Pozmeňujúci a doplňujúci návrh
poslancov Národnej rady Slovenskej republiky
Juraja KRÚPU, Milana VETRÁKA a Milana LAURENČÍKA
k vládnemu 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
(tlač 441)

Vládny návrh 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, sa mení a dopĺňa takto:

1. **V čl. I bod 12 znie:**

„12. V § 5 sa odsek 1 dopĺňa písmenami y) až af), ktoré znejú:

„y) je vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti a orgánom posudzovania zhody podľa osobitného predpisu[10aa)],
z) plní úlohy kompetenčného a odvetvového centra podľa osobitného predpisu[10ab)],
aa) odníma certifikát kybernetickej bezpečnosti,
ab) v rámci systému certifikácie kybernetickej bezpečnosti vydáva bezpečnostné štandardy, certifikačné schémy a postupy,
ac) plní úlohy ústredného orgánu podľa prílohy č. 1,
ad) vedie a zverejňuje na svojom webovom sídle zoznam orgánov posudzovania zhody v systéme certifikácie kybernetickej bezpečnosti, zoznam certifikačných orgánov audítorov kybernetickej bezpečnosti a zoznam právnických osôb, prostredníctvom ktorých je možné realizovať audity kybernetickej bezpečnosti,
ae) posudzuje bezpečnostné riziká dodávateľa na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby (ďalej len „tretia strana“) pre kybernetickú bezpečnosť Slovenskej republiky a správu o tomto posúdení predkladá Bezpečnostnej rade Slovenskej republiky,
af) predkladá príslušnému osobitnému kontrolnému výboru Národnej rady Slovenskej republiky každoročne správu o dodržiavaní noriem týkajúcich sa ochrany telekomunikačného tajomstva a osobných údajov občanov Slovenskej republiky.“.

Poznámky pod čiarou k odkazom 10aa a 10ab znejú:
„[10aa)] Čl. 58 a 60 ods. 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 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) (Ú. v. EÚ L 151, 7.6.2019).
[10ab)] Čl. 7 nariadenia Európskeho parlamentu a Rady (EÚ) 2021/887, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier (Ú. v. EÚ L 202, 8.6.2021).“.“.

Odôvodnenie: *Vypúšťa sa ustanovenie o blokovaní z celého návrhu zákona z dôvodu neprimeranosti výkonu kompetencií úradu. Blokovanie ako riešenie kybernetického bezpečnostného incidentu, ako jeden*

z nástrojov úradu pri riešení závažného kybernetického incidentu, zostáva naďalej platným nástrojom v zmysle aplikácie ustanovení v § 27 platného znenia zákona.
Navrhovaným vypustením ustanovenia § 19 ods. 2 prvá veta, s čím pracuje vládny návrh zákona, by v zákone úplne absentovala definícia tretej strany. Tretia strana je pritom pojem, resp. legislatívna skratka, s ktorou zákon na viacerých miestach pracuje. Preto túto legislatívnu skratku navrhujeme presunúť z ust. § 19 ods. 2 prvá veta do ust. § 5 ods. 1 písm. ae), kde sa tento pojem prvýkrát používa.

2. V čl. I bod 13, § 5a odseky 4 až 6 znejú:

„(4) Úrad odníme európske certifikáty kybernetickej bezpečnosti, ktoré vydal alebo európske certifikáty kybernetickej bezpečnosti vydané podľa čl. 56 ods. 6 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 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) (ďalej len „nariadenie (EÚ) 2019/881“) orgánmi posudzovania zhody, ktoré nie sú v súlade s nariadením (EÚ) 2019/881 alebo s európskym systémom certifikácie kybernetickej bezpečnosti.
(5) Úrad môže odňať vydaný európsky certifikát kybernetickej bezpečnosti aj držiteľovi certifikátu, ak tento
a) poruší povinnosť podľa čl. 56 ods. 8 nariadenia (EÚ) 2019/881,
b) neumožní úradu získať prístup do priestorov podľa čl. 58 ods. 8 písm. d) nariadenia (EÚ) 2019/881,
c) akýmkoľvek spôsobom znemožní vykonávať oprávnenie podľa čl. 58 ods. 8 písm. b) nariadenia (EÚ) 2019/881.
(6) Na účely tohto zákona sa rozumie
a) produktom produkt IKT podľa čl. 2 ods. 12 nariadenia (EÚ) 2019/881,
b) službou služba IKT podľa čl. 2 ods. 13 nariadenia (EÚ) 2019/881,
c) procesom proces IKT podľa čl. 2 ods. 14 nariadenia (EÚ) 2019/881.“.“

Poznámky pod čiarou [10h]) až [10o]) sa vypúšťajú. V súvislosti s touto zmenou sa v čl. I bode 13 primerane upraví úvodná veta k poznámkam pod čiarou.

Odôvodnenie: *Namiesto techniky odkazu na príslušné články sa navrhuje technika odkazu na články nariadenia priamo v texte predpisu.*

3. V čl. I sa za bod 14 vkladá nový bod 15, ktorý znie:

„15. V § 8 ods. 5 sa vkladá nové písmeno f), ktoré znie:

„f) Úrad pre reguláciu elektronických komunikácií a poštových služieb,“.

Doterajšie písmeno f) sa označuje ako písmeno g).“

Nasledujúce novelizačné body sa primerane prečíslujú.

Odôvodnenie*: Navrhovaná úprava reflektuje zmeny v navrhovanom právnom predpise uvedené v čl. I a aj v čl. III. a zaradí Úrad pre*

reguláciu elektronických komunikácií a poštových služieb medzi subjekty s prístupom k jednotnému informačnému systému kybernetickej bezpečnosti na účely koordinovaného výkonu pôsobnosti a dodržania zásady jedného prístupového miesta.

4. V čl. I bod 20, § 10a odsek 1 znie:

„(1) Orgán verejnej moci, prevádzkovateľ základnej služby a právnická osoba v sektore podľa prílohy č. 1 sú povinní poskytnúť úradu na plnenie jeho úloh pri riešení kybernetického bezpečnostného incidentu podľa tohto zákona požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité na zabezpečenie kybernetickej bezpečnosti a riešenie kybernetického bezpečnostného incidentu; informácie sa poskytujú len za podmienky, že sú nevyhnutné pre riešenie kybernetického bezpečnostného incidentu a ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu[13a]) alebo spravodajskej služby podľa osobitného predpisu[13]) alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb, ktoré konajú v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce.“

Odôvodnenie: *Navrhovanou úpravou sa v porovnaní s vládnym návrhom zužuje zoznam subjektov, od ktorých je úrad oprávnený požadovať poskytnutie súčinnosti a zdôrazňuje sa, že ide o súčinnosť výlučne na riešenie kybernetického bezpečnostného incidentu.*

5. V čl. I bod 33 znie:

„33. V § 20 sa za odsek 4 vkladá nový odsek 5, ktorý znie:

„(5) