované v jednotnom informačnom systéme kybernetickej bezpečnosti
MZVEZ SR	K čl. I bodu 19 Odporúčame vypustiť bod 19 a ponechať pôvodné znenie § 17 ods. 1. Odôvodnenie: Navrhované znenie prenáša zodpovednosť na prevádzkovateľa služby neustále monitorovať prekročenie identifikačných kritérií a do 30 dní od tohto prekročenia oznámiť úradu, že tieto kritériá prekročil, pričom v pôvodnom znení bola táto oznamovacia povinnosť naviazaná na moment, kedy sa prevádzkovateľ dozvedel o prekročení. Zároveň navrhujeme doplniť metodiku výpočtu plnenia jednotlivých identifikačných kritérií či už vo vzťahu k samoidentifikácii, ako aj metodiku monitoringu a vyhodnocovania ukazovateľov, ktoré musí prevádzkovateľ základnej služby vyhodnocovať, keďže z aplikačnej praxe vyplýva, že je mimoriadne ťažké spoľahlivo a jednoznačne identifikovať vybrané kritériá, resp. identifikovať ich prekročenie.	O	ČA	
MZVEZ SR	K čl. I bodu 24 V § 19 ods. 2 odporúčame vypustiť slová „pri uzatvorení zmluvy sa analyzujú riziká podľa § 20 ods. 3 písm. b) zákona,“. Odôvodnenie: Analýza rizík je dokument vytvorený pre každý informačný systém	O	N	platí predpoklad v pripomienke, že PZS musí vyhodnocovať riziká už pred VO a podmienky nastaviť tak, aby boli splniteľné požiadavky bezpečnosti.

	a jej súčasťou je aj posúdenie toho, aké riziká sú spojené s prístupom tretích strán do tohto systému alebo na jeho správu. Uvedené znenie vytvára povinnosť pre prevádzkovateľa základnej služby pri uzatváraní každej zmluvy osobitne posudzovať riziká, ktoré predstavuje konkrétny poskytovateľ, čo je spojené s dodatočnou administratívnou a ťažko vykonateľnou povinnosťou, pričom už pri samotnej zmluve s poskytovateľom služieb prevádzkovateľ základnej služby ustanovuje základné podmienky a bezpečnostné kritériá, ktoré sa poskytovateľ zaväzuje dodržiavať. Táto povinnosť je ťažko vykonateľná najmä po realizácii procesu verejného obstarávania, keďže verejný obstarávateľ musí už pri nastavovaní kritérií podmienok účasti v súťaži nastaviť rôzne bezpečnostné požiadavky tak, aby boli splnené požiadavky na bezpečnosť dodávaného produktu alebo služby a poskytovateľ/dodávateľ mohol plniť predmet zákazky.			Analýza rizík sa vyhodnocuje v celom životnom cykle a je základným predpokladom dostatočného nastavenia opatrení zaisťujúcich kybernetickú bezpečnosť. Analýza okrem toho vytvára prehľad o aktuálnom stave aktív a dokáže v zájomných súvislostiach predikovať budúci stav.
MZVEZ SR	K doložke zlučiteľnosti V bode 3. doložky zlučiteľnosti odporúčame doplniť gestora smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 a nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881. V bode 4 písm. a) doložky zlučiteľnosti navrhujeme doplniť lehotu na prebratie smernice 2016/1148 a doplniť lehotu na implementáciu ostatných ustanovení nariadenia 2019/881.	O	A	
MZVEZ SR	K čl. III bodu 5 V bode 5 odporúčame na konci pripojiť vetu: „Doterajšie písmená j) a k)“ sa označujú ako písmená i) a j). V súvislosti s vypustením splnomocňovacieho ustanovenia z § 31 písm. i) odporúčame súčasne zrušiť alebo novelizovať tie vykonávacie predpisy, ktoré boli vydané na jeho základe, a to aj s poukazom na dôvodovú správu k čl. III, v	O	A	

	ktorej sa uvádza, že „ak budú potrebné prísnejšie opatrenia, budú upravené v sektorovej vyhláške podľa § 32 ods. 2 zákona o kybernetickej bezpečnosti“.			
MZVEZ SR	K vlastnému materiálu V čl. I úvodnej vete odporúčame slová „neskorších predpisov“ nahradiť slovami „zákona č. 373/2018 Z. z. a zákona č. 134/2020 Z. z.“. V bode 5 odporúčame slovo „prípadne“ nahradiť slovom „alebo“. V bode 12 v poznámkach pod čiarou k odkazom 10ac až 10ah odporúčame citované predpisy vložiť do úvodzoviek a novelizačný bod ukončiť bodkou. V bode 28 odporúčame úvodnú vetu formulovať takto: „V § 20 ods. 4 sa vkladá nové písmeno a), ktoré znie:“. V bode 39 úvodnej vete odporúčame slová „ods. 5“ nahradiť slovami „odsek 5“. V bode 40 poslednej vete odporúčame slovo „písmená“ nahradiť slovom „odseky“. V bode 42 ods. 2 písm. b) a c) odporúčame slová „podľa č. 58“ nahradiť slovami „podľa článku 58“. V čl. III úvodnej vete odporúčame vypustiť slová „a dopĺňa“. V čl. IV úvodnej vete odporúčame vypustiť slová „mení a“. Legislatívno-technické pripomienky.	O	A	
MZVEZ SR	K bodu 10 V poznámke pod čiarou k odkazu 10aa odporúčame vypustiť slová „§ 11 zákona č. .../2020 Z. z. o dohľade v oblasti ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov.“. Odôvodnenie: Uvedené ustanovenie odkazuje na zatiaľ neexistujúci zákon, ku ktorému sa nie je možné relevantne vyjadriť.	O	A	
MZVEZ SR	K čl. I bodom 11 a 39 Z návrhu zákona žiadame vypustiť bod 11 (§ 5 ods. 4) a v bode 39 žiadame vypustiť § 31 ods. 5 písm. a). Odôvodnenie: Podľa	O	ČA	text preformulovaný aj s ohľadom na iné vznesené pripomienky

navrhovaného § 5 ods. 4 je Národný bezpečnostný úrad (ďalej len „úrad“) oprávnený požadovať od ústredných orgánov, prevádzkovateľov základnej služby, orgánov verejnej moci a právnických osôb poskytnutie súčinnosti, alebo informácií, ktoré sú potrebné na plnenie úloh podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon“) a tieto subjekty sú povinné úradu požadovanú súčinnosť alebo informácie poskytnúť. V nadväznosti na navrhovanú povinnosť sa v § 31 ods. 5 písm. a) návrhu zákona ustanovuje sankcia za jej nesplnenie vo forme pokuty až do výšky 100 000 eur. Upozorňujeme, že povinnosť ústredných orgánov, prevádzkovateľov základnej služby a orgánov verejnej moci poskytovať súčinnosť a informácie úradu už v súčasnosti vyplýva z ustanovení § 9 ods. 1 písm. b), § 10 ods. 2 a § 19 ods. 6 písm. c) zákona aj s ustanovenými sankciami za jej nesplnenie pokiaľ ide o prevádzkovateľov základnej služby. Návrhom zákona sa tak, vo vzťahu k zákonom ustanovenej povinnosti dotknutých subjektov poskytnúť úradu súčinnosť a informácie, vytvára duplicitná úprava. Predmetné ustanovenie je nejednoznačné aj vo vzťahu k subjektom tejto povinnosti, keďže povinnosť súčinnosti sa ukladá ústredným orgánom a aj orgánom verejnej moci, avšak z ustanovenia § 4 zákona vyplýva, že na účely zákona sa za orgány verejnej moci považujú aj ústredné orgány taxatívne vymenované v § 4 písm. b) zákona. Na základe uvedeného žiadame vypustenie predmetných ustanovení a súčasne na účely právnej istoty a jednoznačnosti výkladu zákona žiadame, aby boli ustanovené sankcie za porušenie konkrétnych a jednoznačne formulovaných zákonom ustanovených povinností v oblasti kybernetickej			
--	--	--	--

	bezpečnosti.			
NBS	čl. I bodu 10 1. V čl. I bode 10 úvodnej vete je potrebné slová „až ac)“ nahradiť slovami „až ad“.	O	A	
NBS	k čl. I bodu 10 2. V čl. I § 5 ods. 1 písm. y) nevieme vecne posúdiť obsah navrhnutého ustanovenia, pretože odkazuje na § 35ea zákona č. 747/2004 Z. z. o dohľade nad finančným trhom, ako aj na zákon o dohľade v oblasti ochrany spotrebiteľa, ktorých obsah nepoznáme. Návrhy týchto zákonov boli predmetom medzirezortného pripomienkového konania (LP/2019/496), avšak doteraz neboli schválené, nemáme vedomosť, že by sa v ich legislatívnom procese aktuálne pokračovalo. V podobe, v akej je návrh zákona predložený do medzirezortného pripomienkového konania, nespĺňa základné atribúty kladené na právny predpis a ustanovené v § 3 ods. 2 zákona č. 400/2015 Z. z. o tvorbe právnych predpisov a o Zbierke zákonov Slovenskej republiky a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, nespĺňa atribút všeobecnej zrozumiteľnosti. Rovnako nie je dodržaný bod 22.11. Legislatívnych pravidiel vlády Slovenskej republiky. Táto pripomienka platí primerane aj pre novelizačný bod 33, v súvislosti s ktorým by Národná banka Slovenska mala mať právomoc rozhodovať o blokovaní (§ 27a), avšak NBS takúto právomoc podľa platného právneho stavu nemá. Z uvedených dôvodov žiadame spresnenie uvedených ustanovení, resp. predloženie návrhu zákona do medzirezortného pripomienkového konania až vtedy, keď budeme vedieť v celom rozsahu posúdiť návrh právneho predpisu a jeho dôsledky pre Národnú banku Slovenska. Tieto pripomienky sú	Z	A	

	zásadné.			
NBS	k čl. I bodu 10 3. V poznámke pod čiarou k odkazu 10aa je pri citácii § 35ea zákona č. 747/2004 Z. z. potrebné vypustiť slová „o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov“. 4. V poznámke pod čiarou k odkazu 10ab odporúčame vypustiť písmeno „č.“ v slovnom spojení „(EÚ) č. 2019/881“ a za slová „(akt o kybernetickej bezpečnosti)“ doplniť publikačný zdroj predmetného nariadenia „(Ú. v. EÚ L 151, 7.6.2019).“	O	A	
NBS	k čl. I bodu 40 a 42 K čl. I bodom 40 a 42 V čl. I bodoch 40 a 42 návrhu zákona odporúčame odkazy na jednotlivé ustanovenia nariadenia (EÚ) 2019/881 uviesť formou poznámok pod čiarou a v slovnom spojení „(EÚ) č. 2019/881“ vypustiť písmeno „č.“.	O	A	
NBS	k čl. I bodu 11 K čl. I bodu 11 V čl. I bode 11 navrhujeme na konci druhej vety bodku nahradiť bodkočiarkou a doplniť tieto slová: „to neplatí, ak by mohlo dôjsť k zmareniu alebo ohrozeniu výkonu dohľadu podľa osobitného predpisu) a nie je tým dotknutá ochrana utajovaných skutočností, osobných údajov, bankového tajomstva, daňového tajomstva a iných informácií utajovaných alebo chránených povinnosťou mlčanlivosti výslovne uloženou alebo uznanou podľa osobitných predpisov.y) Poznámky pod čiarou k odkazom x a y znejú: x) Zákon č. 747/2004 Z. z. v znení neskorších predpisov. y) Napríklad čl. 37 ods. 37.1 Protokolu (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky v platnom znení (Ú. v. EÚ C 202, 7.6.2016), zákon č. 483/2001 Z. z. v znení	O	N	je obsahom § 12 ods 1 platného znenia

	neskorších predpisov, zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.“. Odôvodnenie: Keďže sa zákon o kybernetickej bezpečnosti na Národnú banku Slovenska nevzťahuje, navrhujeme z hľadiska právnej istoty a explicitného vyjadrenia v tomto ustanovení, že predkladateľom navrhovaná právna úprava nezasahuje do existujúcej právnej úpravy osobitných právnych predpisov v danej oblasti, a tiež z dôvodu, že Národná banka Slovenska by mohla poskytnúť len informácie, ktoré nezmária jej dohľadové činnosti.			
NBS	k čl. I bodu 12, 21, 24 a 28 K čl. I bodu 12 V čl. I bode 12 návrhu zákona odporúčame v poznámkach pod čiarou k odkazom 10ac a 10ae až 10ah vypustiť písmeno „č.“ v slovnom spojení „(EÚ) č. 2019/881“. K čl. I bodu 21 V čl. I v § 17 ods. 8 prvej vete navrhujeme na konci doplniť slová „odo dňa doručenia žiadosti o výmaz“, a to z dôvodu, že z hľadiska právnej istoty je potrebné uviesť skutočnosť, od ktorej bude plynúť lehota na rozhodnutie úradu vo veci žiadosti o výmaz. K čl. I bodu 24 V čl. I bode 24 navrhujeme spresniť, kto sa rozumie treťou stranou; legislatívnu skratku zavedenú v § 19 ods. 2 platného znenia zákona novelizované ustanovenie už neobsahuje. K čl. I bodu 28 V čl. I bode 28 navrhujeme úvodnú vetu upraviť takto: „V § 20 ods. 4 sa vkladá nové písmeno a), ktoré znie:“.	O	A	
NBS	k čl. I bodu 33 K čl. I bodu 33 1. V súvislosti s novým ustanovením § 27a navrhujeme zvážiť do návrhu zákona vložiť spresňujúce ustanovenie v tom zmysle, aký je vzťah medzi všeobecnou výnimkou ustanovenou v § 2 ods. 2 písm. d), ktorá sektor bankovníctva,	Z	N	Vaša pripomienka je obsiahnutá v texte návrhu. Žiadateľ o blokovanie pred vydaním vlastného rozhodnutia, na základe ktorého sa má blokovanie vykonať spolupracuje s úradom. Bližšie

	financií a finančný systém vyníma spod pôsobnosti zákona o kybernetickej bezpečnosti a právomocou úradu vykonávať blokovanie. Z predloženého znenia návrhu zákona nie je jednoznačné, či v prípade, ak bude potrebné vykonať blokovanie vo vzťahu k dohliadanému subjektu finančného trhu (napríklad úverovej inštitúcii), s čím návrh zákona výslovne počíta, keďže v poznámke pod čiarou odkazuje na zákon č. 747/2004 Z. z., môže úrad postupovať podľa § 27a zákona o kybernetickej bezpečnosti s ohľadom na výnimku ustanovenú v § 2 ods. 2 písm. d). 2. Navrhované znenie ustanovenia § 27a ods. 8 návrhu zákona sa nám javí ako nevyvážené v právach a povinnostiach, nakoľko žiadateľ o blokovanie, ktorým môže byť aj NBS, je zodpovedný za škodu súvisiacu s vykonaním blokovaní a znáša aj náklady za blokovanie ako také, avšak o spôsobe blokovaní rozhoduje úrad, ktorý aj zabezpečuje vykonanie blokovaní. Požadujeme toto ustanovenie upraviť v tom zmysle, že každý subjekt by mal byť zodpovedný za škodu iba v časti (rozsahu) svojho rozhodnutia. Zodpovednosť za škodu súvisiacu s rozhodnutím o spôsobe blokovaní a vykonaním blokovaní by mal znášať subjekt, ktorý škodu svojím konaním spôsobil. Z návrhu zákona taktiež nie je zrejmé, v akej výške sa náklady za blokovanie budú uhrádzať, nie je uvedený ani spôsob výpočtu nákladov. Tieto pripomienky sú zásadné.			upravené v DS
NBS	k čl. I úvodnej vete K čl. I úvodnej vete Čl. I úvodnú vetu je potrebné upraviť v súlade s bodom 28.1. Legislatívnych pravidiel vlády Slovenskej republiky, a to slová „v znení neskorších predpisov“ nahradiť slovami „v znení zákona č. 373/2018 Z. z. a zákona č. 134/2020 Z. z.“.	O	A	

NBS	k čl. V K čl. V V čl. V je potrebné doplniť účinnosť návrhu zákona.	O	A	
NBS	k doložke zlučiteľnosti K doložke zlučiteľnosti Formu a obsah doložky zlučiteľnosti odporúčame upraviť podľa platných Legislatívnych pravidiel vlády SR.	O	A	
NBS	k osobitnej časti dôvodovej správy K osobitnej časti dôvodovej správy 1. V časti k bodu 1 odporúčame za slová „v Únii“ doplniť publikačný zdroj predmetnej smernice „(Ú. v. EÚ L 194, 19.7.2016)“. 2. V časti k bodu 4 a 5 odporúčame slová „Smernice Európskeho parlamentu a Rady č. 2002/21/ES o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica)“ nahradiť slovami „smernice Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica) (Ú. v. ES L 108, 24.4.2002; Mimoriadne vydanie Ú. v. EÚ kap. 13/zv. 029) v platnom znení“. 3. Pre časť k bodu 33 platí primerane pripomienka č. 1. písm. a) tohto stanoviska. 4. V celej osobitnej časti dôvodovej správy odporúčame vypustiť písmeno „č.“ v slovnom spojení „(EÚ) č. 2019/881“; táto pripomienka platí aj pre doložku vybraných vplyvov.	O	A	
NBS	k predkladacej správe K predkladacej správe V druhom odseku predkladacej správy odporúčame za slová „(akt o kybernetickej bezpečnosti)“ doplniť publikačný zdroj predmetného nariadenia „(Ú. v. EÚ L 151, 7.6.2019)“; to platí primerane aj pre všeobecnú časť dôvodovej	O	A	

	správy k návrhu zákona.			
RÚZSR	20. Zásadná pripomienka k čl. I., novelizačný bod 24 v časti §19 odsek 3 V § 19 ods. 3 navrhujeme nasledovné doplnenie: „(3) Povinnosť uzatvoriť zmluvu podľa odseku 2 neplatí, ak je tretia strana prevádzkovateľom základnej služby alebo poskytovateľom digitálnej služby alebo podnikom na poskytovanie elektronických komunikačných služieb alebo sietí podľa osobitného predpisu x), x) Doplniť aj poznámku s odkazom na príslušné ust. zákona č. 351/2011 Z. z. Taktiež navrhujeme doplniť ustanovenie tak, aby sa uplatňovalo aj na prevádzkovateľov základnej služby, resp. poskytovateľov digitálnej služby v inom členskom štáte EÚ v zmysle článku 5 resp. článku 4 ods. 6 Smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.“ Odôvodnenie: Navrhujeme aby sa jednoznačne vylúčili aj podniky poskytujúce verejné služby a siete pre prípad, ak by nespádali do skupiny PZS resp. poskytovateľov digitálnych služieb. Podniky elektronických komunikácií musia inak pri poskytovaní sietí a služieb implementovať primerané bezpečnostné opatrenia už na základe ustanovení §64 zák. č. 351/2011 Z. z. o elektronických komunikáciách a prenášanie ďalších individuálnych bezpečnostných opatrení na podniky, by bolo nevykonateľné a nesystémové. Verejné elektronické komunikačné služby sú totiž poskytované všetkým účastníkom v rovnakom rozsahu a za rovnakých podmienok z hľadiska dostupnosti a kvality. Nie je teda možné, aby zmluvy s účastníkmi definovali individuálne požiadavky na bezpečnosť sietí a služieb. Domnievame sa, že za	Z	A	Obsah Vašej pripomienky je uvedený v odseku 2.

	účelom dodržania základných princípov vnútorného trhu EÚ a to princípu rovnakého zaobchádzania a zákazu diskriminácie by prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb z iných členských štátov EÚ mali byť posudzovaní rovnako ako prevádzkovatelia základných služieb registrovaní v zozname prevádzkovateľov základných služieb a poskytovatelia digitálnej služby v zmysle ZoKB a na zmluvy, ktoré s nimi uzatvárajú domáci prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb by sa nemal uplatňovať prísnejší režim. Pokiaľ nedôjde k zrovnoprávneniu postavenia ekvivalentných zahraničných prevádzkovateľov základnej služby a poskytovateľov digitálnej služby s domácimi subjektmi toto ustanovenie v predloženom znení novely ZoKB je spôsobilé neodôvodnene obmedziť slobodu poskytovať služby v zmysle článku 56 ZFEÚ			
RÚZSR	1. Všeobecná zásadná pripomienka k návrhu ako celku A. Použitá terminológia a najmä jej zmeny spôsobia rozdielne definície rovnakých alebo podobných pojmov v rôznych právnych predpisoch. Terminológia je nekonzistentná, rozporuplná a neúplná. Odporúčame preto zadefinovať v spolupráci s odborníkmi v danej oblasti a akademickou obcou odbornú terminológiu pre oblasť kybernetickej bezpečnosti. Ako optimálne navrhujeme po vzore napr. Českej republiky vydať ‘Výkladový slovník Kybernetické bezpečnosti’, ktorý bol v Českej republike vydaný v spolupráci s českou pobočkou AFCEA a pod záštitou NBÚ ČR a NÚKIB. Po ustálení odbornej terminológie potom túto následne používať vo všetkých právnych predpisoch jednotným a konzistentným spôsobom. B. V návrhu zákona sa analýze rizík resp. manažmentu rizík prikladá minimálny priestor pričom ide o základný	Z	ČA	predkladateľ vzal pripomienku na vedomie a pojmy upravil

	východiskový bod pri návrhu opatrení podobne ako to je v legislatíve EÚ a NATO. C. Niektoré vybrané ustanovenia zberu informácií (bod 31 návrhu zákona), zákazu alebo obmedzenia produktu, procesu alebo služby (bod 32 návrhu zákona), blokovania (bod 33 návrhu zákona) a odňatie certifikátu kybernetickej bezpečnosti (bod 42 návrhu zákona) (§ 24 ods. 7, § 27 ods. 1 písm. a) a § 27a), ktoré neboli predmetom predbežnej informácie k novele zákona a teda ani predmetom konzultácií so zainteresovanými stranami považujeme za nevyhnutné riešiť v rámci širšej odbornej a celospoločenskej diskusie, vypracovať k nim podrobnú analýzu vplyvov, ich právne posúdenie a navrhujeme ich preto z predkladaného návrhu zákona vypustiť. Uvedené je nevyhnutné najmä v záujme zabezpečenia súladného legislatívneho postupu vychádzajúc z Legislatívnych pravidiel vlády SR ako aj z Jednotnej metodiky na posudzovanie vplyvov. Ide najmä o otázky zberu informácií (§ 24 odsek 7 návrhu), zákazu alebo obmedzenia produktu, procesu alebo služby (§ 27 odsek 1 písmeno e) návrhu), blokovania (§27a návrhu) a odňatie certifikátu kybernetickej bezpečnosti (§ 31a) sú veľmi citlivé otázky, kde okrem hrozby zneužitia moci voči konkrétnym osobám a subjektom bez existujúceho kontrolného mechanizmu, ktorý v danom rozsahu vôbec nie je riešený, môžu SR hroziť potencionálne žaloby pre podozrenia z nekalej obchodnej súťaže, prípadne narúšajúce princíp voľného trhu presadzovaného EÚ. Naviac nie sú ani vopred dané a vopred predvídateľné dôvody, kvôli ktorým je úrad oprávnený produkt zakázať alebo obmedziť. V neposlednom rade otázka odnímania certifikátu kybernetickej bezpečnosti (ktorý mimochodom nie je vôbec v návrhu zadefinovaný) vydaného inou certifikačnou autoritou napr. aj iného štátu je sama o sebe veľmi			
--	--	--	--	--

	citlivou záležitostí. Uvedené ustanovenia nie sú žiadnym relevantným spôsobom zdôvodnené, pričom úplne absentuje ich analýza a vplyvy na podnikateľské prostredie a iné zainteresované subjekty a neboli zvážené ani možné právne dôsledky a s nimi súvisiace problémy. Navrhujeme preto zabezpečiť širšiu a dôkladnejšiu diskusiu s odbornou verejnosťou a akademickou obcou. Uvedené časti zákona navrhujeme vypustiť a po širokej odbornej diskusii ich v rámci iných legislatívnych konaní zásadne prepracovať. D. Mnohé ustanovenia v návrhu zákona sú nad rámec vyžadujúceho z pohľadu legislatívy EÚ a nastavením prísnejších podmienok oproti krajinám EÚ môže v konečnom dôsledku dôjsť k znevýhodneniu subjektov riešiacich túto problematiku v SR. Samotné riešenie otázky certifikátov kybernetickej bezpečnosti je pravdepodobne predčasné vzhľadom na neexistenciu európskeho certifikačného rámca. E. Vzhľadom na potrebu širšej a dôkladnejšej diskusie s odbornou a akademickou obcou navrhujeme predmetný návrh zmeny zákona stiahnuť a vypracovať nový upravujúci vhodným spôsobom najmä sporné a citlivé oblasti vrátane dôkladného zváženia možných právnych dôsledkov. F. Spolu s návrhom zákona by mali byť v legislatívnom procese aj vykonávacie predpisy (Vyhláška).			
RÚZSR	21. Zásadná pripomienka k čl. I., novelizačný bod 28 Bod 28 navrhujeme upraviť nasledovne: V § 20 ods. 4 písmeno a) znie: „a) určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení podľa § 20 ods. 1 až 3 nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti, podľa	Z	ČA	pripomienka je čo do svojho účelu akceptovaná

	osobitného predpisu“. Odôvodnenie: Riešenie nezávislosti od prevádzky a vývoja prostredníctvom zaradenia v organizačnej štruktúre, nezaručuje túto nezávislosť. Tá by mala byť pri plánovaní a prijímaní opatrení a tiež plánovaní zdrojov. V súčasnosti je určenie manažéra kybernetickej bezpečnosti upravené vo vyhláške NBÚ 362/2018 Z. z. V zmysle súčasnej úpravy manažér má spĺňať znalostné štandardy, ktoré majú byť určené osobitným predpisom. V zmysle dôvodovej správy k navrhovanému bodu 28 by mal stav ostať zachovaný a na výkon činnosti manažéra sa predpokladá preukázanie odbornej spôsobilosti v súlade s osobitným predpisom vydaným úradom.“ Doplnením úpravy role manažéra priamo do zákona dochádza k duplicite zákonnej úpravy s úpravou v podzákonom predpise. Je predpoklad, že po novelizácii zákona dôjde zo strany NBÚ aj k úprave vyhlášky 362/2018 Z. z.. V prípade vypustenia úpravy role manažéra z uvedenej vyhlášky by sa stratila legislatívna úprava stanovenia požiadaviek na manažéra			
RÚZSR	22. Zásadná pripomienka k čl. I., novelizačný bod 29 Bod 29. navrhujeme upraviť nasledovne: V § 22 odseky 4 a 5 znejú: „(4) Ak poskytovateľ digitálnej služby využíva tretiu stranu na výkon činností, ktoré priamo súvisia s poskytovaním digitálnej služby, je povinný uzatvoriť s treťou strany na výkon týchto činností zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby, keď poskytovateľ digitálnej služby využíva na poskytovanie svojej digitálnej služby tretiu stranu. Povinnosť uzatvoriť zmluvu podľa predchádzajúcej vety neplatí, ak je tretia strana prevádzkovateľom základnej služby poskytovateľom digitálnej služby, alebo podnikom na poskytovanie elektronických komunikačných služieb alebo sietí	Z	N	neodôvodnená pripomienka vo vzťahu k zabezpečeniu bezpečnosti je navrhovaná konštrukcia potrebná vzhľadom na postavenie poskytovateľa digitálnej služby.

	podľa osobitného predpisu x). (5) Ak by sa plnenie zmluvy podľa odseku 4 stalo nemožným, poskytovateľ digitálnej služby o hlásenom kybernetickom bezpečnostnom incidente v nevyhnutnom rozsahu informuje tretiu stranu, pokiaľ úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.“. Odôvodnenie: Zosúladenie povinnosti uzatvoriť zmluvu s treťou stranou v rovnakom režime ako je to u poskytovateľa základnej služby podľa novo navrhovaného znenie §19 ods. 3.			
RÚZSR	23. Zásadná pripomienka k čl. I., novelizačný bod 31 Bod 31. Navrhujeme upraviť nový § 24 ods. 7 nasledovne: „(7) Na hlásenie kybernetických bezpečnostných incidentov alebo na zaistenie kybernetickej bezpečnosti po nahlásení bezpečnostného incidentu je prevádzkovateľ základnej služby určený rozhodnutím úradu, ktorý je orgánom štátnej správy povinný zasielať automatizovaným spôsobom a v rozsahu ustanovenom týmto zákonom určené systémové informácie zo sietí a informačných systémov. Uloženie povinnosti nemôže byť v rozpore s inými právnymi predpismi, najmä s ohľadom na oblasť ochrany súkromia a povinnosti mlčanlivosti vyplývajúcimi z platnej právnej úpravy.“. Následne navrhujeme v novelizačnom bode 38 vypustiť slová „alebo zasielať automatizovaným spôsobom a v rozsahu ustanovenom v štandarde úradu určené systémové informácie zo sietí a informačných systémov podľa § 24 ods. 7.“, alebo uvedené sankčné ustanovenia preformulovať tak aby z neho výslovne vyplývalo, že sankcia za porušenie tejto povinnosti môže byť uložená len subjektu, ktorým je orgán štátnej správy. Odôvodnenie: Navrhujeme aby boli jasne vopred určené subjekty, ktoré budú podliehať takejto povinnosti s odvolaním sa na príslušné sektory v prílohe I a bol	Z	ČA	text je zásadne preformulovaný tak, aby bol jasný a transparentný. Text je dohodou pripomienkujúcich subjektov. Uvedeným nástrojom sa vytvára "bezpečnostný periméter" na hranici Internetu a vlastnej siete a nedochádza k získavaniu obsahu správ. Tajomstvo a súkromie zostáva zachované.

	vylúčený súkromný sektor. Uloženie takejto povinnosti pre podnikateľské subjekty by bolo neprimerane zaťažujúce a reálne nevykonateľné vzhľadom na požiadavku automatizovaného spôsobu. Nie je jasné ani aké systémové informácie by mali byť zasielané a mali by byť jasne vymedzené v ZoKB. Zavádzať uvedené ako povinnosť môže spôsobiť napríklad konflikt s ustanovením § 63 Telekomunikačné tajomstvo Zákona 351/2011 o elektronických komunikáciách, telekomunikačné podniky nemôžu konať nad rámec zákona č. 351/2011 Z.z. najmä pokiaľ ide o spracúvanie a poskytovanie informácií o prevádzke koncových užívateľov. Osobitné problémy by vznikli v súvislosti s fungovaním bankového sektoru. Navrhované znenie odseku je nad rámec riešenia bezpečnostných incidentov. Zaisťovanie kybernetickej bezpečnosti je kompetenciou a povinnosťou prevádzkovateľa základnej služby. Pre bankový sektor je neprípustné, aby Úrad rozhodnutím nariadil prevádzkovateľovi základnej služby napr. zasielanie sieťovej komunikácie, ktorá môže obsahovať zdrojové a cieľové IP adresy, prípadne dáta z informačných systémov. Navyše Úrad by týmto bankový sektor finančne zaťažil. Dopady na bankový sektor môžu byť minimálne v rozsahu: - systémové informácie môžu obsahovať aj údaje chránené osobitnými predpismi (osobné údaje, bankové tajomstvo) a ich očistenie je zložitý a nákladný informatický problém - náklady na HW a vývoj automatizovaného spôsobu zasielania informácií (zahŕňajúci úpravu do štandardu a zabezpečenie ochrany napr. šifrovaním) - náklady na navýšenie výkonu siete a softvérových nástrojov - náklady na zabezpečenie sieťového pripojenia (vzhľadom na veľké množstvo dát pravdepodobne na nejaký prenajatý okruh), - riziko úniku citlivých informácií vzhľadom na skutočnosť, že úroveň zabezpečenia v			
--	--	--	--	--

	bankovom sektore je vyššia ako na strane vládnych organizácií (viď. nedávny únik dát z NCZI).			
RÚZSR	27. Zásadná pripomienka k čl. I., novelizačný bod 36 Bod 36. navrhujeme preformulovať nasledovne: „(4) Právnická osoba zabezpečuje audit kybernetickej bezpečnosti prostredníctvom certifikovaného audítora kybernetickej bezpečnosti alebo certifikovaných audítorov kybernetickej bezpečnosti. Zabezpečovanie auditu kybernetickej bezpečnosti je podnikaním podľa osobitného predpisu31d), ak nejde o audit kybernetickej bezpečnosti u poskytovateľa základnej služby alebo poskytovateľa digitálnej služby vykonávaný vlastným zamestnancom, alebo zamestnancom iného podniku v rámci skupiny podnikov. Ak audit kybernetickej bezpečnosti realizuje audítor kybernetickej bezpečnosti prostredníctvom právnickej osoby, zodpovedá za škodu spôsobenú pri výkone auditu kybernetickej bezpečnosti táto právnická osoba.“ Odôvodnenie: Spresnenie; aby spoločnosť, ktorá si bude vykonávať vlastný audit prostredníctvom svojho zamestnanca, alebo zamestnanca iného podniku – ovládanej alebo ovládajúcej osoby, nemusela ohlasovať výkon auditu kyber. bezpečnosti ako novú podnikateľskú činnosť.	Z	A	
RÚZSR	34. Zásadná pripomienka k čl. I., novelizačný bod 47 Bod. 47 – navrhujeme upraviť § 33 ods. 1 podľa odôvodnenia nižšie Odôvodnenie: Navrhujeme predmetné ustanovenie preformulovať tak, že z neho bude expressis verbis vyplývať, že na konania podľa tohto zákona sa vzťahuje všeobecný právny predpis o správnom konaní (Správny poriadok) s výnimkou taxatívne vymenovaných ustanovení v rozsahu v akom sa nachádzajú v súčasnom znení v existujúcom predpise. Žiadame aj o vyradenie novodoplnených § 24	Z	N	Neodôvodnená pripomienka. Neaplikovanie Správneho poriadku neznamenaá absenciu právneho rozhodnutia. Na každé rozhodnutie sa vzťahujú princípy SP, každé rozhodnutie je preskúmateľné súdom a teda účastník nie je ukrátený a svojich právach. Vyňatie z režimu SP má svoje

	ods 7, § 27a spomedzi ostatných ustanovení, upravujúcich konania podľa zákona, na ktoré sa nemá vzťahovať Správny poriadok, vzhľadom na pripomienky k súvisiacim novelizačným bodom.			opodstatnene v neodkladnosti rozhodnutia, nie v jeho nepreskúmateľnosti.
RÚZSR	15. Pripomienka k čl. I., novelizačný bod 16 K bodu 16 navrhujeme upraviť slovosled nakoľko takto zaniká základná myšlienka	O	A	
RÚZSR	13. Zásadná pripomienka k čl. I., novelizačný bod 14 Nakoľko z aplikačnej praxe bankového sektora vznikla potreba presadenia sektorových špecifik a zároveň možnosť využívať jednotku CSIRT príslušného ústredného orgánu pre sektor bankovníctvo považujeme za nevyhnutné zaradiť aj sektor Bankovníctvo medzi podsektory, ktoré nevyužívajú Národnú jednotku CSIRT ale iné akreditované jednotky CSIRT, aktuálne CSIRT.MIL.SK a CSIRT.SK. V tomto je potrebné zároveň doplniť aj prechodné ustanovenia k predkladanému zákonu, tak ako navrhujeme v pripomienke o doplnení prechodných a záverečných ustanovení §34.	Z	ČA	Vzhľadom na zmenu textu (ponechaná možnosť vlastného akreditovaného CSIRTu) ako aj vo vzťahu v MIL. CSIRT nie je možné Vašej požiadavke vyhovieť.
RÚZSR	29. Pripomienka k čl. I., novelizačný bod 40 Navrhované znenie § 31 ods. 6 až 9 navrhujeme upraviť. navrhujeme znížiť spodnú hranicu na od 0 eur v prípadoch kedy nedošlo k závažnému správne deliktu a nevznikla žiadna škoda a došlo k promptnej náprave stavu. Navrhujeme precizovať rozdelenie správnych deliktov a výšku pokút za nich ukladaných zhodne ako uvádzame v pripomienke k Bodu 39. Nakoľko najmä u menších subjektov môže byť pokuta v hornom rozsahu likvidačná, všeobecne odporúčame postupovať ako pri škodách v správnom poriadku.	O	N	Rozpätie sumy pokuty nemá súvislosť s kvalitou rozhodnutia. Je vecou správneho orgánu v závislosti od miery porušenia zákona akou výškou sankcie vzhľadom na všetky okolnosti bude pokutovať.

RÚZSR	30. Pripomienka k čl. I., novelizačný bod 42 Navrhované znenie § 31a ods. 3 navrhujeme vypustiť. Odôvodnenie: Ide o legislatívno-technickú pripomienku vzhľadom na znenie § 33 ods. 1, ako aj našu pripomienku k Bodu 47.	O	A	
RÚZSR	32. Pripomienka k čl. I., novelizačný bod 45 Navrhované znenie § 32 ods. 1 písm. g) a h) navrhujeme vypustiť. Odôvodnenie: Ad: § 32 ods. 1 písm. g): Vzhľadom na naše pripomienky k Bodu 10., a Bodu 12. navrhujeme vypustiť, okrem iného, z dôvodu, že nie je žiadúce aby Úrad bol na jednej strane vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti a orgánom posudzovania zhody podľa osobitného predpisu a zároveň na druhej strane sám určoval podmienky v rámci systému certifikácie kybernetickej bezpečnosti, vydávaním bezpečnostných štandardov, certifikačných schém a postupov. O to viac nie v podzákonnom (vykonávacom) predpise. Ad: § 32 ods. 1 písm. h): Vzhľadom na našu pripomienku ku Bodu 33. navrhujeme vypustiť z dôvodu, že žiadame aby pravidlá blokovania boli súčasťou právneho predpisu v dikcii ustanovenia § 27a a nie vo vykonávacom predpise.	O	N	
RÚZSR	35. Zásadná pripomienka k čl. I., novelizačný bod 49 Navrhujeme doplniť prechodné a záverečné ustanovenia o ďalší odsek v nasledovnom znení „(12) Ustanovením §9 ods. 2 nie sú dotknuté zmluvy o využívaní akreditovanej jednotky CSIRT zriadenej a prevádzkovej iným ústredným orgánom, uzatvorené pred DD.MM.RRRR (účinnosťou zákona). Prevádzkovatelia základnej služby, ktorí využívajú akreditovanú jednotku CSIRT podľa predchádzajúcej vety, môžu takúto akreditovanú jednotku CSIRT využívať aj po DD.MM.RRRR (nadobudnutím účinnosti tohto zákona), pričom sa na nich nevzťahuje povinnosť využívať	Z	A	

	Národnú jednotku CSIRT.“			
RÚZSR	26. Pripomienka k čl. I., novelizačný bod 35 Navrhujeme nahradiť slová „orgán posudzovania zhody podľa osobitného predpisu, 31) ktorý je akreditovaný ako orgán príslušný na posudzovanie zhody v oblasti kybernetickej bezpečnosti“ slovami „certifikovaný audítor kybernetickej bezpečnosti, 31a) ktorým je fyzická osoba a spoločník, alebo štatutárny orgán alebo zamestnanec právnickej osoby. Certifikáciu audítora kybernetickej bezpečnosti vykonáva osoba akreditovaná podľa osobitného predpisu 31b) ako orgán certifikujúci osoby 31c) (Ďalej len „orgán certifikujúci osoby“) v oblasti kybernetickej bezpečnosti“.	O	A	
RÚZSR	17. Pripomienka k čl. I., novelizačný bod 18 Navrhujeme ponechať pôvodné znenie alebo nahradiť slová „ústredného orgánu, ktorý má plniť úlohy jednotky CSIRT.“ slovami „orgánu verejnej moci, ktorý má plniť úlohy jednotky CSIRT.“.	O	N	
RÚZSR	28. Pripomienka k čl. I., novelizačný bod 39 Navrhujeme precizovať rozdelenie správnych deliktov s ohľadom na ich závažnosť a subjekt, vrátane bližšej kategorizácie rozsahu výšky pokút. Navrhovaný rozsah medzi výškou pokuty 300 Eur až 100 000 Eur je pre logiku správneho uváženia príliš široký. Takéto široké rozpätie vytvára príliš veľký priestor pre nesprávnosť rozhodnutia o uložení pokuty. Príliš veľký, zákonom ustanovený priestor pri správnom trestaní, môže znamenať neprimeranosť povahy skutku, resp. môže mať v individuálnych prípadoch aj likvidačný charakter pre dotknutý subjekt. Odporúčame predmetné ustanovenie upraviť analogicky s inými právnymi predpismi z oblasti správneho	O	N	Rozpätie sumy pokuty nemá súvislosť s kvalitou rozhodnutia. Je vecou správneho orgánu v závislosti od miery porušenia zákona akou výškou sankcie vzhľadom na všetky okolnosti bude pokutovať.

	trestania.			
RÚZSR	6. Zásadná pripomienka k čl. I., novelizačný bod 10 Navrhujeme upraviť § 5 sa odsek 1 písm. y) nasledovne: „y) v rámci riešenia opatrení o blokovani podľa osobitných predpisov10aa) zabezpečuje vykonanie rozhodnutia o blokovani škodlivého obsahu alebo škodlivej aktivity,“ Odôvodnenie: Rozhodnutie o blokovani môže byť len na základe príkazu súdu podľa osobitného predpisu, čo poskytuje dostatočnú právnu istotu, že ide o blokovanie relevantné a odôvodnené.	Z	ČA	text preformulovaný, blokovanie ako inštitút bolo upravené tak, aby reflektovalo pripomienky subjektov a aby bol vytvorený transparentný rámec.
RÚZSR	10. Zásadná pripomienka k čl. I., novelizačný bod 11 Navrhujeme úpravu a doplnenie znenia § 5 ods. 4 nasledovne: „(4) Úrad je oprávnený požadovať od ústredných orgánov, prevádzkovateľov základnej služby, orgánov verejnej moci a právnických osôb poskytnutie súčinnosti, alebo informácií, ktoré sú potrebné na plnenie úloh podľa tohto zákona. Orgány verejnej moci, prevádzkovatelia základnej služby a právnické osoby sú povinné úradu poskytnúť požadovanú súčinnosť, alebo informácie, ktoré sú potrebné na plnenie úloh podľa tohto zákona pokiaľ im v tom nebránia platné právne predpisy.“ Odôvodnenie: Navrhujeme doplniť na konci: „pokiaľ im v tom nebránia platné právne predpisy“. V prípade bánk a informácií ktoré sú bankovým tajomstvom by takéto znenie nestačilo, keďže by bolo potrebné prelomiť aj zákon o bankách a bankové tajomstvo, keďže tu sa taxatívne vymedzuje akým orgánom je banka oprávnená poskytnúť súčinnosť. NBU má síce v zákone o bankách oprávnenie na informácie, no iba vo vzťahu k bezpečnostným previerkam a k hláseniu incidentov.	Z	ČA	text preformulovaný aj s ohľadom na iné vznesené pripomienky, obmedzenia sú uvádzané v poznámkach pod čiarou podľa požiadaviek subjektov.

RÚZSR	31. Pripomienka k čl. I., novelizačný bod 44 Navrhujeme určiť periodicitu záväzne z dôvodu plánovania výdavkov na audity v nadväznosti k štandardizácii informačných systémov a harmonizovať v súlade so zákonom 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.	O	N	Uvedené je predmetom vyhlášky o audite
RÚZSR	33. Zásadná pripomienka k čl. I., novelizačný bod 46 Navrhujeme zachovať pôvodné znenie a prerokovať ho so všetkými rezortmi. Odôvodnenie: Uvedené navrhujeme prerokovať s orgánmi príslušnými na tvorbu právnych predpisov, nakoľko máme za to, že úrad nie je oprávnený v rámci legislatívneho procesu udeľovať súhlas s vydaním, resp. v akejkoľvek fáze legislatívneho procesu schvaľovať vykonávací právny predpis iného ústredného orgánu. Toto považujeme za rozporné s pravidlami tvorby právnych predpisov, ide o prekračovanie právomocí úradu a navrhujeme novelizačný bod vypustiť	Z	A	
RÚZSR	7. Zásadná pripomienka k čl. I., novelizačný bod 10, v časti §5 odsek 1, písm. z) a ab) Nie je žiaduce aby Úrad bol na jednej strane vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti a orgánom posudzovania zhody podľa osobitného predpisu a zároveň na druhej strane sám určoval podmienky v rámci systému certifikácie kybernetickej bezpečnosti, vydávaním bezpečnostných štandardov, certifikačných schém a postupov. Vychádzajúc z OZNÁMENIA KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNŮV, Bezpečné zavádzanie 5G v EÚ – Vykonávanie súboru nástrojov, skupina pre spoluprácu v oblasti kybernetickej	Z	N	Úrad plní úlohy ako akreditovaný orgán, spĺňa všetky predpoklady kladené jednak legislatívou EÚ ako aj národnou. Vaša pripomienka je vo vzťahu k naplneniu predpokladov zo strany úradu neodôvodnená.

	bezpečnosti predstavila súbor strategických a technických opatrení, ako aj príslušné podporné opatrenia na posilnenie ich účinnosti, ktoré sa môžu zaviesť s cieľom zmierniť zistené riziká. Strategické opatrenia sa vzťahujú na opatrenia týkajúce sa rozšírených regulačných právomocí orgánov. Z uvedeného vyplýva, že hoci majú byť posilnené regulačné právomoci, nemôže byť všetka právomoc sústredená u jedného konkrétneho orgánu.			
RÚZSR	24. Zásadná pripomienka k čl. I., novelizačný bod 32 Novelizačný bod 32 navrhujeme vypustiť. Odôvodnenie: Kompetencia Úradu zakázať, alebo obmedziť prevádzkovateľovi základnej služby, v individuálnom konaní bez bližšieho určenia (stanovenia podmienok) je v rozpore s Čl. 46 Ústavy Slovenskej republiky a Čl. 6 Dohovoru o ochrane ľudských práv a základných slobôd („Dohovor“). O to viac, že v navrhovanom Bode 47. (§ 33) sa stanovuje, že na tento typ konania sa nevzťahuje zákon č. 71/1967 Zb. o správnom konaní („Správny poriadok“). O to viac, že samotný zákon, resp. jeho navrhovaná novela, neobsahuje osobitné procesné ustanovenia v tejto súvislosti. Ide o veľmi široké oprávnenie úradu zakázať alebo obmedziť ktorémukoľvek prevádzkovateľovi základnej služby používať konkrétny produkt, proces alebo službu pod vágne koncipovanou podmienkou „ak je to potrebné na zaistenie kybernetickej bezpečnosti, alebo z dôvodov bezpečnostného záujmu Slovenskej republiky“, pod čo je možné subsumovať v zásade čokoľvek. Táto skutočnosť v aplikačnej praxi spôsobí protiústavný stav a to najmä v dôsledku toho, že sa neprecizuje presný procesný postup akým bude Úrad rozhodovať a presné hmotnoprávne podmienky ktoré bude Úrad v tomto rozhodovacom procese skúmať. V takomto prípade je porušená precedenčná zásada – teda	Z	N	Text je zásadne prepracovaný tak, aby bol jasný a transparentný. Je implementáciu EU Toolbox v najširšom zmysle slova a predstavuje nevyhnutný bezpečnostný nástroj. Uvedený nástroj sa realizuje na základe vyhodnotenia rizík, po odporúčaní BRSR a rozhodnutie je zverejňované v Zbierke zákonov.

	predvídateľnosti procesných úkonov správneho orgánu, ktorou sú správne orgány viazané. Obsahom základného práva na súdnu ochranu podľa čl. 46 ods. 1 ústavy je aj právo účastníka konania, ako aj iného zainteresovaného subjektu na rozhodnutie, ktorého dôvody sú zjavné a zreteľné, pretože práve odôvodnenie rozhodnutia je zárukou toho, že výkon spravodlivosti nebude arbitrárny (I. ÚS 117/07). Keďže správne orgány vystupujú v roli toho, kto rozhoduje právne záväzným spôsobom o právach, povinnostiach, alebo právom chránených záujmoch, je veľmi dôležité, aby bolo jednoznačne a jasne stanovený postup a pravidlá, ako má správny orgán pri svojom rozhodovaní postupovať. Ak by takéto pravidlá v zákone stanovené neboli, správny orgán, ako zástupca štátu, by mohol pri svojom rozhodovaní postupovať svojvoľne, napr. takým spôsobom, ktorým by porušoval práva dotknutých osôb, alebo im ich neumožnil dostatočným spôsobom hájiť (https://viaiuris.sk/wp-content/uploads/2017/08/publikacia-2011-ako-maju-urady-postupovat.pdf). Takto navrhnutý rozhodovací proces môže výrazným spôsobom zasiahnuť do slobodného výkonu vlastníckych práv (Čl. 20 Ústavy Slovenskej republiky, Čl. 1 Dodatkového protokolu č. 1 Dohovoru) a slobody podnikania (Čl. 35 Ústavy Slovenskej republiky). Súčasne nespĺňa ani obsahové požiadavky Rezolúcie Výboru ministrov Rady Európy (77)31 z 28. 9. 1977 o ochrane jednotlivca v súvislosti s rozhodnutiami správnych, resp. Odporúčania Výboru ministrov Rady Európy Rec (2007)7 z 20. 6. 2007 o dobrej verejnej správe. Pre účely vylúčenia služieb alebo produktov, ktorých používanie nie je bezpečné, je potrebné využiť reguláciu umiestňovanie tovarov a služieb na tuzemský alebo EÚ trh, prípadne akreditačné schémy a pod. Navyše uvedené ustanovenie je pravdepodobne v rozpore s platným zákonom o			
--	--	--	--	--

	verejnom obstarávaní č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov, tzv. „nediskriminačný prístup“. Uvedené ustanovenie nebolo predmetom predbežnej informácie k novele zákona a teda ani predmetom konzultácií so zainteresovanými stranami, na ktoré sa zavedená povinnosť vzťahuje. Považujeme za nevyhnutné riešiť v rámci širšej odbornej a celospoločenskej diskusie, vypracovať k nim podrobnú analýzu vplyvov, ich právne posúdenie a navrhujeme ich preto z predkladaného návrhu zákona vypustiť. Pre účely vylúčenia služieb alebo produktov, ktorých používanie nie je bezpečné, je potrebné využiť reguláciu umiestňovanie tovarov a služieb na tuzemský alebo EÚ trh, prípadne akreditačné schémy a pod. Oprávnenie úradu rozhodovať individuálnom konaní o zákaze používania konkrétneho produktu, alebo technológie bez bližšie určenia podmienok takéhoto rozhodovania a ešte k tomu mimo správneho konania je v rozpore s ústavou a dohovorom. Takáto konanie zasahuje do slobodného výkonu vlastníckych práv. Telekomunikačné podniky nemôžu používať iné ako bezpečné sieťové prvky, ktoré spĺňajú technické normy a požiadavky z hľadiska bezpečnosti a integrity siete, takáto povinnosť im vyplýva z vlastného regulačného rámca a technických požiadaviek, ktoré sú na sieť a jej prvky kladené (§ 64 ods. 8 zákona č. 351/2011 Z. z., požiadavky plynúce zo všeobecného povolenia pre telekomunikačný sektor). Prevádzkovateľ by nemal znášať náklady spojené s výmenou infraštruktúry, ktorá je vo verejnom záujme a keď situáciu nezavinil. Zároveň každé rozhodnutie, ktorým sa zasahuje do užívacieho práva v rámci vlastníckeho práva musí byť preskúmateľné súdom, iná právna úprava by odporovala čl. 46 ods. 2 Ústavy SR. Dotknutý prevádzkovateľ by mal mať preto prístup k riadnym aj			
--	---	--	--	--

	mimoriadnym opravným prostriedkom V prípade bankového sektoru ide o zásadný zásah do kompetencií NBS. O Zákaze činnosti v sektore bankovníctvo by mala rozhodovať jedine NBS v odôvodnených prípadoch, nie je možné zo strany NBÚ zakázať napr. platobný styk a pod. Navyše dopady na bankový sektor môžu byť enormné. Ako príklad uvádzame situáciu, ak napr. úrad rozhodne o zákaze používať sieťové komunikačné zariadenia alebo diskové úložiská od konkrétneho výrobcu. Nákup, zaškolenie a výmena takejto technológie môže trvať aj viac ako 12 mesiacov a mať dopad radovo v miliónoch eur. Navyše v prípade takéhoto záväzného rozhodnutia musí úrad vymedziť mantinely rozhodnutia (časový rámec, kompenzácia prostredníctvom iných technických opatrení, ai.). Zároveň si dovoľujeme upozorniť na skutočnosť, že nakoľko má ísť o obmedzenie ktoré sa vzťahuje len na prevádzkovateľov základnej služby a v bankovom sektore pôsobia aj banky, ktoré nie sú prevádzkovateľom základnej služby dôjde k narušeniu rovnováhy trhu a hospodárskej súťaže			
RÚZSR	37. Zásadná pripomienka k čl. I., novelizačný bod 51 a vloženie nového novelizačného bodu v čl. III Novelizačný bod 51. navrhujeme upraviť nasledovne: V prílohe č. 1 v sektore „4. Elektronické komunikácie“ v podsektore „Siete a služby pevných a mobilných elektronických komunikácií“ v stĺpci „Prevádzkovateľ služieb“ sa vkladá nový riadok, ktorý znie: „služby vysokorýchlostného prenosu dát a hlasu v mobilnej elektronickej komunikačnej sieti piatej generácie (5G)“. Zároveň doplniť v článku III návrhu do § 64 ods. 1 zákona č. 351/2011 Z.z. „ Ak podnik plní súčasne bezpečnostné opatrenia podľa osobitného predpisu, tieto opatrenia plní prednostne pred inými opatreniami podľa tohto	Z	ČA	riesi §27a

	zákona. Štátny dozor nad dodržiavaním bezpečnostných opatrení podľa osobitného predpisu vykonáva a sankciu za ich porušenie ukladá Národný bezpečnostný úrad podľa osobitného predpisu. Odôvodnenie: Ak berieme do úvahy súčasný vývoj v oblasti regulácie bezpečnosti EK sietí a služieb v Európskej únii, tak momentálne jediným podnetom na špecifickú reguláciu v oblasti elektronických komunikácií nad rámec všeobecných bezpečnostných opatrení pre elektronické komunikačné siete a služby (ktoré by ale mali vychádzať a mali by byť súčasťou transpozície EECC – teda súčasťou novej legislatívy upravujúcej elektronické komunikácie) je tzv. 5G security toolbox. Tento dokument vychádzajúc z procesu analýzy rizík na úrovni EÚ pripúšťa, či skôr vyžaduje osobitnú bezpečnostnú reguláciu avšak výlučne pre mobilné siete piatej generácie (5G). Dôvodom je predovšetkým fakt, že sa očakáva, že práve mnohé základné služby z iných sektorov (doprava, priemysel, verejná správa a pod.) budú v budúcnosti využívať 5G siete pre masívny rozvoj dôležitých informačných systémov na riadenie a monitoring základných služieb. Pokiaľ teda stratégia implementácie tzv. 5G security toolbox-u v Slovenskej republike počíta so špecifickým technickým bezpečnostným štandardom pre mobilné 5G siete takým spôsobom, že kompetencie v oblasti regulácie a štátneho dohľadu na kybernetickú bezpečnosťou 5G sietí majú byť prenesené orgánom definovaným v zákone o KB, potom je akceptovateľné zaradenie avšak výlučne 5G sietí, resp. vysokorýchlostného prenosu dát prostredníctvom 5G siete medzi základné služby.			
RÚZSR	25. Zásadná pripomienka k čl. I., novelizačný bod 33 Požadujeme vypustiť bod 33 v čl. I z návrhu. Odôvodnenie: Inštitút	Z	N	Text je prepracovaný. NBÚ využíva nástroj blokovania ako jeden z možností

blokovania v takto navrhovanom znení považujeme vzhľadom na jeho závažnosť a významný zásah do práv a slobôd garantovaných Ústavou SR za nedostatočne koncipovaný. Absentuje tu definícia, čo sa blokovaním rozumie, taktiež vzhľadom na významný zásah do práv a slobôd tu absentuje ingerencia napr. súdu či prokuratúry alebo možnosti kontroly či garantovania spravodlivého procesu. Takýmto spôsobom môže neodôvodnene dochádzať k zásahom do práv bez toho, aby mal dotknutý subjekt možnosť obrany či posúdenia nezávislým orgánom. Blokovanie čísiel a služieb upravuje zákon č. 351/2011 Z.z o elektronických komunikáciách (ďalej len „ZEK“), ktorý v § 41 ods. 4 ustanovuje, že blokovať sa môže iba na základe žiadosti orgánu činného v trestnom konaní. Toto ustanovenie tak, ako aj celý ZEK plne implementuje nariadenie č. 2015/2120 o sieťovej neutralite. Hlavnou ideou tohto nariadenie je: Koncoví užívatelia majú právo na prístup k informáciám a obsahu a právo šíriť informácie a obsah, využívať a poskytovať aplikácie a služby a využívať koncové zariadenie podľa vlastného výberu, bez ohľadu na umiestnenie koncového užívateľa alebo poskytovateľa, alebo na umiestnenie, pôvod či určenie informácií, obsahu, aplikácie alebo služby prostredníctvom ich služby prístupu k internetu. Uvedené znamená, že každý má právo na prístup k elektronickým komunikačným službám, pokiaľ orgán činný v trestnom konaní nepožiadá o zablokovanie. Navrhované ustanovenie je príliš všeobecné a je v rozpore s ZEK ako aj s nariadením a legislatívou EÚ, , keďže v prípade jeho prijatia nie sú garantované uvedené práva užívateľov. Zároveň zakladá neistotu vo využívaní čísel a služieb z dôvodu príliš všeobecného návrhu ustanovenia bez garancie ochrany základných práv. Problematika blokovania je riešená napr. aj v zákone č. 73/1998 Z. z. o štátnej službe		pri riešení KBI, ide o nástroj ultima ratio, s ktorým počíta aj legislatíva EÚ (nariadenie ešte nie je schválené). Uvedený nástroj riešenia KBI vychádza z podrobného štandardu (rovnaký v celej EÚ), ktorý bude zverejnený vo forme vykonávacieho predpisu. NBÚ zákonnou konštrukciou dáva možnosť, aby odbornú spôsobilosť, ktorou úrad disponuje, mohli využiť aj iné subjekty. Ustanovenie je pre lepšiu orientáciu rozdelené do 2 paragrafov.
---	--	---

	príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení neskorších predpisov SIS, kde blokovanie je realizované až po doručení súdneho príkazu, čiže existuje „právna istota“ v tom, že ide o blokovanie, ktoré je relevantné a odôvodnené. Ďalšia situácia je riešená v zákone č. 30/2019 Z. z. o hazardných hrách a o zmene a doplnení niektorých zákonov v platnom znení hazardu, kde je blokovanie vykonávané na základe príkazu súdu. Odporúčame zjednotiť legislatívu, a to v tom smere, že blokovanie je možné len na základe súhlasu/príkazu súdu, čo poskytuje dostatočnú právnu istotu, že ide o blokovanie relevantné a odôvodnené. Taktiež je nevyhnutné zdefinovať rozsah blokovaní (vyšpecifikovať čo môže byť predmetom blokovaní), ktorý bude uplatňovaný rovnako pre všetkých operátorov/poskytovateľov služieb. Blokovanie musí byť transparente odkomunikované smerom na užívateľa úradom/orgánom, ktorý o blokovanie žiada, napr. presmerovaním na stránky úradu/orgánu, kde sa užívateľ dozvie o dôvode blokovaní. Musia byť zohľadnené aktuálne technické možnosti výkonu blokovaní. Tzn. úrad nemôže žiadať operátorov o blokovanie obsahu služieb, ktorých nie je prevádzkovateľom (napr. obsah na Facebook, správy zasielané cez WA, Viber,...). Ak úrad bude požadovať blokovanie, ktoré vyžaduje dodatočnú technickú implementáciu na strane poskytovateľa služby musí sa podieľať na nákladoch s tým spojených. Podniky nemôžu konať v oblastiach, ktoré sú regulované zákonom č. 351 /2011 Z.z. nad jeho rámec. Ďalej upozorňujeme na to, že pri používaní neurčitých právnych pojmov je zákonodarca so zreteľom na princíp právnej istoty vyplývajúci z čl. 1 ods. 1 prvej vety ústavy obmedzený. Z hľadiska			
--	--	--	--	--

	skutkových predpokladov a obsahu príslušnej právnej úpravy musí zákonodarca koncipovať a formulovať zákon a v ňom obsiahnuté právne normy tak, aby zodpovedali požiadavkám jasnosti, prehľadnosti právnej vykonateľnosti a uplatniteľnosti zo strany orgánov verejnej moci aplikujúcich právnu normu, t.j. najmä súdov, ale i iných orgánov verejnej moci, ktoré vyplývajú z princípu právneho štátu. Ústavný súd v súvislosti s uvedeným poukazuje aj na svoj právny názor vyslovený už v konaní sp. zn. PL. ÚS 19/98, podľa ktorého "Požiadavkou právnej istoty je, aby zákony v právnom štáte boli pochopené dostatočne a aby umožňovali ich adresátom urobiť si aspoň predstavu o svojej právnej situácii. Nejasnosť, viacvýznamovosť a vágnosť pojmu... vytvára stav právnej neistoty, čím sa dostáva do rozporu s čl. 1 Ústavy Slovenskej republiky." (PL. ÚS 29/05).			
RÚZSR	18. Zásadná pripomienka k čl. I., novelizačný bod 23 RÚZ navrhuje slovo „šiestich“ nahradiť slovom „dvadsiatich štyroch“. Odôvodnenie: Uvedené navrhujeme upraviť vo vzťahu k počtu základných služieb, ktoré prevádzkuje rezort ministerstva vnútra a tieto budú pripájané pod rezortnú jednotku CSIRT postupne v priebehu celých 24 mesiacov od navrhovanej účinnosti zákona a zároveň týmto dôjde k harmonizácii lehôt určených v zákone 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. Vzhľadom na neustále pribúdajúce hrozby v kybernetickom priestore je všeobecný konsenzus uskutočniť túto činnosť v čo najskoršom možnom termíne je však potrebné zohľadniť špecifické postavenie rezortu ministerstva vnútra vzhľadom na počet prevádzkovaných základných služieb	Z	N	Neodôvodnená pripomienka, vo vzťahu k zabezpečovaniu bezpečnosti je lehota dvoch rokov neúmerne dlhá. Nami navrhovaná doba predstavuje dostatočný priestor na prijatie bezpečnostných opatrení.

RÚZSR	19. Zásadná pripomienka k čl. I., novelizačný bod 24 v časti §19 odsek 2 RÚZ navrhuje uvedené ustanovenie formulovať nasledovne: Navrhujeme úpravu a doplnenie znenia §19 ods. 2 nasledovne: „(2) Prevádzkovateľ základnej služby je povinný pri výkone činností, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby výkonu týchto činností. Pred uzatvorením zmluvy sa analyzujú riziká podľa § 20 ods. 3 písm. b) zákona. V prípade, ak v súvislosti s konkrétnou činnosťou súvisiacou s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby, vykonávanú prostredníctvom tretej strany dôjde na základe takejto analýzy k záveru, že príslušné riziko s prihliadnutím na § 20 ods. 3 písm. b) zákona je nízke, uzatvorenie zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností sa vo vzťahu k výkonu príslušnej činnosti nevyžaduje.“ Odôvodnenie: Uvedeným doplnením sa kladie dôraz na výsledok analýzy rizík, ktorá je zásadným predpokladom na posúdenie, či je potrebné uzatvorenie zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností s daným dodávateľom.	Z	A	
RÚZSR	11. Zásadná pripomienka k čl. I., novelizačný bod 12, v časti §5a odsek 2 RÚZ navrhuje uvedené ustanovenie vypustiť. Odôvodnenie: Uvedené znenie nie je v súlade s bodom 6 Prílohy k NARIADENIU EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2019/881 zo 17.	Z	N	predpoklad uvedený v pripomienke je nepochybne zabezpečený navrhovaným ustanovením, text predstavuje zhodu odbornej verejnosti aj príslušných štátnych orgánov, v pôsobnosti ktorých

apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) („Nariadenie“) v zmysle ktorého: „Ak orgán posudzovania zhody vlastní alebo prevádzkuje verejný subjekt alebo verejná inštitúcia, musí sa zabezpečiť a zdokumentovať nezávislosť a absencia akéhokoľvek konfliktu záujmov medzi vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti a orgánom posudzovania zhody.“ Vychádzajúc z OZNÁMENIA KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV, Bezpečné zavádzanie 5G v EÚ – Vykonávanie súboru nástrojov, skupina pre spoluprácu v oblasti kybernetickej bezpečnosti predstavila súbor strategických a technických opatrení, ako aj príslušné podporné opatrenia na posilnenie ich účinnosti, ktoré sa môžu zaviesť s cieľom zmierniť zistené riziká. Strategické opatrenia sa vzťahujú na opatrenia týkajúce sa rozšírených regulačných právomocí orgánov. Z uvedeného vyplýva, že hoci majú byť posilnené regulačné právomoci, nemôže byť všetka právomoc sústredená u jedného konkrétného orgánu. V danom prípade nie je zabezpečená nezávislosť a absencia akéhokoľvek konfliktu záujmov medzi Úradom pri zabezpečovaní certifikácie kybernetickej bezpečnosti a Úradom ako orgánom posudzovania zhody. Alternatívne navrhujeme za orgán posudzovania zhody ustanoviť subjekt, patriaci do obchodného alebo profesijného združenia, ktoré zastupuje podniky, ktoré sa podieľajú na navrhovaní, produkcii, poskytovaní, inštalácii, používaní alebo údržbe produktov IKT, služieb IKT alebo procesov IKT, ktoré tento subjekt posudzuje, za predpokladu			je posúdenie uvedenej problematiky z pohľadu splňania predpokladov na výkon takejto činnosti.
--	--	--	--

	dodržania jeho nezávislosti a absencie konfliktu záujmov v zmysle bodu 3 Prílohy cit. Nariadenia.			
RÚZSR	4. Zásadná pripomienka k čl. I., novelizačný bod 7 RÚZ navrhuje uvedený bod vypustiť Odôvodnenie: Ustanovenie § 3 zákona sa dopĺňa novými definíciami, z ktorých definície pod písm. q) až t) sú definície uvedené a prebraté z nariadenia R a EP (EÚ) č. 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/ 2013 (ďalej len „akt o kybernetickej bezpečnosti“). Keďže vyššie spomenuté nariadenie je priamo aplikovateľné, bez nutnosti prijatia vnútroštátnej transpozičnej normy, nevyžaduje transpozíciu do vnútroštátnej právnej normy, dokonca ju vôbec nepripúšťa. Vzhľadom na priamu aplikovateľnosť nariadenia a zákaz bránenia tejto priamej aplikovateľnosti preberaním znenia nariadenia do vnútroštátnych predpisov navrhujeme definície v bodoch q) až t) vypustiť a nahradiť ich odkazmi na vyššie citovaný akt o kybernetickej bezpečnosti (čl. 2 body 9 – 14 aktu o kybernetickej bezpečnosti).	Z	A	
RÚZSR	36. Zásadná pripomienka k čl. I., novelizačný bod 50 RÚZ navrhuje vypustiť bod 50 v čl. I z návrhu, ktorým sa v prílohe I pre Sektor Digitálna infraštruktúra“ rozširujú prevádzkovatelia základnej služby Odôvodnenie: Ide o rozšírenie na oblasti služieb, ktoré nie sú upravené smernicou NIS a tieto sa nenachádzajú v prílohe II Smernice NIS. Je nie jasné, z akej terminológie sa vychádza pri vymedzení nových služieb tak pre sektor Elektronické komunikácie ako aj sektor Digitálna infraštruktúra a aké je ich obsahové a pojmové určenie. Vychádzajúc aj z pojmológie, ktorú	Z	N	nejde o rozšírenie ale o jasnejšie formulovanie

	zavádza smernica 2018/1972 (EECC) by systematicky služby prístupu do internetu mali spadať pod elektronické komunikačné služby. Prevádzkovateľ obchodu na internete s možnosťou vyhľadávania, objednávaní a nákupu tovarov a služieb sa javí ako iná obdoba on-line trhoviska, ktoré však spadá pod digitálnu službu, rovnako aj služby DNS hostingu a webhostingu, pričom členské štáty nemajú ukladať poskytovateľom digitálnych služieb žiadne ďalšie bezpečnostné ani oznamovacie požiadavky nad rámec Smernice NIS (čl. 16 Smernice). Rovnako nie sú bližšie určené ani identifikačné kritéria pre zaradenie			
RÚZSR	12. Zásadná pripomienka k čl. I., novelizačný bod 14 S uvedenou zmenou zásadne nesúhlasíme, nakoľko nebola vopred prerokovaná s dotknutými ústrednými orgánmi. Navrhujeme preto buď ponechať pôvodné znenie § 9 ods. 2 alebo nové v znení: žiadame slová v § 9 ods. 2 „zriaďuje a prevádzkuje akreditovanú jednotku CSIRT alebo na tento účel využíva akreditovanú jednotku CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, ak sa tak dohodnú. Využívanie akreditovanej jednotky CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, sa vykonáva na základe zmluvy“ nahradiť slovami „Ústredný orgán na účely plnenia úloh podľa odseku 1 písm. a) v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa prílohy č. 1 zriaďuje a prevádzkuje akreditovanú jednotku CSIRT alebo na tento účel využíva akreditovanú jednotku CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, ak sa tak dohodnú. Využívanie akreditovanej jednotky CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, sa vykonáva na základe zmluvy. Ústredný orgán, ktorý nemá zriadenú akreditovanú jednotku CSIRT ani na tento účel nevyužíva akreditovanú jednotku CSIRT iného	Z	A	Ponechaná možnosť zriadiť a prevádzkovať vlastnú akreditovanú jednotku CSIRT alebo využívať Národnú jednotku CSIRT

	ústredného orgánu, využíva Národnú jednotku CSIRT.“ Odôvodnenie: Niektoré vybrané rezorty vzhľadom na plnenie špecifických špeciálnych úloh plánujú zriadiť a prevádzkovať v budúcnosti vlastné akreditované jednotky CSIRT. Rovnako tak rezort Ministerstva vnútra SR pripravuje vybudovanie rezortnej jednotky CSIRT, ktorá bude pokrývať všetky informačné systémy prevádzkované rezortom. Novo navrhované znenie § 9 ods. 2 by znemožnilo zriaďovanie a prevádzku iných jednotiek, s čím zásadne nesúhlasíme			
RÚZSR	5. Zásadná pripomienka k čl. I., novelizačný bod 8 V § 4 písm. b) žiadame slová „Ministerstvo vnútra Slovenskej republiky“ nahradiť slovami „Ministerstvo vnútra Slovenskej republiky okrem zložiek kriminálneho spravodajstva.“ Odôvodnenie: Všetky zložky plniace úlohy v oblasti spravodajských činností a to Slovenská informačná služba, Vojenské spravodajstvo a Kriminálne spravodajstvo by mali mať rovnocenné postavenie vo vzťahu k zákonom ako je napr. zákon o kybernetickej bezpečnosti, zákon o ochrane utajovaných skutočností a pod	Z	N	MVSR vznieslo pripomienku, ktorou sa MVSR vypúšťa z regulácie ako ústredný orgán. Úrad pripomienke vyhovel a teda nie je možné Vašu pripomienku akceptovať.
RÚZSR	2. Zásadná pripomienka k čl. I., novelizačný bod 1 V návrhu zákona § 2 ods. 2 písm. d) navrhujeme doplniť osobitnú časť dôvodovej správy k predmetnému bodu o zreteľné a jednoznačné vysvetlenie úmyslu predkladateľa vrátane sledovaného cieľa navrhovanej zmeny pôvodnej textácie, ktoré eliminuje možnosť nesprávnych interpretácií negatívneho vymedzenia pôsobnosti zákona. Odôvodnenie: Navrhované znenie dotknutého ustanovenia podľa nášho názoru umožňuje viaceré interpretácie, pričom nie je jasné aký cieľ predkladateľ touto zmenou sledoval. Osobitná časť dôvodovej správy neposkytuje potrebné zdôvodnenie	Z	A	V praxi bolo prijaté usmernenie úradu vo veci výkladu, s ktorým sa adresáti stotožnili. Navrhovná zmena predstavuje legislatívno-technickú úpravu vzhľadom na prax.

	navrhovaných zmien. Samotné precizovanie výnimky z pôsobnosti zákona pre sektor bankovníctva, financií, finančných trhov, platobných systémov a zúčtovania cenných papierov ako vysvetlenie pomerne zásadnej úpravy negatívneho vymedzenia pôsobnosti zákona ako dôvod nepostačuje, pokiaľ nie je zrejmý účel navrhovanej zmeny. Nakoľko jednou z možných interpretácií nového znenia je aj úplné vyňatie bankového sektora spod pôsobnosti zákona o kybernetickej bezpečnosti, v záujme zamedzenia nesprávneho výkladu je potrebné uviesť, čo presne bolo úmyslom predkladateľa			
RÚZSR	8. Pripomienka k čl. I., novelizačný bod 10 V odkaze pod čiarou 10aa) sa odkazuje na ešte neexistujúcu právnu normu (zákona o dohľade v oblasti ochrany spotrebiteľa) a v §5 odsek 1 dopĺňané písmeno y) by úrad v otázke blokovania škodlivého obsahu vo vzťahu k informačným systémom prevádzkovanými rezortom ministerstva vnútra mal vydať odporúčanie na blokovanie škodlivého obsahu a samotnú realizáciu je potrebné ponechať na rezortnú jednotku CSIRT.	O	A	
RÚZSR	38. Zásadná pripomienka k čl. I., - vloženie nového novelizačného bodu V prílohe č. 1 v sektore „4. Elektronické komunikácie“ vypustiť 2. Riadok /Podsektor „Sieť a služby pevných a mobilných elektronických komunikácií správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre“. Odôvodnenie: Vid odôvodnenie k pripomienke k novelizačnému bodu 51 a vloženie nového novelizačného bodu v čl. III. Regulácia bezpečnosti EK sietí a služieb je inak štandardne predmetom	Z	N	neodôvodnená pripomienka vzhľadom k platnému právnemu vzťahu na úseku KI

	vlastného regulačného rámca pre oblasť elektronických komunikácií, z čoho vychádza aj smernica NIS, ktorá v ustanovení článku 1 ods. 3 smernice výslovne uvádza, že „bezpečnostné a oznamovacie požiadavky stanovené v tejto smernici sa nevzťahujú na podniky, ktoré podliehajú požiadavkám článkov 13a a 13b smernice 2002/21/ES“.			
RÚZSR	14. Pripomienka k čl. I., novelizačný bod 15 Vzhľadom na pripomienku k novelizačnému bodu 14 a čiastočné zachovanie pôvodného znenia § 9 ods. 2 navrhujeme zachovať tento odsek minimálne v takom rozsahu aby bolo možné kvantifikovať prevádzkové náklady Národnej jednotky CSIRT pri výkone činností pre ústredný orgán	O	N	
RÚZSR	9. Zásadná pripomienka k čl. I., novelizačný bod 10 Z uvedeného bodu nie je zrejmý rozsah súčinnosti ani konkretizácia informácií, ktoré je úrad oprávnený od uvedených subjektov požadovať. Odôvodnenie: Podľa navrhovaného znenia je úrad oprávnený požadovať od vybraných subjektov poskytnutie súčinnosti, alebo informácií, ktoré sú potrebné na plnenie úloh podľa tohto zákona, pričom návrh ide ešte ďalej, keď hovorí, že tieto subjekty sú povinné úradu požadovanú súčinnosť, alebo informácie, ktoré sú potrebné na plnenie úloh podľa tohto zákona aj poskytnúť. Z návrhu nie je zrejmé aké informácie môže úrad požadovať, pričom napr. v prípade, že ide o osobitné kategórie údajov (napr. osobné údaje, utajované skutočnosti, bankové, daňové tajomstvo, lekárske tajomstvo, lokalizačné údaje a pod.) tieto vychádzajúc z iných právnych noriem ani subjekty poskytovať nemôžu. Žiadame preto jasne precizovať druh požadovaných informácií ako aj určenie jasného účelu spracúvania úradom (aby bolo zrejmé čo sa s danými	Z	A	text preformulovaný aj s ohľadom na iné vznesené pripomienky, upravený v novom ustanovení s jasnými pravidlami.

	informáciami následne deje). Naviac ak má oprávneniu úradu korešpondovať povinnosť uvedených subjektov súčinnosť alebo informáciu poskytnúť, toto je v mnohých prípadoch spojené s dodatočnými finančnými nákladmi (nakol'ko ide o novú povinnosť subjektov) a preto požadujeme jej kvantifikáciu a vyčíslenie aj v doložke vybraných vplyvov na jednotlivé subjekty (na rozpočet verejnej správy ako aj na podnikateľské prostredie).			
RÚZSR	3. Zásadná pripomienka k čl. I. – vloženie nového novelizačného bodu Za bod 6. navrhujeme zaradiť nový bod: V § 3 písm. o) znie: „o) poskytovateľom digitálnej služby právnická osoba alebo fyzická osoba – podnikateľ, ktorá poskytuje digitálnu službu a zároveň poskytovanie digitálnej služby zabezpečuje prostredníctvom aspoň 50 zamestnancov a má ročný obrat z činnosti, ktorá je digitálnou službou, alebo celkovú ročnú bilanciou z činnosti, ktorá je digitálnou službou, viac ako 10 000 000 eur,“ Odôvodnenie: Z hľadiska kritéria rozsahu digitálnej služby je potrebné upresniť, že tieto kritéria sa majú vzťahovať výlučne na činnosť, ktorá je digitálnou službou a nie na celého podnikateľa. V opačnom prípade je totiž regulovanou digitálnou službou aj marginálna služba/ činnosť u relatívne veľkého subjektu. Nemalo by byť cieľom legislatívy regulovať z hľadiska verejného záujmu bezvýznamnú činnosť, ktorá síce má povahu digitálnej služby avšak nie je relevantná z hľadiska rozsahu. Napr. malé dátové centrum veľkej spoločnosti využívane predovšetkým pre vlastné potreby.	Z	N	Nad rámec novely, pojem je transpozíciou NIS a predstavuje konsenzus už z roku 2017.
RÚZSR	16. Zásadná pripomienka k čl. I. – vloženie nového novelizačného bodu Za novelizačný bod 16 navrhujeme zaradiť nový bod v nasledovnom	Z	N	je obsiahnuté už v dnešnom § 12

	znení: V §12 ods. 3 sa na konci vkladá veta: „Povinnosť zachovávať mlčanlivosť podľa odseku 1 sa tiež nevzťahuje na toho, kto vykonáva úlohy jednotky CSIRT podľa §15 a jeho zamestnancov v prípade trestného konania, oznamovania skutočnosti nasvedčujúcej tomu, že bol spáchaný trestný čin, alebo oznamovania kriminality.“ Odôvodnenie: V prípade trestného konania, alebo v prípade oznamovania skutočností, že bol spáchaný trestný čin, nie je akceptovateľné aby zamestnanci CSIRT nemohli poskytovať OČTK informácie. Práve jednotky CSIRT majú najviac informácií v rámci celého kontextu bezp. incidentu a práve preto má jednotka CSIRT primárne spolupracovať s OČTK.			
SBA	Čl. I, novelizačný bod 27, § 20 ods. 3 Navrhovaná novela generuje potrebu novelizácie vyhlášky NBÚ č. 362/2018 Z.z. Odôvodnenie: Technická pripomienka z dôvodu odkazovania vyhlášky na jednotlivé ustanovenia zákona.	O	ČA	predkladateľ berie na vedomie
SBA	Čl. I, novelizačný bod 1, § 2 ods. 2 písm. d) Navrhujeme doplniť osobitnú časť dôvodovej správy k predmetnému bodu o zreteľné a jednoznačné vysvetlenie úmyslu predkladateľa vrátane sledovaného cieľa navrhovanej zmeny pôvodnej textácie, ktoré eliminuje možnosť nesprávnych interpretácií negatívneho vymedzenia pôsobnosti zákona. Odôvodnenie: Navrhované znenie dotknutého ustanovenia podľa nášho názoru umožňuje viaceré interpretácie, pričom nie je jasné aký cieľ predkladateľ touto zmenou sledoval. Osobitná časť dôvodovej správy neposkytuje potrebné zdôvodnenie navrhovaných zmien. Samotné precizovanie výnimky z pôsobnosti zákona pre sektor bankovníctva, financií, finančných trhov, platobných systémov a zúčtovania cenných papierov ako vysvetlenie pomerne zásadnej	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	úpravy negatívneho vymedzenia pôsobnosti zákona ako dôvod nepostačuje, pokiaľ nie je zrejmý účel navrhovanej zmeny. Nakoľko jednou z možných interpretácií nového znenia je aj úplné vyňatie bankového sektora spod pôsobnosti zákona o kybernetickej bezpečnosti, v záujme zamedzenia nesprávneho výkladu je potrebné uviesť, čo presne bolo úmyslom predkladateľa.			
SBA	Čl. I, novelizačný bod 49, § 34 Navrhujeme doplniť prechodné a záverečné ustanovenia o ďalší bod, a to nasledovne: (12) „Ustanovením § 9 ods. 2 nie sú dotknuté zmluvy o využívaní akreditovanej jednotky CSIRT zriadenej a prevádzkovanvej iným ústredným orgánom, uzatvorené pred DD.MM.RRRR (účinnosťou zákona). Prevádzkovatelia základnej služby, ktorí využívajú akreditovanú jednotku CSIRT podľa predchádzajúcej vety, môžu takúto akreditovanú jednotku CSIRT využívať aj po DD.MM.RRRR (nadobudnutím účinnosti tohto zákona), pričom sa na nich nevzťahuje povinnosť využívať Národnú jednotku CSIRT.“	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SBA	Čl. I, novelizačný bod 24, § 19 ods. 3 Navrhujeme úpravu a doplnenie znenia § 19 ods. 2 nasledovne: „(3) Povinnosť uzatvoriť zmluvu podľa odseku 2 neplatí, ak je tretia strana prevádzkovateľom základnej služby, poskytovateľom digitálnej služby alebo prevádzkovateľom základnej služby, resp. poskytovateľom digitálnej služby v inom členskom štáte EÚ v zmysle článku 5 resp. článku 4 ods. 6 Smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.“ Odôvodnenie: Domnievame sa, že za účelom dodržania základných princípov vnútorného trhu EÚ a to	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	princípu rovnakého zaobchádzania a zákazu diskriminácie by prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb z iných členských štátov EÚ mali byť posudzovaní rovnako ako prevádzkovatelia základných služieb registrovaní v zozname prevádzkovateľov základných služieb a poskytovatelia digitálnej služby v zmysle ZoKB a na zmluvy, ktoré s nimi uzatvárajú domáci prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb by sa nemal uplatňovať prísnejší režim. Pokiaľ nedôjde k zrovnoprávneniu postavenia ekvivalentných zahraničných prevádzkovateľov základnej služby a poskytovateľov digitálnej služby s domácimi subjektmi toto ustanovenie v predloženom znení novely ZoKB je spôsobilé neodôvodnene obmedziť slobodu poskytovať služby v zmysle článku 56 ZFEÚ.			
SBA	Čl. I, novelizačný bod 24, § 19 ods. 2 Navrhujeme úpravu a doplnenie znenia § 19 ods. 3 nasledovne: „(2) Prevádzkovateľ základnej služby je povinný pri výkone činností, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby výkonu týchto činností. Pred uzatvorením zmluvy sa analyzujú riziká podľa § 20 ods. 3 písm. b) zákona. V prípade, ak v súvislosti s konkrétnou činnosťou súvisiacou s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby, vykonávanú prostredníctvom tretej strany dôjde na základe takejto analýzy k záveru, že príslušné riziko s prihliadnutím na § 20 ods. 3 písm. b) zákona je nízke, uzatvorenie zmluvy o zabezpečení	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	plnenia bezpečnostných opatrení a notifikačných povinností sa vo vzťahu k výkonu príslušnej činnosti nevyžaduje. “ Odôvodnenie: Uvedeným doplnením sa kladie dôraz na výsledok analýzy rizík, ktorá je zásadným predpokladom na posúdenie, či je potrebné uzatvorenie zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností s daným dodávateľom.			
SBA	Čl. I, novelizačný bod 32, § 27 ods. 1 písm. e) Navrhujeme úpravu a doplnenie znenia § 24 ods. 1 písm. e) „e) rozhodnutím zakázať alebo obmedziť prevádzkovateľovi základnej služby používať konkrétny produkt, proces alebo službu, ak je to potrebné na zaistenie kybernetickej bezpečnosti, alebo z dôvodov bezpečnostného záujmu Slovenskej republiky. To neplatí vo vzťahu k prevádzkovateľovi základnej služby v sektore uvedenom v bode 1. prílohy č. 1“. Odôvodnenie: Nami navrhovaným doplnením znenia §24 ods. 1 písm. e) navrhujeme zakotviť výnimku uvedenej v bode 1. prílohy č. 1. O Zákaze činnosti v sektore bankovníctvo by mala rozhodovať jedine NBS v odôvodnených prípadoch, nie je možné zo strany NBÚ zakázať napr. platobný styk a pod. Navyše dopady na bankový sektor môžu byť enormné. Ako príklad uvádzame situáciu, ak napr. úrad rozhodne o zákaze používať sieťové komunikačné zariadenia alebo diskové úložiská od konkrétneho výrobcu. Nákup, zaškolenie a výmena takejto technológie môže trvať aj viac ako 12 mesiacov a mať dopad radovo v miliónoch eur. Navyše v prípade takéhoto záväzného rozhodnutia musí úrad vymedziť mantinely rozhodnutia (časový rámec, kompenzácia prostredníctvom iných technických opatrení, ai.). Zároveň si dovoľujeme upozorniť na skutočnosť, že nakoľko má ísť o obmedzenie ktoré sa vzťahuje len na prevádzkovateľov základnej služby a v bankovom sektore	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	pôsobia aj banky, ktoré nie sú prevádzkovateľom základnej služby dôjde k narušeniu rovnováhy trhu a hospodárskej súťaže.			
SBA	Čl. I, novelizačný bod 11, § 5 ods. 4 Navrhujeme úpravu a doplnenie znenia § 5 ods. 4 nasledovne: „(4) Úrad je oprávnený požadovať od ústredných orgánov, prevádzkovateľov základnej služby, orgánov verejnej moci a právnických osôb poskytnutie súčinnosti, alebo informácií, ktoré sú potrebné na plnenie úloh podľa tohto zákona. Orgány verejnej moci, prevádzkovatelia základnej služby a právnické osoby sú povinné úradu poskytnúť požadovanú súčinnosť, alebo informácie, ktoré sú potrebné na plnenie úloh podľa tohto zákona pokiaľ im v tom nebránia platné právne predpisy.“ Odôvodnenie: Navrhujeme doplniť: „pokiaľ im v tom nebránia platné právne predpisy“. V prípade bánk a informácií ktoré sú bankovým tajomstvom by takéto znenie nestačilo, keďže by bolo potrebné prelomiť aj zákon o bankách a bankové tajomstvo, keďže tu sa taxatívne vymedzuje akým orgánom je banka oprávnená poskytnúť súčinnosť. NBU má síce v zákone o bankách oprávnenie na informácie, no iba vo vzťahu k bezpečnostným previerkam a k hláseniu incidentov.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SBA	Čl. I, novelizačný bod 14, § 9 ods. 2 Navrhujeme úpravu a doplnenie znenia § 9 ods. 2 nasledovne: „zriaďuje a prevádzkuje akreditovanú jednotku CSIRT alebo na tento účel využíva akreditovanú jednotku CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, ak sa tak dohodnú. Využívanie akreditovanej jednotky CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, sa vykonáva na základe zmluvy“ nahrádzajú slovami „využíva Národnú jednotku CSIRT; to neplatí pre podsektor Obrana a podsektor Informačné systémy verejnej správy a sektor	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky

	Bankovníctvo“. Odôvodnenie: Nakoľko z aplikačnej praxe bankového sektora vyvstala potreba presadenia sektorových špecifik a zároveň možnosť využívať jednotku CSIRT príslušného ústredného orgánu pre sektor bankovníctvo považujeme za nevyhnutné zaradiť aj sektor Bankovníctvo medzi podsektory, ktoré nevyužívajú Národnú jednotku CSIRT ale iné akreditované jednotky CSIRT, aktuálne CSIRT.MIL.SK alebo CSIRT.SK. V tomto je potrebné zároveň doplniť aj prechodné ustanovenia k predkladanému zákonu, tak ako navrhujeme v pripomienke o doplnení prechodných a záverečných ustanovení §34.			všetkých subjektov.
SBA	Čl. I, novelizačný bod 28, § 20 ods. 4 písm. a) Navrhujeme úpravu a doplnenie znenia §20 ods. 4 písm. a) nasledovne: „a) určenie manažéra kybernetickej bezpečnosti, ktorý je svojím zaradením v organizačnej štruktúre prevádzkovateľa základnej služby nezávislý od riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti, podľa osobitného predpisu.“ Odôvodnenie: V súčasnosti je určenie manažéra kybernetickej bezpečnosti upravené vo vyhláske NBÚ 362/2018 Z. z. V zmysle súčasnej úpravy manažér má spĺňať znalostné štandardy, ktoré majú byť určené osobitným predpisom. V zmysle dôvodovej správy k navrhovanému bodu 28 by mal stav ostať zachovaný a na výkon činnosti manažéra sa predpokladá preukázanie odbornej spôsobilosti v súlade s osobitným predpisom vydaným úradom.“ Doplnením úpravy role manažéra priamo do zákona dochádza k duplicite zákonnej úpravy s úpravou v podzákonnom predpise. Je predpoklad, že po novelizácii zákona dôjde zo strany NBÚ aj k úprave vyhlášky 362/2018 Z. z.. V prípade	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	vypustenia úpravy role manažéra z uvedenej vyhlášky by sa stratila legislatívna úprava stanovenia požiadaviek na manažéra.			
SBA	Čl. I, novelizačný bod 31, § 24 ods. 7 Navrhujeme vypustiť celý navrhovaný bod 31, ktorý znie: „(7) Na hlásenie kybernetických bezpečnostných incidentov alebo na zaistenie kybernetickej bezpečnosti je prevádzkovateľ základnej služby určený rozhodnutím úradu povinný zasielať automatizovaným spôsobom a v rozsahu ustanovenom v štandarde úradu určené systémové informácie zo sietí a informačných systémov.“. Odôvodnenie: Navrhované znenie odseku 7 je nad rámec riešenia bezpečnostných incidentov. Zaistenie kybernetickej bezpečnosti je kompetenciou a povinnosťou prevádzkovateľa základnej služby. Pre bankový sektor je neprípustné, aby Úrad rozhodnutím nariadil prevádzkovateľovi základnej služby napr. zasielanie sieťovej komunikácie, ktorá môže obsahovať zdrojové a cieľové IP adresy, prípadne dáta z informačných systémov. Navyše Úrad by týmto bankový sektor finančne zaťažil. Dopady na bankový sektor môžu byť minimálne v rozsahu: - systémové informácie môžu obsahovať aj údaje chránené osobitnými predpismi (osobné údaje, bankové tajomstvo) a ich očistenie je zložitý a nákladný informatický problém - náklady na HW a vývoj automatizovaného spôsobu zasielania informácií (zahŕňajúci úpravu do štandardu a zabezpečenie ochrany napr. šifrovaním) - náklady na navýšenie výkonu siete a softvérových nástrojov - náklady na zabezpečenie sieťového pripojenia (vzhľadom na veľké množstvo dát pravdepodobne na nejaký prenajatý okruh), riziko úniku citlivých informácií vzhľadom na skutočnosť, že úroveň zabezpečenia v bankovom sektore je vyššia ako na strane vládnych organizácií (viď.	Z	A	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	nedávny únik dát z NCZI).			
SBA	Čl. I, novelizačný bod 38, § 31 ods. 2 písm. d) Navrhujeme vypustiť navrhovaný bod 38 a ponechať súčasné znenie § 31 ods. 2 písm. d) ZoKB nasledovne: „d) nahlásiť závažný kybernetický bezpečnostný incident podľa § 24 ods. 1, alebo odoslať neúplné hlásenie podľa § 24 ods. 5“. Odôvodnenie: Nakoľko v pripomienkach SBA navrhujeme vypustiť celý navrhovaný bod 31, nemôže navrhovaný bod 38 figurovať ani v ustanoveniach o správnych deliktoch.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SBA	Čl. I, novelizačný bod 6, §3 písm. h) Odporúčame nahradiť pojem „sietí“ pojmom „elektronická komunikačná sieť“.	O	N	vzhľadom na akceptáciu pripomienok iných pripomienkujúcich subjektov sa pripomienka stáva bezpredmetnou
SBA	Čl. I, novelizačný bod 4, §3 písm. a) Odporúčame nahradiť pojem „údajov“ pojmom „digitálnych údajov“, nakoľko taký pojem používa aj smernica NIS.	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SBA	Čl. I, novelizačný bod 21, § 17 ods. 7 Odporúčame zvoliť vhodnejšiu formu slova „nedošlo“, a nahradiť ho nedokonavým slovesom napr. „nedochádza“ alebo pod. Odôvodnenie: Ak sa jedná o subjekt, ktorý už je v registri, tak s	O	N	vzhľadom na akceptáciu pripomienok iných pripomienkujúcich subjektov sa pripomienka stáva bezpredmetnou

	veľkou pravdepodobnosťou niekedy v minulosti k prekročeniu došlo.			
SBA	Čl. I, novelizačný bod 33, § 27a Požadujeme kompletne prepracovanie textácie navrhovaného znenia. Odôvodnenie: Inštitút blokovania v takto navrhovanom znení považujeme vzhľadom na jeho závažnosť a významný zásah do práv a slobôd garantovaných Ústavou SR za nedostatočne koncipovaný. Absentuje tu definícia, čo sa blokovaním rozumie, taktiež vzhľadom na významný zásah do práv a slobôd tu absentuje ingerencia napr. súdu či prokuratúry alebo možnosti kontroly či garantovania spravodlivého procesu. Takýmto spôsobom môže neodôvodnene dochádzať k zásahom do práv bez toho, aby mal dotknutý subjekt možnosť obrany či posúdenia nezávislým orgánom.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SBA	K celému návrhu zákona Vzhľadom na požiadavky ktoré vyplynuli z aplikačnej praxe bankového sektora vyvstala potreba novelizácie nasledovných vyhlášok: 1) Vyhláška NBÚ č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby) 2) Vyhláška NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení 3) Vyhláška NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora	O	ČA	predkladateľ berie na vedomie
SCI	Čl. I Žiadame dôsledne implementovať Európsky toolbox kybernetickej bezpečnosti 5G sietí (https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k

	mitigating-measures). Obzvlášť doplniť návrh zákona o rozmer hybridných hrozieb či politických rizík, ktoré by prevádzkovatelia základných služieb pri vyhodnocovaní rizikovosti využívania konkrétneho produktu, služby či procesu boli povinní zohľadňovať. Odôvodnenie: Slovenská republika je spolu s ďalšími členskými štátmi EÚ povinná implementovať požiadavky Európskeho toolboxu kybernetickej bezpečnosti 5G sietí do vnútroštátnej právnej úpravy. Vzhľadom na povahu a obsah tohto dokumentu sme presvedčení o tom, že jeho požiadavky by mali byť implementované práve do zákona o kybernetickej bezpečnosti ako jediného právneho predpisu svojho druhu, ktorý vo všeobecnej rovine a celoplošne naprieč všetkými sektormi a podsektormi ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti, a teda aj požiadavky na zaistenie bezpečnosti pre sektor Elektronické komunikácie, podsektor siete a služby pevných a mobilných elektronických komunikácií, kam patrí aj nová sieť piatej generácie. Účelom Európskeho toolboxu je najmä stanovenie spoločného súboru opatrení, ktoré sú schopné zmierniť hlavné riziká kybernetickej bezpečnosti sietí 5G, ktoré boli identifikované v rámci EU coordinated risk assessment report (za Slovenskú republiku dával príspevok v podobe analýzy rizík práve úrad) a poskytnúť usmernenie pre výber opatrení, ktoré by mali mať prioritu. Európsky toolbox teda identifikuje opatrenia, ktoré sú štáty vrátane Slovenskej republiky povinné implementovať do svojich vnútroštátnych poriadkov, pričom tieto opatrenia sa delia na strategické a technické a tzv. podporné činnosti. Práve tzv. strategické opatrenia sú oblasťou, na ktorú zákon žiadnym spôsobom nereflektuje, nakoľko mu nie sú známe pojmy ako politické riziká, riziká spojené s vplyvmi tretích štátov na dodávateľov, hybridné hrozby a pod..		ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
--	---	--	---

	Obmedzuje sa len na hrozby, zraniteľnosti a riziká technického charakteru. Preto považujeme za vysoko prioritné doplniť zákon o nový rozmer tzv. hybridných hrozieb, politických rizík, ktoré by prevádzkovatelia základných služieb pri vyhodnocovaní rizikovosti využívania konkrétneho produktu, služby či procesu boli povinní zohľadňovať. Uvedený model by kopíroval postup iných štátov implementujúcich Európsky toolbox, ako napríklad Poľsko alebo Francúzsko. Takto by bolo možné upustiť od zavádzania prvoplánových kompetencií na strane úradu – tie síce vo forme ako „zakázať využívať konkrétny produkt, službu, proces“ alebo „blokovat“, alebo „povinný presun informácií z prevádzky“ môžu plniť túto implementačnú úlohu, vyznačujú sa však vysokou rizikovosťou, zneužívateľnosťou, netransparentnosťou, nepredvídateľnosťou a nepreskúmateľnosťou. Navrhujeme tiež do procesu medzirezortného pripomienkového konania vložiť aj návrh sektorovej vyhlášky (vydanej podľa § 32 ods. 2 zákona o kybernetickej bezpečnosti), keďže by mala riešiť ďalší proces vyhodnocovania rizík / rizikovosti na strane dodávateľov a je s návrhom zákona úzko prepojená.			
SIS	Nad rámec novelizácie návrhu zákona a) K § 9 ods. 1 písm. b) zákona o kybernetickej bezpečnosti V § 9 ods. 1 písm. b) sa za slovo „úlohy“ vkladajú slová „spravodajskej služby“. Pripomienka je odporúčajúca. Uvedené odporúča Slovenská informačná služba predkladateľovi v rámci legislatívno-technickej úpravy zákona o kybernetickej bezpečnosti z dôvodu absencie explicitného vymedzenia konkrétneho subjektu v § 9 ods. 1 písm. b) zákona o kybernetickej bezpečnosti vo vzťahu ku ktorému sa viaže slovo „jej“. Poznamenávame, že nami	O	A	

	navrhovanou legislatívno-technickou úpravou sa nemení obsahová podstata predmetného ustanovenia.			
SIS	Nad rámec novelizácie návrhu zákona K § 10 ods. 2 zákona o kybernetickej bezpečnosti Slovenská informačná služba požaduje v rámci legislatívno-technickej úpravy zákona o kybernetickej bezpečnosti 1. za slovo „úlohy“ vložiť slová „spravodajskej služby“ z dôvodu absencie explicitného vymedzenia konkrétneho subjektu v § 10 ods. 2 zákona o kybernetickej bezpečnosti vo vzťahu ku ktorému sa viaže slovo „jej“; 2. nesprávny odkaz 19, ktorý v poznámke pod čiarou uvádza zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (§ 6 ods. 10, § 55 ods. 9, § 56 ods. 7, § 58 ods. 4 a § 69) nahradiť správnym odkazom 13, ktorý v poznámke pod čiarou odkazuje na zákon Národnej rady Slovenskej republiky č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov a zákon Národnej rady Slovenskej republiky č. 198/1994 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov. Pripomienka je odporúčajúca. Ako už bolo uvedené, ide o legislatívno-technické úpravy znenia § 10 ods. 2 zákona o kybernetickej bezpečnosti, ktorými sa nemení obsahová podstata predmetného ustanovenia.	O	A	
SIS	Čl. I - novelizačný bod 11 návrhu zákona V § 5 ods. 4 návrhu zákona sa na konci pripája táto veta: „Informácie sa poskytujú len za podmienky, že ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy spravodajskej služby podľa osobitného predpisu) alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb konajúcich v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce.“. Poznámka pod	Z	A	

	čiarou k odkazu X) znie: „X) Zákon Národnej rady Slovenskej republiky č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov.“. Odôvodnenie: Ustanovenie § 5 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej ako „zákon o kybernetickej bezpečnosti“) ustanovuje právny rámec pôsobnosti Národného bezpečnostného úradu (ďalej ako „úrad“) v oblasti kybernetickej bezpečnosti. Navrhovanou právnou úpravou sa zavádza jednak oprávnenie úradu požadovať od ústredných orgánov, prevádzkovateľov základnej služby, orgánov verejnej moci a právnických osôb poskytnutie súčinnosti alebo informácií, ktoré sú potrebné na plnenie úloh podľa tohto zákona a zároveň sa ustanovuje tomu reflektujúca povinnosť orgánov verejnej moci, prevádzkovateľov základnej služby a právnických osôb poskytnúť úradu požadovanú súčinnosť alebo informácie, ktoré sú potrebné na plnenie úloh podľa tohto zákona. Slovenská informačná služba vo vzťahu k navrhovanému doplneniu predmetného ustanovenia zákona o kybernetickej bezpečnosti konštatuje potrebu zákonnej úpravy spôsobom, ktorý zabezpečí inštitucionálne vyňatie Slovenskej informačnej služby z navrhovanej formy oprávnenia úradu a jej zodpovedajúcej povinnosti určených subjektov, a to obdobným spôsobom ako už v súčasnosti ustanovuje § 9 ods. 1 písm. b) a § 10 ods. 2 zákona o kybernetickej bezpečnosti. V tomto kontexte vo vzťahu k odôvodneniu pripomienky uvádzame, že neakceptovanie nami navrhovanej zákonnej výnimky z okruhu povinností uložených určeným subjektom predmetnou zákonnou reguláciou by mohlo viesť k ohrozeniu plnenia konkrétnej úlohy Slovenskej informačnej služby podľa zákona N R SR č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov, alebo k odhaleniu			
--	---	--	--	--

	zdrojov a prostriedkov Slovenskej informačnej služby alebo k odhaleniu totožnosti jej príslušníkov alebo osôb konajúcich v prospech Slovenskej informačnej služby. V tejto súvislosti je potrebné poznamenať, že v evidenciách a informačných systémoch vedených v pôsobnosti Slovenskej informačnej služby sú uchovávané nielen utajované skutočnosti získané vlastnou činnosťou Slovenskej informačnej služby, ale aj informácie poskytnuté Slovenskej informačnej službe v rámci medzinárodnej spravodajskej spolupráce, ktoré nie je možné poskytnúť mimo sféru dispozície Slovenskej informačnej služby bez aplikácie pravidla tretej strany, teda bez súhlasu zahraničného subjektu, ktorý je pôvodcom predmetných informácií. V tejto súvislosti poznamenávame, že uvedená zákonná požiadavka Slovenskej informačnej služby je v súlade s plnením jej zákonných úloh, ako štátneho orgánu sui generis s celoštátnou pôsobnosťou vo veciach ochrany ústavného zriadenia, vnútorného poriadku, bezpečnosti štátu a ochrany zahraničnopolitických a hospodárskych záujmov štátu.			
SK-NIC	bodu 35 Definičná formulácia „ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby” je zmätočná a jej účel je nezrozumiteľný – zamestnanec právnickej osoby je tiež vždy fyzická osoba, vo vzťahu k vykonaniu auditu však prevádzkovateľ neuzatvára právny vzťah so zamestnancom, ale s danou právnickou osobou. Takisto nie je zrejmé, prečo sú špecificky vytiahnuté niektoré typy osôb ako spoločník či štatutárny orgán, ale absentuje napr. fyzická osoba – podnikateľ, čo nie je inštitút totožný s fyzickou osobou a podobne. Túto časť odporúčame vypustiť.	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

SK-NIC	bodu 7 Návrh výrazne nesprávne pracuje s terminológiou, nakoľko - zavádza priame definície všeobecných pojmov v extrémne zúženom výklade (produkt, služba, proces) - a navyše zbytočne zavádza disharmonizáciu s pojmami už bežne zavedenými a dlhodobo používanými inou legislatívou (služba: zákon č. 136/2010 Z. z. o službách na vnútornom trhu, zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu, zákon č. 222/2004 Z. z. o dani z pridanej hodnoty, produkt: zákon č. 37/2007 o veterinárnej starostlivosti, zákon č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach, proces: zákon č. 162/2015 Z. z. Správny súdny poriadok, zákon č. 254/2008 Z. z. Školský zákon atď.), vrátane samotného tohto zákona („ropa a ropné produkty“ v prílohe č. 1), a to aj s nesprávnou vecnou definíciou, čím spôsobuje problematické výklady a možnosť kolízií pri aplikácii požiadaviek zákonov, čo je stav, ktorý by mal byť v slovenskej legislatíve neprípustný – použitie „na účely tohto zákona“ uvedené z dopadového hľadiska nijako nezmení. Pre použitie v tomto zákone odporúčame zaviesť prívlastky.	O	ČA	
SK-NIC	bodom 19 a 22 Navrhovaná zmena má vážny negatívny dopad na praktickú vykonateľnosť, pretože dotknutý prevádzkovateľ služby nemôže konať, keď o tom, nevie, zatiaľ čo k prekročeniu už mohlo objektívne prísť. Tieto body odporúčame vypustiť.	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

SK-NIC	bodu 39 Navrhované pokuty majú extrémne široký rozsah od nízkych až po principiálne ničivé, pričom nie sú definované žiadne racionálne rozhodovacie kritériá, čo je nutné doplniť.	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SK-NIC	bodu 33 Obdobne ako bod 32, uvedené ustanovenie § 27a zavádza nad rámec predmetu tohto zákona extrémne široko definovanú kompetenciu zásahov do fungovania a činnosti ľubovoľných subjektov, a to dokonca subjektov, ktoré ani nie sú predmetom tohto zákona (tzv. nedefinovaný pojem „prevádzkovateľ infraštruktúry“). Pojem „prevádzkovateľ infraštruktúry“ je tak neurčitým a vágnym pojmom, umožňujúcim svojvoľnú a účelovú interpretáciu zo strany úradu, resp. ďalších štátnych orgánov. Ods. 5 uvádza pravidlá blokovania, ktoré však nie sú na rozdiel napr. od odkazovaného návrhu zákona č. .../2020 Z. z. o dohl'ade v oblasti ochrany spotrebiteľa v návrhu pre posúdenie dopadu k dispozícii, v skutočnosti tak dotknuté ustanovenie ponecháva plnú svojvôľu určiť akékoľvek opatrenie nezávisle od jeho vykonateľnosti a dopadu na subjekt, ktorý ho má vykonať, a takisto nezávisle od možností a časovej, vecnej či právnej realizovateľnosti na strane daného subjektu a takisto zaväzuje k súčinnosti ďalšie subjekty, vrátane orgánov verejnej moci, vykonať niečo, čo nemusí byť z ich strany vykonateľné. Ods. 6 neumožňuje žiadnu právnu ochranu, čím navrhuje dať úradu vyššie kompetencie	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

ako majú súdy Slovenskej republiky alebo Policajný zbor, čo nie je pri takto vágnej kompetencii súladné so základnými princípmi právneho štátu. Navrhované znenie je v rozpore s princípom právnej istoty, ktorý je v právnom poriadku implicitne zakotvený v čl. 1 ods. 1 Ústavy SR a vyjadruje požiadavku aj na jasnosť, zrozumiteľnosť a predvídateľnosť právnych noriem a predvídateľnosť postupu orgánov verejnej moci. Návrh (ani súčasné znenie zákona) neobsahuje žiadnu konkrétnu definíciu blokovania ani obsahu, ktorý môže podliehať blokovaniu, resp. neobsahuje žiadne legislatívne vymedzenie pojmu „škodlivý obsah“ a „škodlivá aktivita“. Je pritom nevyhnutné legislatívne vymedziť predmet podliehajúci blokovaniu zo strany úradu ako aj jednotlivé formy a postupy blokovania. V opačnom prípade budú úradu priznané extrémne široké právomoci, pričom úrad tak v podstate môže rozhodnúť o blokovaní akéhokoľvek obsahu alebo aktivity. Neurčitost' a vágnosť pojmov „blokované“, „škodlivý obsah“ a „škodlivá aktivita“ je navyše v rozpore s princípom právnej istoty zakotveným v čl. 1 ods. 1 Ústavy SR, ktorá spôsobuje nepredvídateľnosť aplikácie predmetnej normy. Oprávnenie úradu svojvoľne rozhodnúť o blokovaní bližšie nevymedzeného obsahu môže naplňať znaky cenzúry, ktorá je v zmysle čl. 26 ods. 3 Ústavy SR zakázaná. Nevymedzenie pojmu „škodlivý obsah“ a „škodlivá aktivita“ považujeme za nedostatočné aj z pohľadu oprávnenosti obmedzenia základných ľudských práv a slobôd, resp. politických práv upravených Ústavou SR, a to najmä v súvislosti s obmedzením slobody prejavu a práva na informácie garantovaného v čl. 26 Ústavy SR (v rámci európskeho právneho priestoru je blokovanie prístupu k obsahu považované za flagrantný zásah do práva na slobodu prejavu). Podľa čl. 26 ods. 4 Ústavy SR právo na slobodu prejavu a právo vyhl'adávať a šíriť informácie			
--	--	--	--

možno obmedziť zákonom, ak ide o opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti. Príslušný cieľ obmedzenia musí byť v zákone stanovený jasne a zrozumiteľne. Zo všeobecnej formulácie „škodlivý obsah“ a „škodlivá aktivita“ však nie je možné vyvodiť, či má blokovaniu podliehať obsah a aktivity, ktoré ohrozujú práva a slobody iných, bezpečnosť štátu, verejný poriadok, verejné zdravie alebo mravnosť. Iné právne predpisy zakotvujúce možnosť „blokovaní“ obsahujú nielen konkretizované formy takejto blokácie, ale aj vymedzenie obsahu, resp. aktivity podliehajúc takémuto obmedzeniu. Vid' napr. § 16a ods. 1 zákona č. 43/1993 Z. z. o Slovenskej informačnej službe v alebo § 85 ods. 8 zákona č. 30/2019 Z. z. o hazardných hrách. Navyše odsek 7 neponecháva dotknutému subjektu vykonať úkon podľa zvyklosti, štandardných postupov a bežného práva, ale snaží sa mu priamo nadiktovať čo a ako má urobiť, opäť nezávisle od jeho technických, ľudských či iných možností, diskusie a analýzy dopadov. Takisto nie je zrejmé, ako chce úrad vykonať v štandardných právnych podmienkach blokovanie na aktívach a majetku tretej strany. Návrh ponecháva výlučne na rozhodnutí úradu, aby stanovil spôsob (metódu) blokovaní, pričom jediným kritériom podľa § 27a ods. 5 návrhu je, aby takýto spôsob bol „účinný, účelný a primeraný vo vzťahu k možným rizikám spojeným s blokovaním“. Úradu by tak v podstate prináležala právomoc uložiť tretiemu subjektu povinnosť výlučne podľa svojho vlastného rozhodnutia a uváženia, a to bez ohľadu na reálnu vykonateľnosť takejto povinnosti z technického, ekonomického či časového hľadiska, ako aj bez ohľadu na dopad vykonania povinnosti na povinný subjekt (tzv. prevádzkovateľa infraštruktúry) alebo iné			
---	--	--	--

	osoby, či bez ohľadu na efektívnosť a bezpečnosť takéhoto kroku. Podľa rozhodovacej praxe Európskeho súdu pre ľudské práva je pritom v rozpore s princípmi právneho štátu taká právna úprava, v ktorej je právna úvaha poskytnutá výkonnej moci vyjadrená ako neobmedzená právomoc. Zákon tak podľa ESĽP musí vyjadriť s dostatočnou jasnosťou rozsah úvahy udelenej príslušným orgánom a tiež aj spôsob jej výkonu. Z vyššie uvedeného vyplýva, že prijatím Návrhu by bola úradu v oblasti blokovania poskytnutá v podstate neobmedzená rozhodovacia aj výkonná moc, čo je v rozpore so základnými princípmi právneho štátu. Návrh navyše v rozpore s rozhodovacou praxou ESĽP nedostatočne a nejednoznačne vyjadruje rozsah úvahy udelenej úradu v oblasti rozhodovania o pristúpení k blokovaní ako i v oblasti spôsobu výkonu blokovania. Náklady na vykonanie blokovania podľa znenia návrhu v akejkoľvek situácii v plnom rozsahu znáša dotknutý subjekt, čo nie je možné napr. ani pri postupoch podľa GDPR, pričom v prípade, že je rozhodnutie priamo zo strany úradu, tento neprevezme ani len zodpovednosť za škodu, ktorá môže vyplývať z jeho rozhodnutia, t.j. dopad a riziko na strane subjektu, ktorý má vykonať blokovanie sú ešte vyššie. V tejto súvislosti je nutné všeobecne skonštatovať, že návrh je aj v rozpore s právom na súdnu a inú právnu ochranu zakotveným v čl. 46 Ústavy SR. Vzhľadom na to, že rozhodnutie Úradu o blokovaní sa podľa § 27a ods. 6 návrhu doručí len tzv. prevádzkovateľovi infraštruktúry, ďalšie osoby, do ktorých práv môže byť blokovaním zasiahnuté (napr. držiteľ domény, prevádzkovateľ blokovanej webovej stránky), sa o tomto zásahu v prvom rade ani nemusia dozvedieť a v druhom rade nemajú k dispozícii účinný prostriedok nápravy, prípadne obrany proti danému rozhodnutiu. Držiteľ domény, prevádzkovateľ webovej stránky alebo iná osoba, ktorá blokovaním utrpela zásah do			
--	--	--	--	--

	svojich práv nemá možnosť žiadať o preskúmanie rozhodnutia úradu v odvolacom konaní a ani v rámci správneho súdnictva (napríklad v prípade obrany pred vydaním nezákonného rozhodnutia). Dané osoby totiž nemajú aktívnu legitimáciu na podanie správnej žaloby proti rozhodnutiu orgánu verejnej správy podľa Správneho súdneho poriadku. Návrh nezabezpečuje účinné mechanizmy nápravy nezákonných rozhodnutí a nerešpektuje procesné záruky pre tieto tretie osoby (napríklad pre držiteľov domén). Upozorňujeme aj na to, že i keď v iných právnych predpisoch existuje možnosť vydania príkazu na zamedzenie prevádzky webového sídla alebo prístupu na doménové meno, príslušné rozhodnutie vydáva súd na žiadosť orgánu výkonnej moci. Takýmto spôsobom je na rozdiel od predloženého návrhu zabezpečené aspoň minimálne preskúmanie dôvodnosti a rozsahu blokovania (tzn. zásahu do práv iných osôb), jeho trvania a vyváženosti zo strany nezávislého a nestranného súdu. Navrhované ustanovenie zasahuje aj do práva vlastníť a pokojne užívať majetok garantovaného čl. 20 Ústavy SR ako aj do práva podnikateľ zakotveného v čl. 35 Ústavy SR. Znenie návrhu totiž pripúšťa možnosť výkonu blokovania priamo úradom a to nielen v prípade, že by tzv. prevádzkovateľ infraštruktúry nevykonával blokovanie na základe rozhodnutia úradu, ale v podstate v akejkoľvek situácii. Uvedené znamená, že úradu ako orgánu verejnej moci by mohli byť priznané právomoci zasiahnuť do infraštruktúry, systémov, priestorov či iného technického vybavenia daného prevádzkovateľa a teda obmedziť jeho vlastnícke práva. Nútené obmedzenie vlastníckych práv je dovolené, iba ak sa uskutoční v súlade s kumulatívne určenými podmienkami stanovenými v čl. 20 ods. 4 Ústavy. V danom prípade nie sú splnené kritéria oprávnenosti zásahu do majetku zo strany štátnych orgánov, nakoľko návrh			
--	---	--	--	--

	nielenže neupravuje nevyhnutnú mieru takéhoto zásahu, súčasne predložené znenie neobsahuje ani žiadne vysvetlenie, z ktorého by bolo možné odôvodniť verejný záujem na zásahu štátu do vlastníctva fyzických či právnických osôb. Nad rámec toho návrh žiadnym spôsobom nerieši povinnosť štátu poskytnúť prevádzkovateľovi infraštruktúry primeranú náhradu za spôsobený zásah do vlastníckeho práva. Uvedené ustanovenie je nutné bezpodmienečne vypustiť v celom rozsahu alebo zásadne prepracovať. Táto pripomienka je zásadná.			
SK-NIC	bodu 24 Odsek 2 je nutné doplniť, nakoľko zavádza povinnosť uzatvoriť zmluvu v súvislosti s akýmkoľvek sieťami a informačnými systémami prevádzkovateľa základnej služby a nie iba tými, ktoré sú nutné pre poskytovanie základnej služby. Uvedený problém sa nachádza už aj v pôvodnom znení, čím presahuje rámec pôvodného zámeru a snaží sa regulovať aktíva, ktoré nie sú predmetom tohto zákona. Táto pripomienka je zásadná.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SK-NIC	bodu 45 Písmeno h) je nutné vypustiť – požiadavky s tak závažným dopadom je v prípade ponechania ustanovenia o blokovaní potrebné zadefinovať priamo v zákone. Nejasnosť navrhovaného § 27a neodstránia ani pravidlá pre blokovanie, ktorý by mali byť vydané úradom, nakoľko dané pravidlá si opäť stanoví, vydá a môže kedykoľvek zmeniť sám úrad. Sme presvedčení, že bližšie vymedzenie nejasných a neurčitých pojmov použitých v návrhu, ktoré umožňujú úradu zasiahnuť do viacerých ústavných práv jednotlivcov nemôžu byť vykonané formou podzákonného právneho	Z	A	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	predpisu ale musí byť súčasťou predpisu s právnou silou zákona. V opačnom prípade by došlo k zjavnému porušeniu ústavných garancií upravujúcich striktné podmienky, za splnenia ktorých môžu byť základné práva obmedzené napríklad rozhodnutím štátneho orgánu (napríklad čl. 13 Ústavy SR a čl. 26 ods. 4 Ústavy SR). Táto pripomienka je zásadná.			
SK-NIC	bodu 10 Podľa odkazovaného (10aa) pripravovaného zákona č. .../2020 Z. z. o dohľade v oblasti ochrany spotrebiteľa rozhodnutie o blokovaní vydáva súd, čo zaručuje primerané vecné preskúmanie aj právnu ochranu, zatiaľ čo úrad nie je orgánom kompetentným pre riešenie otázok ochrany spotrebiteľa a nie je teda dôvodné, aby mu bola pridelená kompetencia podľa odkazovaného predpisu, môže nanajvýš vydať podporné stanovisko, uvedené prepojenie na nepríslušnú legislatívu je preto potrebné odstrániť. Takisto vôbec nie je zrejmé ako by mal úrad zabezpečovať vykonanie naznačované v tomto ustanovení, keďže spravidla ide o služby, činnosti a majetok patriace tretím stranám a nie úradu, čo bez ďalšieho spresnenia takisto nie je možné akceptovať. Táto pripomienka je zásadná.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SK-NIC	analýze podnikateľského prostredia Popísaná analýza je skutkovo nesprávna – za prvé sa dotýka akéhokoľvek prevádzkovateľa základnej služby a nie iba podnikov s viac ako 250 zamestnancami (naša spoločnosť má napr. niečo cez 10 interných zamestnancov) a za druhé má návrh vážny negatívny vplyv, ktorý je tu skonštatovaný ako „nepredpokladá priamy vplyv na podnikateľské prostredie“. Negatívny vplyv vyplýva najmä z nutnosti - implementovať funkčné automatizované zasielanie údajov podľa bodu 31, čo môže znamenať programátorský zásah do	O	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky

	neznámeho množstva systémov, vrátane možnosti ohrozenia bezpečnosti keď daný systém nie je stavaný na akýkoľvek takýto export a dotknuté údaje podliehajú rôznym typom právnej ochrany, - prestať používať ľubovoľnú technológiu resp. produkt podľa bodu 32, čo môže znamenať nutnosť úplnej výmeny hardvéru alebo softvéru alebo dokonca znefunkčnenie služieb, ku ktorým sa viažu právne aj legislatívne záväzky a sankcie, - vyčleniť finančné prostriedky na zamestnanie bezpečnostného manažéra podľa bodu 28 a - vykonávať neznáme ľubovoľné opatrenia na blokovanie podľa bodu 33, ktoré môže úrad uložiť, a to technického, organizačného či akéhokoľvek iného charakteru bez ohľadu na možnosti a zdroje dotknutého subjektu (predpoklad, že pri blokovaní sa nepredpokladajú finančné dopady je v tomto tiež nesprávny, pretože minimálne procesno-technická implementácia má vysokú pravdepodobnosť osobitných výdajov), a vo všetkých prípadoch bez možnosti primerane reagovať alebo namietat' voči vecne neprimeraným rozhodnutiam, resp. dôjsť k racionálnemu riešeniu. Zároveň konštatujeme, že spomínaná konzultácia bola uskutočnená pravdepodobne iba s niektorými vybranými subjektmi, zd'aleka však nie so všetkými oblasťami a subjektmi nepriamo vymenovanými zákonom a zodpovednými za konkrétnu oblasť – konkrétne dotknutý subjekt v sektore č. 3, časti „subjekt spravujúci alebo prevádzkujúci register internetových domén najvyššej úrovne” prílohy č. 1 zákona je na Slovensku práve jeden (naša spoločnosť) a s nami žiadna konzultácia neprebehla. Predbežná informácia má takisto iba informatívny charakter a dotknutý obsah nie je možné považovať za záväzný ani finálny, pričom subjektom, ktoré nie sú povinne pripomienkujúcimi informácia o takomto konaní nie je zasielaná.			všetkých subjektov.
--	---	--	--	---------------------

SK-NIC	 bodu 11 Uvedená kompetencia je príliš vágna a výklad môže byť veľmi široký, je preto nutné doplniť v akej veci a v akom rozsahu majú jednotlivé subjekty poskytovať súčinnosť, nakoľko uvedené ustanovenie umožňuje požadovať súčinnosť v ľubovoľnom plnení zákona úradom, napr. aj ktoréhokoľvek prevádzkovateľa základnej služby pri posudzovaní zhody zo strany úradu voči úplne inému subjektu. Táto pripomienka je zásadná.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SK-NIC	 bodu 25 Uvedená úprava má opäť negatívny dopad, pretože prevádzkovateľ nemá kompetenciu a ani odbornú znalosť či možnosť analýzy na identifikáciu a určovanie čo je trestný čin, oznamovať ho teda môže iba keď mu to oznámi niekto, kto takúto kompetenciu má. Navyše nie je zrejmé akým spôsobom by ho mal oznamovať, nakoľko od bežného súkromného subjektu nie je možné očakávať, že bude podávať celé trestné oznámenie, keď ani nevie, či je to tak. Formulácia „že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka“ je takisto v celkovom kontexte identifikácie incidentu a príslušnej notifikácie nezrozumiteľná, pretože bezpečnostný incident je buď spôsobom alebo nástrojom na spáchanie trestného činu, t.j. trestný čin je dôsledok, ale nejde tu o „týkanie sa“. Uvedené znenie je preto potrebné preformulovať, aby bolo vykonateľné a nezaďávalo neprimeranú povinnosť. Táto pripomienka je zásadná.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SK-NIC	 bodu 28 Uvedené má zásadný finančný a funkčný dopad na prevádzkovateľa základnej služby, pretože mu vnucuje povinné zamestnanie	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť

	konkrétnej osoby so zásahom do jeho organizačnej štruktúry nezávisle od možností a počtu zamestnancov prevádzkovateľa základnej služby a navyše nepriamo vyžaduje povinnú certifikáciu takejto osoby. Uvedené ustanovenie je nutné vypustiť alebo preformulovať do podoby, ktorá nemá takýto vážny dopad. Táto pripomienka je zásadná.			návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SK-NIC	 bodu 31 Uvedené ustanovenie ide úplne nad rámec ohlasovania incidentov a snaží sa neregulovaným spôsobom získať neznámy rozsah informácií, ktoré môžu byť aj predmetom inej zákonnej ochrany a núti prevádzkovateľa programovo vytvárať nejaké aplikačné riešenia k tejto osobitnej oznamovacej povinnosti, ku ktorým nemusí mať ani prostriedky, ani schopnosť ich urobiť, pričom úrad si môže svojvoľne určiť ľubovoľného prevádzkovateľa základnej služby. Znenie javí rovnaký problém nesúladnosti s Ústavou a nezaistenia právnej istoty ako body 32 a 33. Celé ustanovenie je nutné vypustiť, k osobitným spôsobom ohlasovania je postačujúci § 24 odsek 6. Táto pripomienka je zásadná.	Z	A	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SK-NIC	 bodu 29 Uvedené ustanovenie nie je zrozumiteľné, ani riadne vykonateľné – prečo sa má uzatvárať táto zbytočná vzájomná zmluva, keď prevádzkovateľovi základnej služby aj poskytovateľovi digitálnej služby vyplýva notifikačná povinnosť aj ostatné povinnosti priamo z tohto zákona a navyše prevádzkovateľ základnej služby ju nemá uzatvárať v opačnom vzťahu už podľa bodu 24 samotného tohto návrhu. V praxi to znamená, že každý poskytovateľ digitálnej služby môže vyžadovať od prevádzkovateľa základnej služby zmluvu s inými podmienkami, keďže zmluva je dvojstranný právny akt,	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	pričom prevádzkovateľ poskytuje základnú službu všetkým rovnako, a takáto zákonná povinnosť má zásadný dopad vo všetkých aspektoch vzájomného vzťahu týchto subjektov a narušuje riadne poskytovanie základnej služby za riadnych podmienok. Uvedené znenie je nutné zosúladiť s princípmi obdobného znenia v § 19, pričom totožný problém je už v aktuálne platnom znení. Táto pripomienka je zásadná.			
SK-NIC	bod 32 Uvedené ustanovenie porušuje základné princípy právneho štátu, pretože bez akejkoľvek možnosti právnej ochrany, vzájomnej komunikácie, analýzy dopadu a prevzatia zodpovednosti navrhuje vykonať zásah do fungovania a činnosti prevádzkovateľa základnej služby takým spôsobom, ktorý môže zásadne porušiť iné právne záväzky a podmienky pre fungovanie a činnosť prevádzkovateľa základnej služby, a to dokonca v ľubovoľnej lehote a v neobmedzenom rozsahu aj nad rámec toho, čo sa týka jeho pozície prevádzkovateľa základnej služby. Takisto to neprimerane zasahuje do podmienok podnikateľského prostredia na strane výrobcov produktov, pričom kritériá k iniciácii takéhoto zákazu návrh v princípe nedefinuje – odôvodnenie použité v znení je extrémne široké a umožňuje prakticky čokoľvek. Navrhované znenie je teda v rozpore s princípom právnej istoty, ktorý je v právnom poriadku implicitne zakotvený v článku 1 ods. 1 Ústavy SR a vyjadruje požiadavku aj na jasnosť, zrozumiteľnosť a predvídateľnosť právnych noriem a predvídateľnosť postupu orgánov verejnej moci. Navrhnutá právna úprava takisto nerešpektuje závery predmetného Odporúčanie Výboru ministrov Rady Európy CM/Rec(2018)2 o úlohách a zodpovednosti internetových sprostredkovateľov zo 7.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	marca 2018 v dôsledku čoho môže v budúcnosti dochádzať k neoprávneným zásahom zo strany štátu do ľudských práv a základných slobôd adresátov rozhodnutí o blokovaní, ako aj osôb dotknutých týmito rozhodnutiami. Uvedené sa týka aj bodu 33 návrhu. Toto ustanovenie je nutné vypustiť v celom rozsahu. Táto pripomienka je zásadná.			
SK-NIC	bodu 36 V uvedenom ustanovení nie je zrejmé o akú právnickú osobu má ísť, zákon pracuje s inými názvami subjektov a navyše prvá a posledná veta pôsobia vo vzájomnom kontexte veľmi zmätočne. Odporúčame upraviť. V odseku sa aj zbytočne miešajú viaceré nezávislé aspekty – ako sa zabezpečuje audit a jeho podmienky a možnosti na strane audítora – odporúčame rozdeliť na samostatné odseky.	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SK-NIC	bodu 27 Zákon pozná a pracuje iba s pojmom kybernetická bezpečnosť, nie je preto zrejmé prečo návrh obsahuje aj pojem informačná bezpečnosť a čo má tento pojem na rozdiel od kybernetickej bezpečnosti znamenať – presah do spravovania informácií mimo digitálneho priestoru nie je v rozsahu ani kompetencii tohto zákona.	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SK-NIC	bodu 44 Zákonné podmienky s tak závažným dopadom na činnosť prevádzkovateľa základnej služby, akými sú pravidlá auditu	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť

	kybernetickej bezpečnosti, časový rozsah a periodicita vykonávania auditu kybernetickej bezpečnosti nemožno stanoviť vykonávacím predpisom, ale je nutné ich zadefinovať priamo v tomto zákone. Táto pripomienka je zásadná.			návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SK-NIC	bod 50 Znenie zavádza neznámy pojem “DNS hosting” a “mailhosting”, pričom poskytovatelia služieb systému doménových mien na internete sú už v prílohe č. 1 zahrnutí aj v platnom znení. Uvedené znenie je nutné spresniť, resp. odstrániť duplicity. Elektronický obchod ako taký nemožno považovať za základnú službu, navyše zahrnutie poskytovateľa akéhokoľvek malého elektronického obchodu do podmienok takejto striktnej regulácie je zásadne neprimerané a preto je potrebné ho vypustiť. Zároveň sa týmto zavádza neadekvátne nepriama regulácia subjektov už regulovaných napr. zákonom č. 22/2004 Z. z. o elektronickom obchode a ďalšími predpismi, ako napr. tými z oblasti zdravotníctva či bankovníctva, ktoré takisto definične spĺňajú navrhované znenie a zároveň sú krížovo zahrnuté aj pod inými sektormi podľa tejto prílohy. Túto časť je nutné vypustiť. Táto pripomienka je zásadná.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
SOCPOIST	K článku I - k bodu 11 – k § 5 ods. 4 Podľa navrhovaného znenia Národný bezpečnostný úrad (ďalej len „úrad“) je oprávnený požadovať od ústredných orgánov, prevádzkovateľov základnej služby, orgánov verejnej moci a právnických osôb poskytnutie súčinnosti, alebo informácií, ktoré sú potrebné na plnenie úloh podľa tohto zákona, pričom orgány verejnej moci, prevádzkovatelia základnej služby a právnické osoby	O	N	vzhľadom na skutočnosť, že ustanovenie bolo vypustené, pripomienka sa stáva bezpredmetnou

	sú povinné úradu poskytnúť požadovanú súčinnosť, alebo informácie, ktoré sú potrebné na plnenie úloh podľa tohto zákona. Podľa § 170 ods. 2 zákona č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov, Sociálna poisťovňa môže poskytovať údaje zo svojho informačného systému len so súhlasom fyzických osôb a právnických osôb, ktorých sa údaje priamo týkajú, ak tento zákon alebo osobitný predpis neustanovuje inak. Ak podľa navrhovaného odseku 4 povinné subjekty majú poskytovať úradu aj osobné údaje a údaje zo svojho informačného systému, na zabezpečenie zákonnosti poskytovania údajov bez súhlasu dotknutej osoby v súlade s § 13 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a s § 170 ods. 2 zákona č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov, považujeme za potrebné znenie upraviť tak, aby bolo jednoznačné, že subjekty uvedené v odseku 4 poskytnú požadovanú súčinnosť, alebo informácie bez súhlasu dotknutej osoby.			
ÚJDSR	I. K vlastnému materiálu Čl. I: 1. K § 3 písm. h): text vloženého ustanovenia logicky nenadväzuje na predchádzajúci text. Úrad žiada text opraviť. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.	O	A	
ÚJDSR	I. K vlastnému materiálu Čl. I: 10. K § 20 ods. 1: v predvetí tohto ustanovenia úrad odporúča konkretizovať o zmenu ktorej konkrétnej vety ide, nakoľko ide rozsahom o veľký odsek. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.	O	A	

ÚJDSR	I. K vlastnému materiálu Čl. I: 11. K § 20 ods. 3: rozsah bezpečnostných opatrení bol rozšírený a čiastočne prevzatý z doteraz platného zákona. Medzi jednotlivými oblasťami chýba: - riadenie hrozieb a aktív (§ 20 ods. 3 písm. b) súčasne platného zákona), - testovanie bezpečnosti (§ 20 ods. 3 písm. k) súčasne platného zákona). Závažnejším dôvodom pripomienky je to, že zákon nebude vykonateľný, ak sa nebude súčasne s ním novelizovať vyhláška NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška č. 362/2018 Z. z.“). V prípade, že nie je možné súčasne so zákonom novelizovať aj uvedenú vyhlášku, je nevyhnutné, aby bolo určené prechodné obdobie, do ktorého bude musieť byť vyhláška č. 362/2018 Z. z. novelizovaná a určenie doby, do ktorej nebudú musieť orgány a organizácie meniť dosiaľ platnú internú dokumentáciu. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Zásadná pripomienka.	Z	N	Zavádzané bezpečnostné opatrenia nie sú nové inštitúty, vychádzajú z platných štandardov a postupov. To znamená, že aj keď vykonávací predpis momentálne neustanovuje podrobnosti o nich, "nejakým" spôsobom sa dajú plniť. Vykonávací predpis bude predmetom MPK po nadobnutí účinnosti novely zákona, uvedenie prechodného obdobia nie je možné vzhľadom na nepredvídateľné trvanie legislatívneho procesu upraviť tak, aby nebolo jednak príliš krátke alebo na strane druhej príliš dlhé. Máme za to, že plnenie bezpečnostných opatrení je zjavne možné a realizovateľné aj bez podrobností vo vyhláške, ktorá v zásade kopíruje bezpečnostný štandard (ISO 27 000 vyššie)
ÚJDSR	I. K vlastnému materiálu Čl. I: 12. K § 20 ods. 4 písm. a) návrhu zákona a k doložke vybraných vplyvov: úrad žiada vyčiarknuť v navrhovanom ustanovení slová „svojím zaradením v organizačnej štruktúre prevádzkovateľa základnej služby“. Text ustanovenia tak bude znieť takto: „a) určenie manažéra kybernetickej bezpečnosti, ktorý je nezávislý od riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,“. Definovaním manažéra kybernetickej	Z	ČA	Organizačné zaradenie funkcie manažéra kybernetickej bezpečnosti nepredstavuje žiadne objektívne znemožnenie riešenia situácií popísaných vo Vašej pripomienke. Ide o formálne určenie funkcie, nie o konkrétne zaradenie konkrétnej osoby. Rovnako je z povahy Vašich vznesených pripomienok dôležité uviesť, že povinnosť určiť manažéra

bezpečnosti medzi kmeňovými zamestnancov prevádzkovateľa základnej služby je odopretá možnosť pre malé orgány štátnej správy a samosprávy vrátane obcí a obecných úradov, zazmluvniť si jedného manažéra kybernetickej bezpečnosti pre viaceré orgány, organizácie alebo obce. Odôvodnenie: V praxi sa stále úrad potýka s tým, že sú podmienky pre oblasť informačnej a kybernetickej bezpečnosti stanovené podľa predstáv o fungovaní veľkých rezortov. Nie je možné ani reálne aplikovať tieto požiadavky v plnom rozsahu a v plnej výške bez rozdielu na všetky ministerstvá a ostatné ústredné orgány štátnej správy a na všetkých prevádzkovateľov základnej služby. Stav odborných kapacít na riadenie kybernetickej bezpečnosti je v SR žalostný, a nie je to len finančný, ale aj personálny problém. Obsadenie a možnosti jednotlivých ústredných orgánov a vôbec prevádzkovateľov základných služieb, veľmi variuje, niekde je celá sekcia informatiky, niekde je odbor informatiky a niekde sú k dispozícii len 1-2 informatici. Všetko záleží od veľkosti rezortu, ale i od možnosti financovania týchto odborných kapacít, pričom verejná správa rieši všeobecný nedostatok odborníkov v tejto oblasti. Okrem toho kapitoly, ktoré nečerpajú peniaze z fondov EÚ, keďže finančné limity projektov sú pre projekty vskutku vysoké, nemajú dodatočné zdroje na financovanie vysokokvalifikovaných zamestnancov a je aj otázne, či je im možné pridelovať prácu na plný úväzok, keďže to má byť informatik, ale vykonávať štandardnú prácu informatických služieb vlastne nemôže. Otázne je, či práca manažéra kybernetickej bezpečnosti je prácou na plný úväzok na celý rok. V prípade, že aj napriek našej požiadavke, bude trvať predkladateľ na výkone týchto činností interným zamestnancom, tak sa má požiadavka v praxi realizovať, je nutné potrebné vyčíslieť a vyčleniť finančné		kybernetickej bezpečnosti nie je vyžadovaná pre všetkých PZS. Vo vyhláske č. 362/2018 ZZ sa uvádza, že funkcia určenia manažéra kybernetickej bezpečnosti je povinná pre kategórie sietí a informačných systémov III, čo prakticky znamená, že sa týka PZS so složitějšími IS a tými najcitlivejšími údajmi a pre subjekty (ako napríklad malé obce) nie je povinná, ale len odporúčaná.
---	--	---

	prostriedky na ich pozíciu, t. j. v rozsahu minimálne 1 štátnozamestnanecké miesto v 9. platovej triede (aby bola aspoň malá šanca, že niekoho s takto nastavenými požadovanými znalostnými štandardmi vôbec úrad získa). Z uvedených dôvodov úrad navrhuje ponechať možnosť výkonu týchto služieb externe alebo vyčíslit' a uviesť náklady na plnenie tejto povinnosti pre prevádzkovateľov v doložke vybraných vplyvov a zabezpečiť jej financovanie z prostriedkov štátneho rozpočtu alebo z iných zdrojov tak, aby povinné osoby mali vytvorené možnosti pre jej naplnenie. Na základe uvedeného úrad žiada, aby prioritne bola zachovaná možnosť realizovať tento princíp aj prostredníctvom externých odborných kapacít. Zároveň úrad žiada doplniť znenie zákona aj o znalostné štandardy manažéra KB alebo odkázať na konkrétny predpis, ktorý upravuje znalostné štandardy v záujme právnej istoty. Doterajšia vyhláška č. 362/2018 Z. z. síce odkazovala na osobitný predpis, ktorý ale nebol konkretizovaný. Zásadná pripomienka.			
ÚJDSR	I. K vlastnému materiálu Čl. I: 13. K § 20 ods. 4 písm. a): v súvislosti s predchádzajúcou pripomienkou č. 12 úrad navrhuje doplniť všeobecnú definíciu znalostných štandardov a definovanie základných znalostných štandardov priamo v zákone. Detailné rozpracovanie týchto štandardov bude následne vo všeobecne záväznom právnom predpise, ktorý vydá NBÚ. Bez základných znalostných štandardov nie je v súčasnosti možné zamestnať manažéra kybernetickej bezpečnosti. Ak by ktorýkoľvek orgán verejnej moci prijal zamestnanca do služobného alebo pracovného pomeru na miesto manažéra kybernetickej bezpečnosti a po prijatí všeobecne záväzného právneho predpisu určujúceho znalostné štandardy by	Z	N	Znalostný štandard na manažéra kybernetickej bezpečnosti je už dnes dostupný a aplikovateľný. Vyhláška bude reflektovať tento štandard a tak, ako je to aj pri bezpečnostných opatreniach, nebude v tomto vykonávacom predpise obsiahnuté nič nad rámec týchto štandardov. Pre náš zaužívaný systém legislatívy ja naozaj neprínosné, aby sa v texte zákona odkazovalo na štandardy, ktoré môžu podliehať rýchlym zmenám vzhľadom

	musel prepustiť kvôli tomu, že prijatý zamestnanec tieto štandardy nespĺňa, bolo by to v rozpore s morálkou a etikou a následne by to mohlo vyústiť až do súdneho sporu medzi prepusteným zamestnancom a orgánom verejnej moci. Ak by boli základné znalostné štandardy definované zákonom, bolo by pre orgán verejnej moci oveľa jednoduchšie nastaviť výberové podmienky pre prijatie manažéra kybernetickej bezpečnosti bez rizika následných súdnych sporov. V súčasnosti, práve pre neexistenciu základných znalostných štandardov, nie sú miesta manažérov kybernetickej bezpečnosti obsadené na viacerých orgánoch verejnej moci. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Zásadná pripomienka.			na meniace sa bezpečnostné prostredie. V takom zmysle by potom mohlo dôjsť k situácii, kedy by bol zozávezený štandard nevykonateľný.
ÚJDSR	I. K vlastnému materiálu Čl. I: 14. K § 24 ods. 7 a § 31 ods. 2 písm. d): podľa názoru úradu ide o nejasné ustanovenia. Aký je automatizovaný spôsob zasielania hlásení? A aký je rozsah zasielaných údajov? Úrad žiada doplniť význam slovného spojenia „automatizovaný spôsob“ a vysvetliť o aké informácie má NBÚ záujem. Alternatívne riešenie by mohlo byť vypustiť toto ustanovenie z dôvodu, že nie je možné trvale zasielať systémové a sieťové informácie z každej základnej služby. Niektoré základné služby nie sú pripojené do verejnej siete, pretože takéto pripojenie by mohlo narušiť ich bezpečnosť. Vzhľadom na novú povinnosť, ktorá si vyžiada navýšené kapacity z dôvodu projektového riadenia, finančných nákladov na samotný systém a aj technické zabezpečenie, úrad žiada odložiť účinnosť tohto ustanovenia a určenie prechodného obdobia. Zároveň je potrebné brať do úvahy, že bude nevyhnutné uzatvoriť zmluvu s integračným zámerom a testovacím prostredím pre automatizáciu, navýšenie dátového pripojenia do siete Govnet pre orgány štátnej správy.	Z	ČA	text preformulovaný aj s ohľadom na iné vznesené pripomienky, doplnená dôvodová správa

	Takisto je potrebné vziať do úvahy aj fakt, že nie je možné jednoduchým spôsobom zasielať veľký počet dát v prípade kybernetického bezpečnostného incidentu na veľké vzdialenosti. Z týchto dôvodov úrad uprednostňuje vypustiť predmetné ustanovenia z návrhu zákona. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Zásadná pripomienka.			
ÚJDSR	I. K vlastnému materiálu Čl. I: 15. K § 24 ods. 7: uvedené ustanovenie je nejasné aj z dôvodu, že „rozhodnutie úradu“ sa týka „určenia prevádzkovateľa základnej služby“, „určenia povinnosti hlásenia kybernetických bezpečnostných incidentov alebo na zaistenie kybernetickej bezpečnosti“ alebo povinnosti zasielať ich „automatizovaným spôsobom“. V prípade prvej možnosti sa naráža na rozpor s § 17 zákona a tiež uvedená rozhodovacia právomoc nevyplýva z § 5 zákona. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.	O	A	text preformulovaný aj s ohľadom na iné vznesené pripomienky
ÚJDSR	I. K vlastnému materiálu Čl. I: 16. K § 27 ods. 1 písm. e): definovať pojem „bezpečnostný záujem“. Odôvodnenie: používanie pojmov bez ich konkretizácie, resp. definovania môže v budúcnosti vyvolávať výkladové problémy pri ich aplikácii v praxi. Odporúčajúca pripomienka.	O	A	
ÚJDSR	I. K vlastnému materiálu Čl. I: 17. K § 27a: definovať pojem „blokovanie“. Odôvodnenie: používanie pojmov bez ich konkretizácie, resp. definovania môže v budúcnosti vyvolávať výkladové problémy pri ich aplikácii v praxi. Zrozumiteľne definovaný pojem „blokovanie“ prispeje k	O	N	Konkrétnosti budú uvedené vo vykonávacom predpise, vzhľadom na rôzne možnosti a spôsoby blokovania nie je možné pojem dostatočne zovšeobecniť.

	jednoznačnému výkladu novej činnosti. Odporúčajúca pripomienka.			
ÚJDSR	I. K vlastnému materiálu Čl. I: 18. K § 27a ods. 2: podľa navrhnutého ustanovenia NBÚ rozhodne o blokovani, ale neurčuje sa, kto znáša náklady na blokovanie. Bude to financovať štát, NBÚ alebo prevádzkovateľ základnej služby? Úrad žiada doplniť spôsob financovania blokowania a v zmysle úpravy doplniť Doložku vybraných vplyvov a Analýzu vplyvov na rozpočet verejnej správy, na zamestnanosť vo verejnej správe a financovanie návrhu. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Pripomienka je zásadná.	Z	A	text preformulovaný aj s ohľadom na iné vznesené pripomienky
ÚJDSR	I. K vlastnému materiálu Čl. I: 19. K § 27a ods. 4: text „súčasťou rozhodnutia úradu o blokovani je vykonateľné rozhodnutie žiadateľa o blokovanie“ upraviť, nakoľko podľa navrhnutého znenia bude vydávať rozhodnutie aj žiadateľ? Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.	O	A	bližšie vysvetlené v DS
ÚJDSR	I. K vlastnému materiálu Čl. I: 2. K § 3 písm. s): úrad žiada zosúladiť definíciu pojmu „služba“ s definíciou pojmu „základná služba“. Z definície pojmu „služba“ vyplýva, že ide o virtuálny systém, kým pri definícii pojmu „základná služba“ ide o činnosť, ktorá závisí od sietí a informačných systémov alebo je prvkom kritickej infraštruktúry, čo môžu byť objekty, stavby, služby vo verejnom záujme. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.	O	A	
ÚJDSR	I. K vlastnému materiálu Čl. I:	O	A	

	20. K § 27a ods. 6: rozhodnutie o blokovani nemôže byť konečným rozhodnutím, pretože sa na tento akt správneho práva nevzťahuje výnimka zo správneho poriadku podľa § 33 ods. 1 zákona. Úrad navrhuje poslednú vetu vyčiarknuť a doplniť do § 5 ods. 1 písm. u) zákona ďalší typ rozhodnutie, ktoré NBÚ vydáva o blokovani. Alternatívne riešenie je doplniť do § 33 ods. 1 zákona odkaz na § 27a ods. 6 návrhu zákona . Tým bude zabezpečené, že sa na toto rozhodnutie nevzťahuje správny poriadok. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.			
ÚJDSR	I. K vlastnému materiálu Čl. I: 21. K poznámke pod čiarou k odkazu 28a): úrad navrhuje vypustiť text „zákon č. .../2020 Z. z. o dohľade v oblasti ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov“ alebo číslo zákona doplniť. Nie je možné odvolávať sa na neexistujúci právny predpis. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.	O	A	
ÚJDSR	I. K vlastnému materiálu Čl. I: 22. K § 29 ods. 3: nie je zrejmé o akú osobu v prípade pojmu „fyzická osoba“ ide. Úrad predpokladá, že nakoľko v prípade zabezpečovania auditu kybernetickej bezpečnosti podľa § 29 ods. 4 návrhu zákona pôjde o podnikanie, malo by ísť v prípade fyzickej osoby o živnostníka. Ak je tomu naozaj tak, je potrebné text upraviť. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.	O	A	Upravené na základe požiadaviek praxe, vysvetlené v DS, že ide vždy o FO, ktorú môže zamestnávať aj PO, aj sám môže byť štatutárom.
ÚJDSR	I. K vlastnému materiálu Čl. I: 23. K § 31 ods. 5 písm. c): doplniť na koniec textu „písm. e)“.	O	N	

	Odôvodnenie: požiadavka presnosti právneho predpisu. Odporúčajúca pripomienka.			
ÚJDSR	I. K vlastnému materiálu Čl. I: 24. K § 32 ods. 1 písm. b): po nahradení slovného spojenia „prevádzkovej služby CSIRT“ slovami „prevádzkovateľa základnej služby“ navrhované ustanovenie stráca zmysel. Úrad nepredpokladá, že NBÚ vydá identifikačné kritéria prevádzkovateľa základnej služby, ale že skôr vydá všeobecne záväzný predpis definujúci identifikačné kritéria prevádzkovej základnej služby. Úrad žiada navrhované znenie opraviť. Zároveň týmto odkazuje úrad aj na znenie § 18 zákona, ktoré upravuje „Identifikačné kritériá prevádzkovej služby“, nie „prevádzkovateľa základnej služby“. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.	O	A	
ÚJDSR	I. K vlastnému materiálu Čl. I: 25. K § 34 ods. 11: úrad predpokladá, že úmyslom predkladateľa je prechodné obdobie začínajúce dátumom 1. januárom 2021, a nie dátumom so spätnou platnosťou k 1. januáru 2020. Úrad žiada opraviť. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.	O	A	
ÚJDSR	I. K vlastnému materiálu Čl. I: 26. Všeobecne: doplniť, resp. vypustiť čiarky v súlade s pravidlami slovenského pravopisu. Odôvodnenie: legislatívno-technická pripomienka. Odporúčajúca pripomienka.	O	A	
ÚJDSR	II. K vlastnému materiálu Čl. V: 27. Doplniť účinnosť návrhu zákona, podľa Dôvodovej správy by	O	A	

	mala byť k 1. januáru 2021. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.			
ÚJDSR	III. K Doložke vybraných vplyvov a Analýze vplyvov na rozpočet verejnej správy, na zamestnanosť vo verejnej správe a financovanie návrhu: 28. K § 24 ods. 7: v prípade vybudovania automatizovaného spôsobu hlásenia kybernetických incidentov bude potrebné vyčleniť finančné prostriedky, čo v Doložke vybraných vplyvov a v Analýze vplyvov na rozpočet verejnej správy, na zamestnanosť vo verejnej správe a financovanie návrhu nie je vyhodnotené. ÚJD SR žiada o doplnenie oboch doložiek v zmysle navýšených finančných prostriedkov na vybudovanie tohto automatizovaného spôsobu hlásenia kybernetických incidentov a integráciu všetkých prevádzkovateľov základnej služby do tohto systému. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Pripomienka je zásadná.	Z	N	technické zabezpečenie je na náklady úradu
ÚJDSR	I. K vlastnému materiálu Čl. I: 3. K § 4 písm. b): na začiatku textu slová „Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky“ nahradiť slovami „Úrad podpredsedu vlády pre investície a informatizáciu“. Odôvodnenie: zosúladenie so súčasne platným textom zákona. Odporúčajúca pripomienka.	O	N	Novelou kompetenčného zákona došlo ku všeobecnej zmene názvu.
ÚJDSR	I. K vlastnému materiálu Čl. I: 4. K § 5 ods. 1 písm. w) – nad rámec návrhu zákona: úrad odporúča za slová „znalostné štandardy“ vložiť slová „a zverejňuje ich na svojom webovom sídle“. Odôvodnenie: vzhľadom na kompetenciu vydávania znalostných štandardov by bolo žiadúce definovať v	O	A	

	normatívnom predpise kde sú uvedené štandardy zverejnené. Odporúčajúca pripomienka.			
ÚJDSR	I. K vlastnému materiálu Čl. I: 5. K § 5 ods. 4: definovať o aké „orgány verejnej moci“ v oboch vetách odseku ide. Nakoľko v prípade prvej vety sú to zrejme iné ako „ústredné orgány“ a „iný orgán štátnej správy“ v zmysle § 4 písm. b) a c) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon“). Podľa predpokladu úradu ide o „iný orgán štátnej správy“. Úrad žiada opraviť. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.	O	A	Do DS, ide o iné orgány verejnej moci, ako sú ústredné orgány v zmysle zákona o KB
ÚJDSR	I. K vlastnému materiálu Čl. I: 6. K § 17 ods. 7: definovať pojem „hodnoverným spôsobom“. Odôvodnenie: používanie pojmov bez ich konkretizácie, resp. definovania môže v budúcnosti vyvolávať výkladové problémy pri ich aplikácii v praxi. Odporúčajúca pripomienka.	O	N	text vypustený
ÚJDSR	I. K vlastnému materiálu Čl. I: 7. K § 17 ods. 7, 8: konkretizovať o aký výmaz ide pri textoch „žiada o výmaz“ a „požiadať úrad o výmaz“. Iba z dôvodovej správy je zrejmé, že ide o výmaz prevádzkovateľa základnej služby z registra prevádzkovateľov základnej služby a výmaz základnej služby zo zoznamu základných služieb. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.	O	N	text vypustený
ÚJDSR	I. K vlastnému materiálu Čl. I: 8. K § 17 ods. 7, 8: podľa navrhovaného textu NBÚ bude vydávať	O	N	text vypustený

	rozhodnutie, ktorým rozhodne o výmaze do 30 dní. Uvedená rozhodovacia činnosť však nie je uvedená v § 5 ods. 1 písm. u) zákona. Úrad žiada doplniť tento typ rozhodnutia do § 5 ods. 1 písm. u) zákona. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.			
ÚJDSR	I. K vlastnému materiálu Čl. I: 9. K § 18 ods. 4: text ustanovenia nedáva zmysel. Úrad navrhuje text odseku upraviť nasledovne: „4) Ak prevádzkovateľ služby podľa prílohy č. 1 prekročí špecifické sektorové kritériá, ak sú určené, oznámi to úradu do 30 dní odo dňa prekročenia, v rozsahu podľa § 17 ods. 5 aj v prípade, ak neprekročí dopadové kritériá.“. Ak úrad nepochopil navrhované ustanovenie správne, žiada ustanovenie preformulovať tak, aby dávalo zmysel. Odôvodnenie: text odôvodnenia je súčasťou textu pripomienky. Odporúčajúca pripomienka.	O	N	text vypustený
UpREKaPŠ	k Čl. IV Návrh Čl. IV, ktorým sa dopĺňa zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov ustanovuje, že dohľad nad splnením navrhovanej povinnosti všetkých podnikov podľa osobitného predpisu, ktorým je § 20 zákona č. 69/2018 Z. z. by mal vykonávať Úrad pre reguláciu elektronických komunikácií a poštových služieb (ďalej len „úrad“). S ohľadom na navrhovanú úpravu taktiež poukazujeme na skutočnosť, že podľa § 19 ods. 1 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony „Prevádzkovateľ základnej služby je povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra	Z	A	

prevádzkovateľov základných služieb prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté.“. Za porušenie uvedeného ustanovenia Národný bezpečnostný úrad (ďalej len „NBÚ“) ukladá sankciu podľa § 31 ods. 2 písm. b) zákona č. 69/2018 Z. z. V tejto súvislosti poukazujeme na skutočnosť, že úrad za nesplnenie si povinnosti podniku podľa ustanovenia § 64 je po preukázaní správneho deliktu výkonom štátneho dohľadu podľa § 38 zákona č. 351/2011 Z. z. povinnosť uložiť sankciu podľa § 73 ods. 1 písm. a) „od 200 eur do 10 % z obratu“. Uvedené ustanovenia môžu spôsobiť kompetenčný spor, nakoľko sú v navrhovanej podobe duplicitné. Pokiaľ má úrad vykonávať dohľad v súvislosti s prijímaním bezpečnostných opatrení podľa zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov (ďalej len „ZEK“), je potrebné podniky ako subjekty povinnosti podľa § 19 ods. 1 zákona o KB z pôsobnosti zákona o KB vyňať v súvislosti s plnením povinnosti prijímať bezpečnostné opatrenia a zväžiť úpravu výšky sankcie, nakoľko všetky ostatné subjekty by boli sankcionované podľa inej sadzby sankcie. Úrad na základe vyššie uvedených skutočností trvá na zosúladení navrhovaných ustanovení uvedených zákonov. Úrad taktiež poukazuje na skutočnosť, že rozsah navrhovaných opatrení, ustanovených v navrhovanom § 20 ods. 3 a 4 (novelizračné body 27 a 28), ktoré by mal dodržiavať každý podnik presahuje rozsah kontrolovaných povinností súvisiacich so zabezpečením bezpečnosti a integrity sietí a služieb podľa zákona č. 351/2011 Z. z., v ktorom je implementovaný rozsah povinností v súlade s čl. 13a a 13b smernice EP a Rady č. 2002/21/ES o spoločnom regulačnom rámci. V tejto súvislosti úrad požaduje rozdelenie predmetného rozsahu dohľadovaných a			
---	--	--	--

	vynucovaných povinností podnikov v spolupráci s NBÚ.			
ÚPVSR	čl. I, bod 39 V odseku 5 písm. c) za slovami "v rozpore s § 27 ods. 1" odporúčame uviesť aj "písm. e)" z dôvodu precizovania vnútorného odkazu.	O	N	vzhľadom na vypustenie predmetného novelizačného bodu sa pripomienka stáva bezpredmetnou
ÚPVSR	čl. I, bod 7 V písmene u) odporúčame v slovnom spojení "s požiadavkami podľa zákona" uviesť nad slovom "zákona" odkaz na príslušnú poznámku pod čiarou a túto poznámku uviesť, prípadne iným spôsobom (napr. doplnením slova "tohto") určiť konkrétny zákon (zákony).	O	N	vypustením predmetného ustanovenia sa pripomienka stala bezpredmetnou
Verejnosť	V poznámke pod čiarou k odkazu 7 sa vypúšťa citácia: „zákon 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, zákon č. 351.2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.“. Ak sa novelou zákona vypúšťa ustanovenie, že zákon č.69/2019 sa nevzťahuje na osobitné predpisy, konkrétne na zákon č.166/2003, vznikne situácia, že akúkoľvek komunikáciu (upozorňujeme AKÚKOL'VEK - bez ohľadu na druh prenášaných informácií) bude predkladateľ zákona (NBÚ SR) môcť monitorovať, analyzovať a kontrolovať. V praxi to ale znamená, že z titulu zákona č.69/2018 bude možné odpočúvať nad rámec ochrany súkromia stanoveným zákonom č.166/2003. (Aj bez povolenia sudcu alebo prokurátora). Máme za to, že je to najhrubší zásah do ústavných práv občana na ochranu svojho súkromia. Navrhujeme, aby k odkazu 7 sa citácia	O	A	

	nevypustila.			
Verejnosť	§ 3 sa dopĺňa V § 3 sa za písmeno a) vkladá nové písmeno b), ktoré znie: „b) elektronickou komunikačnou sieťou prenosové systémy, prípadne prepájacie alebo smerovacie zariadenia a iné prostriedky, ktoré umožňujú prenos signálov po vedení, rádiovými vlnami, optickými alebo inými elektromagnetickými prostriedkami, vrátane družicových sietí, pevných sietí s prepájaním okruhov a s prepájaním paketov vrátane internetu, mobilných sietí a sietí káblovej televízie bez ohľadu na druh prenášaných informácií (ďalej len „sieť“),“. Definícia v tejto podobe vytvára predpoklad na hrubý zásah do súkromia. Uzákonením takejto definície by zákonodarca vytvoril právny rámec aj na monitoring hlasovej komunikácie (VoIP) ako aj monitoring sledovania kanálov káblovej televízie, čo predstavuje vážny zásah do ústavných práv na ochranu súkromia. Navrhujeme slová „bez ohľadu na druh prenášaných informácií“ vypustiť.	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
Verejnosť	k čl. I Navrhujeme vložiť do § 31 ods.1 nové písmeno h) v znení: h) nesplní povinnosť podať návrh podľa § 27c ods. 2 alebo koná v rozpore s rozhodnutím podľa § 27f ods. (1), (2) alebo (3) Odôvodnenie: Ustanovenie na uloženie sankcie poskytovateľovi základnej služby od 300 eur do až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok sa rozširuje o sankciu v prípade, ak nepodá návrh na posúdenie rizika dodávateľa pre národnú kybernetickú bezpečnosť alebo nevykoná rozhodnutie úradu v zmysle navrhnutého doplnenia § 27b až 27g.	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

Verejnosť	čl. I. Navrhujeme vložiť do § 31 ods.1 nové písmeno h) v znení: h) nesplní povinnosť podať návrh podľa § 27c ods. 2 alebo koná v rozpore s rozhodnutím podľa § 27f ods. (1), (2) alebo (3) Odôvodnenie: Ustanovenie na uloženie sankcie poskytovateľovi základnej služby od 300 eur do až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok sa rozširuje o sankciu v prípade, ak nepodá návrh na posúdenie rizika dodávateľa pre národnú kybernetickú bezpečnosť alebo nevykoná rozhodnutie úradu v zmysle návrhu na doplnenie §27b-27g	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
Verejnosť	K čl. I. Navrhujeme vložiť nové znenie § 34 ods. 1 v znení: „Úrad uloží pokutu od 300 eur až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok, poskytovateľovi digitálnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť podľa § 21 ods. 1, § 22 ods. 3, § 24 ods. 3, § 25 ods. 1 alebo ods. 2 alebo povinnosť vykonať reaktívne opatrenie na základe rozhodnutia úradu podľa § 27 ods. 5., podať návrh podľa § 27c ods. 2 alebo koná v rozpore s rozhodnutím podľa § 27f ods. (1), (2) alebo (3)“ Odôvodnenie: Ustanovenie na uloženie sankcie poskytovateľovi digitálnej služby od 300 eur do až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok sa rozširuje o sankciu v prípade, ak nepodá návrh na posúdenie rizika dodávateľa pre národnú kybernetickú bezpečnosť alebo nevykoná rozhodnutie úradu v zmysle navrhnutého doplnenia § 27b až 27g.	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
Verejnosť	k čl. I. Navrhujeme vložiť nové znenie § 34 ods. 1 v znení: „Úrad uloží pokutu od 300 eur až do výšky 1 % celkového ročného obratu za	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť

	predchádzajúci účtovný rok, poskytovateľovi digitálnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť podľa § 21 ods. 1, § 22 ods. 3, § 24 ods. 3, § 25 ods. 1 alebo ods. 2 alebo povinnosť vykonať reaktívne opatrenie na základe rozhodnutia úradu podľa § 27 ods. 5., podať návrh podľa § 27c ods. 2 alebo koná v rozpore s rozhodnutím podľa § 27f ods. (1), (2) alebo (3)“ Odôvodnenie: Ustanovenie na uloženie sankcie poskytovateľovi digitálnej služby od 300 eur do až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok sa rozširuje o sankciu v prípade, ak nepodá návrh na posúdenie rizika dodávateľa pre národnú kybernetickú bezpečnosť alebo nevykoná rozhodnutie úradu v zmysle navrhovaného doplnenia §27b-27g			návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
Verejnosť	V § 9 ods. 2 sa slová „zriaďuje a prevádzkuje akreditovanú jednotku CSIRT alebo na tento účel využíva akreditovanú jednotku CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, ak sa tak dohodnú. Využívanie akreditovanej jednotky CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, sa vykonáva na základe zmluvy“ nahrádzajú slovami „využíva Národnú jednotku CSIRT; to neplatí pre podsektor Obrana a podsektor Informačné systémy verejnej správy“. Predmetné ustanovenie navrhujeme v plnom rozsahu vypustiť. Návrh znenia odseku je v rozpore s povinnosťou ustanovenou §9 ods.1. Ústredný orgán nemôže zodpovedať za zabezpečenie kybernetickej bezpečnosti ak nemá zriadené pracovisko CSIRT. Taktiež nemôže byť zodpovedné za riešenie kybernetických bezpečnostných incidentov a nemôže vykonávať preventívne služby a reaktívne služby lebo na to nemá spôsobilosti. A z toho vyplýva aj to, že bez práva budovať spôsobilosti (zriaďovať CSIRT) ako to	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	predkladateľ navrhuje, žiadny ústredný orgán nemôže byť zodpovedný za sektor/podsektor definovaný v prílohe č.1 zákona a táto zodpovednosť by mala byť delegovaná zákonodarcom pre NBÚ.			
Verejnosť	Za § 27 sa vkladá § 27a, ktorý vrátane nadpisu znie: Ustanovenia navrhovaného §27a navrhujeme prepracovať v plnom znení. Z návrhu nie je zrejmé či predmetom blokovania môže byť len časti infraštruktúry poskytovateľa základnej služby a poskytovateľa digitálnej služby alebo aj ľubovoľná sieť prevádzkovaná fyzickými alebo právnickými osobami. Taktiež nie je žiadnym spôsobom definovaný pojem „škodlivá aktivita“, pričom máme za to že škodlivou aktivitou a môže rozumieť aj vytvorenie VPN pripojenia, ktoré pre CSIRT nie je „čitateľné“. Predkladateľovi navrhujeme tiež zadať rozsah okolností/podmienok, za ktorých môže byť blokovanie vykonané.	O	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
Verejnosť	Č.II §5 V §5 ods.1 pís. n) navrhujeme zmeniť na "akredituje jednotky CSIRT v pôsobnosti ústredných orgánov štátnej správy okrem Národnej jednotky CSIRT a vládnej jednotky CSIRT a zaraďuje ich do zoznamu akreditovaných jednotiek CSIRT," Súčasné znenie zabraňuje slobodnému výberu akreditačného partnera pre právnické osoby súkromného sektoru, ktoré sa rozhodli jednotku CSIRT vytvoriť a môže významným spôsobom zasahovať do ich práv. Akreditácia jednotky CSIRT sa riadi medzinárodným štandardom (Trusted Introducer).	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
Verejnosť	§ 24 sa dopĺňa odsekom 7, ktorý znie: „(7) Na hlásenie kybernetických bezpečnostných incidentov alebo na zaistenie kybernetickej bezpečnosti je prevádzkovateľ základnej služby	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť

	určený rozhodnutím úradu povinný zasielať automatizovaným spôsobom a v rozsahu ustanovenom v štandarde úradu určené systémové informácie zo sietí a informačných systémov.“. V návrhu ustanovenia odseku (7) navrhujeme vypustiť slová „automatizovaným spôsobom“. Ustanovenia §24 zákona č.69/2018 jednoznačne stanovujú spôsob a rozsah oznamovacej povinnosti. Preto automatizácia nahlasovania je absolútne neodôvodnená a zbytočná.			návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
Verejnosť	čl I. Vložiť do § 5 ods. 1 nové písmeno ae) v znení "ae) posudzuje riziko dodávateľa pre národnú kybernetickú bezpečnosť" Ako jeden z výstupov Odporúčania Komisie (EÚ) 2019/534 z 26. marca 2019 o kybernetickej bezpečnosti sietí 5G vznikol EÚ Toolbox pre ošetrovanie rizík v súvislosti s kybernetickou bezpečnosťou 5G sietí (Cybersecurity of 5G networks EU Toolbox of risk mitigating measures). Ten bol predstavený 29. januára 2020 ako sada nástrojov pre zvýšenie bezpečnosti ako aj adresovanie rizík uvedených v dokumente Posúdenie rizík. V súlade a v nadväznosti na dokument Posúdenie rizík, ide o ďalší dôležitý krok ku koordinovanému a efektívnemu zabezpečeniu bezpečnosti 5G sietí a technológií. Je dôležité, aby európsky ekosystém 5G zabezpečoval integritu, dôverynosť, zodpovednosť za správu a prevádzku, bezpečnosť, zameniteľnosť dodávok, interoperabilitu hardvérových a softvérových komponentov, spoločné technické a regulačné normy, kontinuitu služieb, spoľahlivosť toku údajov a ich ochranu, pokrytie vo všetkých oblastiach vrátane riedko osídlených oblastí a jasnosť komunikácie s používateľom ako aktívnym subjektom na digitálnom trhu. Dopĺňa sa právomoc Národného bezpečnostného úradu o	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	posudzovanie rizika dodávateľa pre národnú kybernetickú bezpečnosť.			
Verejnosť	K čl. I. Vložiť nové §§ 27b – 27g v znení: § 27b Konanie o posúdení rizika dodávateľa pre národnú kybernetickú bezpečnosť (1) Účelom konania o posúdení rizika dodávateľa pre národnú kybernetickú bezpečnosť (ďalej iba „konanie o posúdení rizika“) je určiť, či dodávateľ nepredstavuje riziko pre národnú kybernetickú bezpečnosť a ak je to dôvodné, zakázať použitie produktov, procesov alebo služieb dodávateľa. (2) Konanie je neverejné. (3) Účastníkom konania je : a) Ten kto podal návrh na začatie konania podľa § 27c b) dotknutý dodávateľ c) dotknutý prevádzkovateľ základnej služby alebo digitálnej služby (4) Na konanie o posúdení rizika sa nevzťahuje všeobecný predpis o správnom konaní xx) Odkaz pod čiarou: xx) Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov. § 27c Začatie konania o posúdení rizika (1) Úrad začne konanie bez návrhu na základe poznatkov získaných pri výkone svojej pôsobnosti podľa tohto zákona zákonom alebo osobitného predpisu. xxx) (2) Prevádzkovateľ základnej služby a prevádzkovateľ digitálnej služby je oprávnený používať len také kľúčové, kritické a citlivé súčasti (t.j. produkty, procesy alebo služby) u ktorých Úrad posúdil riziko dodávateľa pre národnú kybernetickú bezpečnosť. Konanie o posúdení rizika sa začne na návrh dodávateľa, prevádzkovateľa základnej služby alebo prevádzkovateľa digitálnej služby (ďalej len „navrhovateľ“). (3) Návrh na začatie konania o posúdení rizika podľa odseku 2 (ďalej len „návrh“) musí obsahovať a) Identifikáciu navrhovateľa b) identifikáciu dodávateľa produktov, procesov alebo	O	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

služieb dodávateľa c) oblasti možného využitia produktov, procesov alebo služieb dodávateľa v sektoroch podľa prílohy 1] d) ďalšie informácie a skutočnosti požadované vo vzore návrhu. (4) Úrad uverejní vzor návrhu na svojom webovom sídle. (5) Úrad môže návrh odložiť, ak a) Je návrh zjavne neopodstatnený, b) neobsahuje náležitosti podľa odseku 3 a navrhovateľ ho na výzvu úradu do 14 dní nedoplní (6) Ak návrh doručí úradu iná osoba ako dodávateľ alebo prevádzkovateľ základnej služby alebo prevádzkovateľ digitálnej služby, návrh sa považuje za podnet na začatie konania bez návrhu (ďalej len „podnet“). (7) Úrad podnet posúdi do 14 dní odo dňa doručenia podnetu úradu a ak podnet neodloží podľa odseku 5, začne konanie a vo veci rozhodne podľa § 27f. (8) O spôsobe vybavenia podnetu podľa odseku 7 úrad informuje podávateľa do 14 dní odo dňa doručenia podnetu úradu. (9) Úrad môže konanie zastaviť, ak navrhovateľ vzal návrh späť avšak len so súhlasom ostatných účastníkov konania. Xxx Odkaz na zákon o ochrane utajovaných skutočností a prípadne iné zákony 27d Hodnotenie rizika pre národnú kybernetickú bezpečnosť (1) Pri hodnotení rizika dodávateľa pre národnú kybernetickú bezpečnosť úrad berie do úvahy a. analýzu hrozieb pre národnú kybernetickú bezpečnosť b. medzinárodné záväzky Slovenskej republiky c. pravdepodobnosť, že dodávateľ, výrobca, dovozca alebo distribútor produktu, procesu alebo služby je ovládaný alebo pod vplyvom krajiny, ktorá nie je členom Európskeho spoločenstva alebo organizácia Severoatlantickej zmluvy (ďalej iba „cudzí štát“), pričom sa zohľadní najmä i. vzťah medzi dodávateľom výrobcou, dovozcom alebo distribútorom a cudzím štátom ii. vlastnícka štruktúra dodávateľa, výrobcu, dovozcu alebo distribútora iii. schopnosť cudzieho štátu zasahovať do podnikania dodávateľa, výrobcu,			
---	--	--	--

	dovozcu alebo distribútora iv. kontrola dodávateľa, výrobcu, dovozcu alebo distribútora nad výrobným procesom a procesom dodania v. riziká vyplývajúce z výrobného procesu a procesu dodania vi. právoplatné rozhodnutia úradu týkajúce sa toho istého dodávateľa vii. bezpečnostné opatrenia navrhnuté dodávateľom, výrobcom, dovozcom alebo distribútorom produktu d. legislatívu na ochranu osobných údajov cudzieho štátu e. stanoviská Slovenskej informačnej služby a Vojenského spravodajstva podľa odseku 2 (2) Úrad si pri posudzovaní rizika produktu pre národnú kybernetickú bezpečnosť vyžiada stanovisko Slovenskej informačnej služby a Vojenského spravodajstva, ktorí svoje stanovisko obsahujúce hodnotenie rizika dodávateľa, výrobcu, dovozcu alebo distribútora a produktu pre národnú kybernetickú bezpečnosť a národnú bezpečnosť zašlú úradu do 14 dní od doručenia žiadosti o stanovisko. Slovenská informačná služba a Vojenské spravodajstvo v stanovisku podľa predchádzajúcej vety prihliadajú na záujmy štátu v rozsahu svojej pôsobnosti. (3) Na základe žiadosti Úradu je dodávateľ, výrobca, dovozca alebo distribútor produktu, procesu alebo služby povinný v lehote 15 dní poskytnúť podklady pre hodnotenie rizika podľa odseku 1. (4) Úrad vyhodnotí riziko pre národnú kybernetickú bezpečnosť ako a. Vysoké, ak dodávateľ predstavuje z hľadiska národnej kybernetickej bezpečnosti závažnú hrozbu a takúto hrozbu nie je možné odstrániť prijatím bezpečnostných opatrení podľa § 20 alebo ak dodávateľ, výrobca, dovozca alebo distribútor produktu, procesu alebo služby neposkytne Úradu informácie podľa odseku 3. b. Stredné ak dodávateľ predstavuje z hľadiska národnej kybernetickej bezpečnosti závažnú hrozbu a takúto hrozbu je možné znížiť prijatím bezpečnostných opatrení podľa § 20 c. Nízke, ak dodávateľ			
--	--	--	--	--

	predstavuje z hľadiska národnej kybernetickej bezpečnosti nezávažnú hrozbu alebo d. Nezávažné, ak dodávateľ nepredstavuje z hľadiska národnej kybernetickej bezpečnosti hrozbu (5) Ak úrad určí, že dodávateľ produktu pre národnú kybernetickú bezpečnosť predstavuje stredné alebo nízke riziko, dodávateľ, výrobca, dovozca alebo distribútor môže požiadať úrad o schválenie bezpečnostných opatrení na zníženie hrozby. (6) Ak úrad schváli bezpečnostné opatrenie podľa odseku 4, opätovne vyhodnotí riziko podľa odseku 3. § 27e Lehoty Úrad rozhodne v konaní do 60 dní odo dňa začatia konania. V odôvodnených prípadoch úrad túto lehotu primerane predĺži, najviac však o 60 dní. O predĺžení lehoty úrad písomne informuje účastníkov konania. § 27f Rozhodnutia (1) Ak úrad vyhodnotí riziko dodávateľa pre národnú kybernetickú bezpečnosť ako vysoké, rozhodne o a) zákaze používať produkty, procesy alebo služby daného dodávateľa pri poskytovaní základných služieb a digitálnych služieb a o rozsahu základných služieb a digitálnych služieb, ktorých sa zákaz týka a b) povinnosti poskytovateľov základných služieb a digitálnych služieb odstrániť produkty používané pri poskytovaní základných služieb v rozsahu zákazu podľa písmena a) v primeranej lehote, najdlhšie do 5 rokov od právoplatnosti rozhodnutia o zákaze c) tom, že rozklad nemá odkladný účinok (2) Ak úrad vyhodnotí riziko dodávateľa pre národnú kybernetickú bezpečnosť ako stredné, rozhodne o a) zákaze používať produkt pri poskytovaní základných služieb a digitálnych služieb a o rozsahu základných služieb a digitálnych služieb, ktorých sa zákaz týka a b) možnosti poskytovateľov základných služieb a poskytovateľov digitálnych služieb ďalej používať produkty, procesy alebo služby v rozsahu zákazu podľa písmena a) pri poskytovaní základných služieb a digitálnych služieb v rozsahu v			
--	--	--	--	--

akom ich používali pred právoplatnosťou rozhodnutia o zákaze (3) V rozhodnutí úrad môže úrad rozhodnúť o povinnosti poskytovateľa základnej služby a poskytovateľa digitálnej služby vypracovať a predložiť úradu na schválenie v lehote dvoch mesiacov návrh harmonogramu odstránenia produktu, procesu alebo služby dodávateľa s vysokým stupňom rizika (ďalej len „harmonogram“). Úrad rozhodne o schválení návrhu harmonogramu do 15 dní od jeho doručenia. Ak harmonogram nebude úradu predložený v určenej lehote, úrad rozhodne o harmonograme do 15 dní od márneho uplynutia lehoty. (4) Rozhodnutia podľa odsekov 1 až 3 zverejňuje úrad na elektronickej úradnej tabuli úradu. Zverejnenie rozhodnutia na elektronickej úradnej tabuli nahrádza doručenie, zverejnenie alebo vyvesenie podľa osobitných predpisov. (5) Ak nie je podaný rozklad, alebo ak rozhodnutie vylučuje odkladný účinok podaného rozkladu, rozhodnutie nadobúda právoplatnosť 15. dňom od zverejnenia na elektronickej úradnej tabuli úradu. (6) Právoplatné rozhodnutie Úrad doručí orgánu, ktorý je príslušný na vydanie povolenia alebo licencie pre poskytovateľa základnej služby a poskytovateľa digitálnej služby. § 27g (1) Proti neprávoplatnému rozhodnutiu podľa § 27f možno podať rozklad, o ktorom rozhodne riaditeľ úradu. (2) Včas podaný rozklad má odkladný účinok, ak to rozhodnutie nevylučuje. (3) Podávateľ rozkladu môže rozšíriť podaný rozklad alebo doplniť podaný rozklad o ďalší návrh alebo o ďalšie body len v lehote určenej na podanie rozkladu. Cieľom predkladaného návrhu je posilniť legislatívnu úpravu v oblasti národnej kybernetickej bezpečnosti, pričom sa zameriava na posilnenie právomocí príslušných vnútroštátnych orgánov v zmysle EU Toolboxu. Predmetom návrhu je najmä zavedenie strategických opatrení v oblasti kybernetickej bezpečnosti implementáciou			
--	--	--	--

objektívneho konania o posúdenie rizika dodávateľa. Zavádza sa osobitné konanie o posúdení rizika dodávateľa pre národnú kybernetickú bezpečnosť s možnosťou zakázať rozhodnutím Národného bezpečnostného úradu používanie produktov, služieb a procesov rizikových dodávateľov, najmä pokiaľ sú tieto kľúčové, kritické alebo inak senzitivne, v rámci verejných telekomunikačných sietí. Do zákona sa vkladajú nové ustanovenia § 27b až 27g, ktoré upravujú osobitné konanie o posúdení rizika dodávateľa pre národnú kybernetickú bezpečnosť. Tieto ustanovenia zavádzajú zo zákona opatrenia z EÚ Toolbox pre ošetrenie rizík v súvislosti s národnou kybernetickou bezpečnosťou 5G sietí (Cybersecurity of 5G networks EU Toolbox of risk mitigating measures), tým, že zavádzajú opatrenia na minimalizáciu rizík súvisiacich s dodávateľmi a výrobcami. V §27b sa definuje účel konania o posúdení rizika dodávateľa pre národnú kybernetickú bezpečnosť. Neverejnosť je odôvodnená tým, že v rámci konania budú vyhodnocované informácie, ktorý zverejnenie by bolo v rozpore s oprávnenými záujmami účastníkov konania, prípadne ide o informácie v režime utajenia. Účastníkmi konania sú ten, kto podal návrh na jeho začatie, dotknutý dodávateľ a dotknutý prevádzkovateľ základnej služby alebo digitálnej služby. Vzhľadom na osobitný charakter konania sa navrhuje vylúčenie použitia všeobecného predpisu o správnom konaní. V § 27c sa upravuje začatie konania o posúdení rizika dodávateľa pre národnú kybernetickú bezpečnosť ex offo a na návrh. Úrad môže začať konanie kedykoľvek na základe poznatkov zo svojej činnosti. Tým sa zabezpečuje ex post kontrola v zmysle EÚ Toolboxu. Ukladá sa povinnosť prevádzkovateľa základnej služby a prevádzkovateľa digitálnej služby (t.j. aj telekomunikačných operátorov) používať len také kľúčové, kritické a citlivé súčasti u			
---	--	--	--

	ktorých Úrad vopred posúdil riziko dodávateľa pre národnú kybernetickú bezpečnosť. Táto požiadavka je odôvodnená pred ako aj cez nasadenie až po prevádzku kľúčových 5G komponentov za účelom minimalizácie rizík súvisiacich s dodávateľmi a výrobcami. Možnosť dodávateľa, prevádzkovateľa základnej služby alebo prevádzkovateľa digitálnej služby podať návrh na začatie konania sleduje vyššie uvedené ciele ako aj zavádza prevenciu závislosti na jednom dodávateľovi, umožňuje ex ante kontrolu kritických a senzitívnych častí a súčastí ako je to vyžadované v zmysle EÚ Toolboxu a súčasne umožňuje vstup nových dodávateľov a výrobcov do prostredia základných a digitálnych služieb. Vzor návrhu na začatie konania zverejní úrad na webovom sídle. Neopodstatnené alebo neúplné návrhy na začatie konania môže úrad odložiť. Neúplné návrhy môže úrad vyhodnotiť ako podnet a začať konanie bez návrhu. Ako podnet môže úrad vyhodnotiť aj návrh podaný neoprávnenou osobou, ak obsahuje relevantné údaje. Stanovuje sa 14 dňová lehota na vyhodnotenie podnetu, o spôsobe vybavenie úrad informuje podávateľa. Navrhovateľ môže návrh na začatie konania zobrať späť, avšak len so súhlasom ostatných účastníkov konania, čo umožňuje poskytovateľom základných a digitálnych služieb získať rozhodnutie o posúdení rizika výrobcu, ak keď by tento sám návrh na začatie konania zbral späť. V § 27d sa uvádzajú kritéria, podľa ktorých úrad hodnotí riziká. Tým je zabezpečená transparentnosť, objektívnosť a súlad s EÚ Toolboxom. Úrad si pri hodnotení rizika dodávateľa obligatórne vyžiada stanovisko Slovenskej informačnej služby a Vojenského spravodajstva, ktoré svoje stanovisko poskytnú do 15 dní. Stanovujú sa 4 stupne rizika – vysoké, stredné, nízke a nezávažne. Pri nízkom a strednom riziku môže dodávateľ, výrobca, dovozca alebo distribútor			
--	--	--	--	--

	môže požiadať úrad o schválenie bezpečnostných opatrení na zníženie identifikovaných hrozieb a následne úrad opätovne riziko vyhodnotí. V § 27e sa stanovuje lehota na rozhodnutie o posúdení rizika dodávateľa pre národnú kybernetickú bezpečnosť na 60 dní s možnosťou predĺženie o 60 dní na celkom 120 dní. V § 27f sa ustanovuje právomoc úradu rozhodnúť o zákaze používať produkty, procesy alebo služby dodávateľa považovaného za dodávateľa s vysokým a stredným rizikom pre národnú kybernetickú bezpečnosť pri poskytovaní základných služieb a digitálnych služieb. Úrad môže rozhodnúť o odstránení prvkov s vysokým stupňom rizika v lehote, ktoré nemôže byť dlhšia ako 5 rokov. Pri prvkoch so stredným stupňom rizika môže úrad rozhodnúť o možnosti používať takéto prvky v doterajšom rozsahu. Na odstránenie prvkov s vysokým rizikom môže úrad určiť lehotu na predloženie harmonogramu ich odstránenia na rozhodnutie o schválení. Pri nepredložení návrhu rozhodne o harmonograme úrad. Upravuje sa spôsob zverejnenia právoplatného rozhodnutia a lehota na podanie rozkladu. Právoplatné rozhodnutia sa doručujú aj orgánu (najmä telekomunikačný úrad), ktorý je príslušný na vydanie povolenia alebo licencie pre poskytovateľa základnej služby a poskytovateľa digitálnej služby, nakoľko ide o rozhodnutie, ktoré môže mať pre takých orgán význam pre posúdenie plnenia podmienok povolení alebo licencií. V § 27g sa upravuje opravný prostriedok – rozklad, možnosť doplnenia rozkladu a orgán príslušný na jeho vybavenie – riaditeľ úradu.			
Verejnosť	§ 5 sa dopĺňa odsekom 4 ktorý znie: „(4) Úrad je oprávnený požadovať od ústredných orgánov, prevádzkovateľov základnej služby, orgánov verejnej moci a právnických osôb poskytnutie	O	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť

	súčinnosti, alebo informácií, ktoré sú potrebné na plnenie úloh podľa tohto zákona. Orgány verejnej moci, prevádzkovatelia základnej služby a právnické osoby sú povinné úradu poskytnúť požadovanú súčinnosť, alebo informácie, ktoré sú potrebné na plnenie úloh podľa tohto zákona.“. Z návrhu znenia odseku 4 navrhujeme vypustiť slová „a právnické osoby“ nakoľko samotný zákon upravuje podľa ustanovení § 1 organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti a postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby. Inštitút „Právnickej osoby“ upravuje Občiansky zákonník.			návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
Verejnosť	V § 27 sa odsek 1 dopĺňa písmenom e), ktoré znie: „e) rozhodnutím zakázať alebo obmedziť prevádzkovateľovi základnej služby používať konkrétny produkt, proces alebo službu, ak je to potrebné na zaistenie kybernetickej bezpečnosti, alebo z dôvodov bezpečnostného záujmu Slovenskej republiky.“. Zákonodarcu môže legislatívnou úpravou definovať požiadavky na funkčné, výkonnostné alebo bezpečnostné parametre pre produkty používané na území SR. Navrhovaná právna úprava však hrubým spôsobom zasahuje do kompetencie poskytovateľa základnej služby, pričom nesie značné príznaky diskriminácie. Taktiež absentuje príčinná súvislosť potreby takéhoto vážneho obmedzenia práv poskytovateľa základnej služby. Na základe týchto skutočností navrhujeme vyššie uvedený návrh vypustiť v plnom rozsahu.	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
Verejnosť	ČI.I Žiadame dôsledne implementovať Európsky toolbox kybernetickej bezpečnosti 5G sietí (https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-	O	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k

	mitigating-measures). Obzvlášť doplniť návrh zákona o rozmer hybridných hrozieb či politických rizík, ktoré by prevádzkovatelia základných služieb pri vyhodnocovaní rizikovosti využívania konkrétného produktu, služby či procesu boli povinní zohľadňovať. Odôvodnenie: Slovenská republika je spolu s ďalšími členskými štátmi EÚ povinná implementovať požiadavky Európskeho toolboxu kybernetickej bezpečnosti 5G sietí do vnútroštátnej právnej úpravy. Vzhľadom na povahu a obsah tohto dokumentu sme presvedčení o tom, že jeho požiadavky by mali byť implementované práve do zákona o kybernetickej bezpečnosti ako jediného právneho predpisu svojho druhu, ktorý vo všeobecnej rovine a celoplošne naprieč všetkými sektormi a podsektormi ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti, a teda aj požiadavky na zaistenie bezpečnosti pre sektor Elektronické komunikácie, podsektor siete a služby pevných a mobilných elektronických komunikácií, kam patrí aj nová sieť piatej generácie. Účelom Európskeho toolboxu je najmä stanovenie spoločného súboru opatrení, ktoré sú schopné zmierniť hlavné riziká kybernetickej bezpečnosti sietí 5G, ktoré boli identifikované v rámci EU coordinated risk assessment report (za Slovenskú republiku dával príspevok v podobe analýzy rizík práve úrad) a poskytnúť usmernenie pre výber opatrení, ktoré by mali mať prioritu. Európsky toolbox teda identifikuje opatrenia, ktoré sú štáty vrátane Slovenskej republiky povinné implementovať do svojich vnútroštátnych poriadkov, pričom tieto opatrenia sa delia na strategické a technické a tzv. podporné činnosti. Práve tzv. strategické opatrenia sú oblasťou, na ktorú zákon žiadnym spôsobom nereflektuje, nakoľko mu nie sú známe pojmy ako politické riziká, riziká spojené s vplyvmi tretích štátov na dodávateľov, hybridné hrozby a pod..		ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
--	---	--	---

	Obmedzuje sa len na hrozby, zraniteľnosti a riziká technického charakteru. Preto považujeme za vysoko prioritné doplniť zákon o nový rozmer tzv. hybridných hrozieb, politických rizík, ktoré by prevádzkovatelia základných služieb pri vyhodnocovaní rizikovosti využívania konkrétného produktu, služby či procesu boli povinní zohľadňovať. Uvedený model by kopíroval postup iných štátov implementujúcich Európsky toolbox, ako napríklad Poľsko alebo Francúzsko. Takto by bolo možné upustiť od zavádzania prvoplánových kompetencií na strane úradu – tie síce vo forme ako „zakázať využívať konkrétny produkt, službu, proces“ alebo „blokovat“, alebo „povinný presun informácií z prevádzky“ môžu plniť túto implementačnú úlohu, vyznačujú sa však vysokou rizikovosťou, zneužívateľnosťou, netransparentnosťou, nepredvídateľnosťou a nepreskúmateľnosťou. Navrhujeme tiež do procesu medzirezortného pripomienkového konania vložiť aj návrh sektorovej vyhlášky (vydanej podľa § 32 ods. 2 zákona o kybernetickej bezpečnosti), keďže by mala riešiť ďalší proces vyhodnocovania rizík / rizikovosti na strane dodávateľov a je s návrhom zákona úzko prepojená.			
ZBOP SR	definícia subjektov cloud computingu Pri súčasnom návrhu novely zákona o kybernetickej bezpečnosti je definovaný v oblasti cloud computingu subjekt "Poskytovateľ digitálnej služby". V cloud computing terminológii sú subjekty na strane dodávateľa rozdelené na: - Prevádzkovateľ cloudových služieb - predstavuje organizáciu ktorá disponuje s infraštruktúrou a prevádzkuje danú cloud službu (napr. Amazon AWS, Microsoft Azure, Google cloud a pod.) - Poskytovateľ cloudových služieb - predstavuje organizáciu ktorá zabezpečuje predaj cloud služieb	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	a/alebo implementáciu cloud služieb a/alebo správu/prevádzku cloud služieb. Nakoľko Poskytovateľ cloudových služieb nemá dosah na technologickú a IT infraštruktúru cloudových služieb, tak nevie zabezpečiť kontrolu dodržiavania pravidiel vyplývajúcich z certifikácie. Sme toho názoru že aj pravidlá certifikácie musia byť rozdielne pre jednotlivé subjekty, resp. certifikácia by sa mala vzťahovať prioritne len na Prevádzkovateľa cloudových služieb. Na základe uvedených informácií odporúčame v rámci novely jasne zdefinovať subjekty cloud computingu a najmä vyšpecifikovanie definície a zodpovedností Prevádzkovateľa a Poskytovateľa cloudových služieb.			
ZBOP SR	doplnenie 50. V doplnení č. 50 vypustiť alebo jednoznačne definovať kritériá doplnených služieb, na základe ktorých majú byť zaradené medzi základné služby. Napríklad „prevádzkovateľ obchodu na internete s možnosťou vyhľadávania, objednávanie a nákupu tovarov a služieb“ je prevádzkovateľ každého webshopu, bez ohľadu na obrat webshopu, počet zamestnancov alebo dopadu na štát. prevádzkovateľa internetového obchodu navrhujeme zaradiť ako prevádzkovateľa digitálnej služby. Dôvod: Definícia "prevádzkovateľa obchodu na internete" neuvažuje o rozsahu dopadu kybernetickej bezpečnosti. 50. V prílohe č. 1 v sektore „3. Digitálna infraštruktúra“ sa v stĺpci „Prevádzkovateľ služieb“ vkladajú tri nové riadky, ktorý znejú: „poskytovateľ dátových, hlasových a internetových služieb – služieb pripojenia do internetu“, „poskytovateľ služieb webhostingu, DNS hostingu alebo mailhostingu“.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

ZBOP SR	definícia cloudových služieb V oblasti cloudových služieb sú v platnom zákone č.69 a návrhu novely zákona č.69 uvedené nasledovné definície: - Návrh novely zákona, bod 50. príloha č.1, - časť 3. Digitálna infraštruktúra je rozšírená o „prevádzkovateľ obchodu na internete s možnosťou vyhľadávania, objednávaní a nákupu tovarov a služieb“, „poskytovateľ služieb webhostingu, DNS hostingu alebo mailhostingu“. - V prílohe č.2 zákona č.69 o kybernetickej bezpečnosti sú služby v oblasti cloud computingu definované nasledovne: " digitálna služba, ktorá umožňuje prístup ku škálovateľnému a pružnému súboru počítačových zdrojov, ktoré možno zdieľať." Dávame do pozornosti, že v súčasnosti cloudové služby obsahujú nasledovné typy služieb: - IaaS služby - poskytovanie výpočtového výkonu, diskového úložiska, sieťovej infraštruktúry a ďalších infraštruktúrnych služieb - PaaS služby - poskytovanie databázových služieb, web služieb, kontajnerových platforiem a ďalších platformových služieb - SaaS služby - poskytovanie CRM, ERP, email, DMS a ďalších softvérových služieb. Súčasné definície cloudových služieb v zákone č.69 a novele zákona č.69 sú nedostatočné a sú zamerané hlavne na IaaS služby a čiastočne na PaaS služby. Odporúčame rozšíriť definíciu, tak aby cloudové služby reprezentovali služby z oblasti IaaS, PaaS a SaaS.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
ZBOP SR	certifikačné procesy V súčasnosti je platné metodické usmernenie MIRRI (Ministerstvo investícií, regionálneho rozvoja a informatizácie SR) v oblasti certifikácie cloudových služieb (viď. https://www.mirri.gov.sk/sekcie/certifikacia-a-zapis-sluzieb-	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text

	vladneho-cloudu/index.html), ktoré ukladá povinnosť podnikateľom poskytujúcim cloudové služby pre verejnú a štátnu správu certifikovať jednotlivé cloudové služby. Certifikácia je rozdelená na základe bezpečnostných požiadaviek pre uchovávané a spracovávané dáta, pričom bezpečnostné požiadavky sú analyzované a posudzované osobitne z hľadiska dôvernosti, integrity a dostupnosti spracovávaných a uchovávaných dát. Novela zákona č.69 zvyšuje administratívne zaťaženie podnikateľov, nakoľko už v súčasnosti musia cloudové služby certifikovať prostredníctvom MIRRI a zavedením novely zákona č.69 by museli certifikáciu realizovať aj prostredníctvom Národného Bezpečnostného úradu (NBÚ). Odporúčame zosúladiť oba certifikačné procesy, za účelom eliminácie duplicitných požiadaviek v rámci certifikačného procesu.			tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
ZBOP SR	§3 bod k Zákon 69/2018, §3, bod k navrhujeme jednoznačne doplniť, že sa jedná o základnú službu, ktorá je kombináciou bodu k1 a k2, alebo k1 a k3. Dôvod: Nie sú jasne definované identifikačné kritériá k) základnou službou služba, ktorá je zaradená v zozname základných služieb a 1. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1, a 2. je informačným systémom verejnej správy,8) alebo 3. je prvkom kritickej infraštruktúry,9)	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
ZPW	bodu 35 Definičná formulácia „ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby” je zmätočná a jej účel je nezrozumiteľný – zamestnanec právnickej osoby je tiež vždy fyzická osoba, vo vzťahu k vykonaniu auditu však prevádzkovateľ neuzatvára právny vzťah so zamestnancom, ale s	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a

	danou právnickou osobou. Takisto nie je zrejmé, prečo sú špecificky vytiahnuté niektoré typy osôb ako spoločník či štatutárny orgán, ale absentuje napr. fyzická osoba – podnikateľ, čo nie je inštitút totožný s fyzickou osobou a podobne. Túto časť odporúčame vypustiť.			odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
ZPW	 bodu 10, písm. y) Doplnenie novej právomoci pre NBÚ podľa navrhovaného písm. y) v § 5 ods. 1 zákona je narušením trojdelenia moci a zásahom do právomocí zverených súdom Slovenskej republiky. Posúdiť, čo je alebo nie je „škodlivý obsah“ alebo „škodlivá aktivita“ môže byť v právnom poriadku Slovenskej republiky zverené len nezávislým a nestranným súdom Slovenskej republiky. Per analogiam iuris poukazujeme na zákonný mechanizmus „zamedzenia prístupu k webovému sídlu, prostredníctvom ktorého sa poskytuje zakázaná ponuka“ v zmysle ustanovenia § 15b ods. 7 až 14 zákona č. 171/2005 Z. z. O hazardných hrách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. I v tomto prípade je právomoc vydať takýto zákonný príkaz zverená súdom Slovenskej republiky. Podľa odkazovaného (10aa) pripravovaného zákona č. .../2020 Z. z. o dohľade v oblasti ochrany spotrebiteľa a rozhodnutie o blokovaní vydáva súd, čo zaručuje primerané vecné preskúmanie aj právnu ochranu, zatiaľ čo úrad nie je orgánom kompetentným pre riešenie otázok ochrany spotrebiteľa a nie je teda dôvodné, aby mu bola zverená právomoci podľa odkazovaného predpisu, uvedené prepojenie na nepríslušnú legislatívu je preto potrebné odstrániť. Takisto vôbec nie je zrejmé ako by mal úrad zabezpečovať vykonanie naznačované v tomto ustanovení, keďže spravidla ide o služby, činnosti a majetok patriace tretím stranám a nie úradu, čo bez ďalšieho spresnenia takisto nie je možné akceptovať.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

ZPW	 bodu 7 Návrh výrazne nesprávne pracuje s terminológiou, nakoľko • zavádza priame definície všeobecných pojmov v reštriktívnom výklade právneho pojmu (produkt, služba, proces) • zbytočne zavádza disharmonizáciu s pojmami už bežne zavedenými a dlhodobo používanými inou legislatívou (služba: zákon č. 136/2010 Z. z. o službách na vnútornom trhu, zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu, zákon č. 222/2004 Z. z. o dani z pridanej hodnoty, produkt: zákon č. 37/2007 o veterinárnej starostlivosti, zákon č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach, proces: zákon č. 162/2015 Z. z. Správny súdny poriadok, zákon č. 254/2008 Z. z. Školský zákon atď.), vrátane samotného tohto zákona („ropa a ropné produkty“ v prílohe č. 1), a to aj s nesprávnou vecnou definíciou, čím spôsobuje problematické výklady a možnosť kolízií pri aplikácii požiadaviek zákonov, čo je stav, ktorý by mal byť v slovenskej legislatíve neprípustný – použitie „na účely tohto zákona“ uvedené z dopadového hľadiska nijako nezmení. Pre použitie v tomto zákone odporúčame zaviesť prívlastky.	O	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
ZPW	 body 19 a 22 Navrhovaná zmena má vážny negatívny dopad na praktickú vykonateľnosť, pretože dotknutý prevádzkovateľ služby nemôže konať, keď o tom, nevie, zatiaľ čo k prekročeniu už mohlo objektívne prísť. Tieto body odporúčame vypustiť.	O	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

ZPW	 bodu 25 Navrhované nové znenie !19 ods. 6 písm. e) má opäť negatívny dopad, pretože prevádzkovateľ nemá právomoc a ani odbornú znalosť či možnosť analýzy na identifikáciu a určovanie čo je trestný čin. Navyše nie je zrejmé akým spôsobom by ho mal oznamovať, nakoľko od bežného súkromného subjektu nie je možné očakávať, že bude podávať a odôvodňovať celé trestné oznámenie.. Formulácia „že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka“ je takisto v celkovom kontexte identifikácie incidentu a príslušnej notifikácie nezrozumiteľný, pretože bezpečnostný incident je buď spôsobom alebo nástrojom na spáchanie trestného činu, t.j. trestný čin je dôsledok, ale nejde tu o „týkanie sa“. Odborne posúdiť a zhodnotiť, či skutočnosti nasvedčujú spáchaniu trestného činu, by mal Úrad, resp. SK-CERT na základe oznámenia prevádzkovateľa základnej služby, resp. Poskytovateľa digitálnej služby o vzniku bezpečnostného incidentu. Uvedené znenie je preto potrebné preformulovať, aby bolo vykonateľné a nezaďávalo neprimeranú povinnosť.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
ZPW	 bodu 24 Navrhované znenie odseku 2 je nutné doplniť, nakoľko zavádza povinnosť uzatvoriť zmluvu v súvislosti s akýmkoľvek sieťami a informačnými systémami prevádzkovateľa základnej služby a nie iba tými, ktoré sú nutné pre poskytovanie základnej služby. Uvedený problém sa nachádza už aj v pôvodnom znení, čím presahuje rámec pôvodného zámeru a snaží sa regulovať aktíva, ktoré nie sú predmetom tohto zákona.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

ZPW	bodu 33 Obdobne ako bod 32, uvedené ustanovenie § 27a zavádza nad rámec predmetu tohto zákona extrémne široko definovanú kompetenciu zásahov do fungovania a činnosti ľubovoľných subjektov, a to dokonca subjektov, ktoré ani nie sú predmetom tohto zákona (tzv. nedefinovaný pojem „prevádzkovateľ infraštruktúry“). Doplnenie novej právomoci pre NBÚ podľa navrhovaného ustanovenia § 27a zákona je narušením trojdelenia moci a zásahom do právomocí zverených súdom Slovenskej republiky. Posúdiť, čo je alebo nie je „škodlivý obsah“ alebo „škodlivá aktivita“ môže byť v právnom poriadku Slovenskej republiky zverené len nezávislým a nestranným súdom Slovenskej republiky. Takáto právomoc nemôže byť zverená orgánom výkonnej moci. Už vôbec nie ústrednému orgánu štátnej správy s politickým obsadením riadiacich funkcií. Podľa nášho názoru je navrhované znenie § 27a zákona v rozpore s Ústavou Slovenskej republiky (najmä čl. 46 ods. 2 Ústavy SR). Per analogiam iuris poukazujeme na zákonný mechanizmus „zamedzenia prístupu k webovému sídlu, prostredníctvom ktorého sa poskytuje zakázaná ponuka“ v zmysle ustanovenia § 15b ods. 7 až 14 zákona č. 171/2005 Z. z. O hazardných hrách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. I v tomto prípade je právomoc vydať takýto zákonný príkaz zverená súdom Slovenskej republiky. Ods. 5 uvádza pravidlá blokovania, ktoré však nie sú na rozdiel napr. od odkazovaného návrhu zákona č. .../2020 Z. z. o dohľade v oblasti ochrany spotrebiteľa v návrhu pre posúdenie dopadu k dispozícii, v skutočnosti tak dotknuté ustanovenie ponecháva plnú svojvôľu určiť akékoľvek opatrenie nezávisle od jeho vykonateľnosti a dopadu na subjekt, ktorý ho má vykonať, a takisto nezávisle od možností a časovej, vecnej či právnej	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
-----	---	---	----	---

	realizovateľnosti na strane daného subjektu a takisto zaväzuje k súčinnosti ďalšie subjekty, vrátane orgánov verejnej moci, vykonať niečo, čo nemusí byť z ich strany vykonateľné. Ods. 6 neumožňuje žiadnu právnu ochranu, čím navrhuje dať úradu vyššie právomoci ako majú súdy Slovenskej republiky alebo Policajný zbor, čo nie je pri takto vágnej právomoci súladné so základnými princípmi právneho štátu. Navyše odsek 7 neponecháva dotknutému subjektu vykonať úkon podľa zvyklosti, štandardných postupov a bežného práva, ale snaží sa mu priamo nadiktovať čo a ako má urobiť, opäť nezávisle od jeho technických, ľudských či iných možností, diskusie a analýzy dopadov. Takisto nie je zrejmé, ako chce úrad vykonať v štandardných právnych podmienkach blokovanie na aktívach a majetku tretej strany. Náklady na vykonanie blokovania podľa znenia návrhu v akejkoľvek situácii v plnom rozsahu znáša dotknutý subjekt, čo nie je možné napr. ani pri postupoch podľa GDPR, pričom v prípade, že je rozhodnutie priamo zo strany úradu, tento neprevezme ani len zodpovednosť za škodu, ktorá môže vyplývať z jeho rozhodnutia, t.j. dopad a riziko na strane subjektu, ktorý má vykonať blokovanie sú ešte vyššie. Uvedené ustanovenie je nutné bezpodmienečne vypustiť v celom rozsahu alebo zásadne prepracovať.			
ZPW	bod 45 Písmeno h) je nutné vypustiť a ustanovenie s tak závažným dopadom je v prípade ponechania právomoci blokovania potrebné zdefinovať priamo v zákone. Vo vzťahu k navrhovanému zneniu § 32 ods. 1 písm. h) poukazujeme na pripomienku k bodu 11 návrhu novely zákona.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej

				akceptovateľnej miere pripomienky všetkých subjektov.
ZPW	 bodu 28 Uvedené má zásadný finančný a funkčný dopad na prevádzkovateľa základnej služby, pretože mu nad rámec zákonných medzí ukladá povinnosť zamestnať konkrétnu osobu so zásahom do jeho organizačnej štruktúry nezávisle od možností a počtu zamestnancov prevádzkovateľa základnej služby a navyše nepriamo vyžaduje povinnú certifikáciu takejto osoby. Uvedené ustanovenie je nutné vypustiť alebo preformulovať do podoby, ktorá nemá takýto vážny dopad. Navyše zákon nedôvodne a neprimerane zasahuje do vnútornej organizačnej štruktúry, vzťahov nadriadenosti a podriadenosti subjektu súkromného práva – podnikateľa.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
ZPW	 bodu 11 Uvedené oprávnenie NBÚ a povinnosť subjektov je príliš vágne a výklad môže byť veľmi široký, je preto nutné doplniť v akej veci a v akom rozsahu majú jednotlivé subjekty poskytovať súčinnosť, nakoľko uvedené ustanovenie umožňuje požadovať súčinnosť v ľubovoľnom plnení zákona úradom, napr. aj ktoréhokoľvek prevádzkovateľa základnej služby pri posudzovaní zhody zo strany úradu voči úplne inému subjektu. Uložená povinnosť pritom naráža najmä na štátom ustanovenú alebo uloženú povinnosť mlčanlivosti, ďalej daňové tajomstvo, telekomunikačné tajomstvo, prípadne iné chránené skutočnosti podľa zákona. Mechanizmus poskytovania týchto údajov a informácií je regulovaný osobitnými právnymi predpismi, najmä: a) zákon č. 301/2005 Z. z. Trestný poriadok (najmä § 90, § 115, § 116) b) zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) (§ 4 a 5), c) zákon č. 351/2011 Z. z. O elektronických komunikáciách (§ 63). Poskytovanie súčinnosti a „chránených informácií“ (v zmysle vyššie uvedeného) Národnému bezpečnostnému úradu aj v týchto prípadoch treba podriaďiť pravidlám a postupom, definovaným vyššie citovanými právnymi predpismi. NBÚ nemôže mať ako orgán výkonnej moci v systéme verejnej moci osobitné a výlučné postavenie a právomoci.			
ZPW	bodu 31 Uvedené ustanovenie ide úplne nad rámec ohlasovania incidentov a snaží sa neregulovaným spôsobom získavať neznámy rozsah informácií, ktoré môžu byť aj predmetom inej zákonnej ochrany a núti prevádzkovateľa programovo vytvárať nejaké aplikačné riešenia k tejto osobitnej oznamovacej povinnosti, ku ktorým nemusí mať ani prostriedky, ani schopnosť ich urobiť, pričom úrad si môže svojvoľne určiť ľubovoľného prevádzkovateľa základnej služby. Celé ustanovenie je nutné vypustiť, k osobitným spôsobom ohlasovania je postačujúci § 24 odsek 6.	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
ZPW	bodu 29 Uvedené ustanovenie nie je zrozumiteľné, ani vykonateľné – prečo sa má uzatvárať táto zbytočná vzájomná zmluva, keď prevádzkovateľovi základnej služby aj poskytovateľovi digitálnej služby vyplýva notifikačná povinnosť aj ostatné povinnosti priamo z tohto zákona a navyše prevádzkovateľ základnej služby ju nemá uzatvárať v opačnom vzťahu už podľa bodu 24 samotného tohto návrhu. V praxi to znamená, že každý poskytovateľ digitálnej služby môže vyžadovať od prevádzkovateľa základnej služby zmluvu s inými podmienkami, keďže zmluva je dvojstranný právny akt,	Z	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	pričom prevádzkovateľ poskytuje základnú službu všetkým rovnako, a takáto zákonná povinnosť má zásadný dopad vo všetkých aspektoch vzájomného vzťahu týchto subjektov a narušuje riadne poskytovanie základnej služby za riadnych podmienok. Uvedené znenie je nutné zosúladiť s princípmi obdobného znenia v § 19, pričom totožný problém je už v aktuálne platnom znení.			
ZPW	 bodu 32 Uvedené ustanovenie porušuje základné princípy právneho štátu, pretože bez akejkoľvek možnosti právnej ochrany, vzájomnej komunikácie, analýzy dopadu a prevzatia zodpovednosti navrhuje vykonať zásah do fungovania a činnosti prevádzkovateľa základnej služby takým spôsobom, ktorý môže zásadne porušiť iné právne záväzky a podmienky pre fungovanie a činnosť prevádzkovateľa základnej služby, a to dokonca v ľubovoľnej lehote a v neobmedzenom rozsahu aj nad rámec toho, čo sa týka jeho pozície prevádzkovateľa základnej služby. Takisto to neprimerane zasahuje do podmienok podnikateľského prostredia na strane výrobcov produktov, pričom kritériá k iniciácii takéhoto zákazu návrh v princípe nedefinuje – odôvodnenie použité v znení je extrémne široké a umožňuje prakticky čokoľvek. Uvedené ustanovenie je nutné vypustiť v celom rozsahu.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
ZPW	 bodu 3 V súvislosti so zmenou odkazu pod čiarou k odkazu 7 považujeme za potrebné uviesť, že už samotné platné znenie zákon v § 2 ods. 2 písmeno f) je právne nezmyselné a v rozpore s legislatívno-technickými pravidlami tvorby právnych predpisov. Hypotéza a dispozícia predmetnej právnej normy totiž znie: „Tento zákon sa nevzťahuje na.... f) osobitné predpisy.“. Špecialita všeobecne	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej

	záväzného právneho predpisu k inému právnenému predpisu (lex generalis) sa spravidla legislatívno-technicky vyjadruje inak, napr. „ak osobitný/všeobecný predpis neustanovuje inak“. Pri aktuálnej novelizácii zákona tak navrhujeme odstrániť aj tento právny nezmysel. Navyše, z Dôvodovej správy vôbec nie je zrejmé, prečo sa odstraňuje odkaz na zákon č. 166/2003 Z.z. a zákon č. 351/2011 Z. z.. Odôvodnenie v Dôvodovej správe je tak nepravdivé a zavádzajúce.			akceptovateľnej miere pripomienky všetkých subjektov.
ZPW	 bodu 36 V uvedenom ustanovení nie je zrejmé o akú právnickú osobu má ísť, zákon pracuje s iným označením subjektov a navyše prvá a posledná veta pôsobia vo vzájomnom kontexte veľmi zmätočne. Odporúčame upraviť. V odseku sa aj zbytočne miešajú viaceré nezávislé aspekty – ako sa zabezpečuje audit a jeho podmienky a možnosti na strane audítora – odporúčame rozdeliť na samostatné odseky.	O	N	
ZPW	 bodu 39 Vo vzťahu k navrhovanému zneniu § 31 ods. 5 písm. a) poukazujeme na pripomienku k bodu 11 návrhu novely zákona. Navrhujeme vypustiť.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
ZPW	 bodu 27 Zákon pozná a pracuje iba s pojmom kybernetická bezpečnosť, nie je preto zrejmé prečo návrh obsahuje aj pojem informačná	O	N	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť

	bezpečnosť a čo má tento pojem na rozdiel od kybernetickej bezpečnosti znamenať – presah do spravovania informácií mimo digitálneho priestoru nie je pôsobnosti tohto zákona.			návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
ZPW	bod 44 Zákonné podmienky s tak závažným dopadom na činnosť prevádzkovateľa základnej služby, akými sú pravidlá auditu kybernetickej bezpečnosti, časový rozsah a periodicita vykonávania auditu kybernetickej bezpečnosti nemožno stanoviť vykonávacím predpisom, ale je nutné ich zadefinovať priamo v tomto zákone. Podzákonnou právnou normou nemožno ukladať subjektom povinnosti.	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.
ZPW	bod 50 Znenie zavádza neznámy pojem “DNS hosting” a “mailhosting”, pričom poskytovatelia služieb systému doménových mien na internete sú už v prílohe č. 1 zahrnutí aj v platnom znení. Uvedené znenie je nutné spresniť, resp. odstrániť duplicity. Elektronický obchod ako taký nemožno považovať za základnú službu, navyše zahrnutie poskytovateľa akéhokoľvek malého elektronického obchodu do podmienok takejto striktnej regulácie je zásadne neprimerané a preto je potrebné ho vypustiť. Zároveň sa týmto zavádza neadekvátna nepriama regulácia subjektov už regulovaných napr. zákonom č. 22/2004 Z. z. o elektronickom obchode a ďalšími predpismi, ako napr. tými z oblasti zdravotníctva či bankovníctva, ktoré takisto definične spĺňajú navrhované znenie a zároveň sú	Z	ČA	Ďakujeme za zaslanie pripomienok, úrad berie na vedomie všetky námety, postrehy a komentáre. Relevantnosť návrhov úrad vyhodnotil vo vzťahu k ostatným pripomienkam a upravil text tak, aby bol jasný, transparentný a odzrkadľoval v najširšie možnej akceptovateľnej miere pripomienky všetkých subjektov.

	krížovo zahrnuté aj pod inými sektormi podľa tejto prílohy. Túto časť je nutné vypustiť.			
--	--	--	--	--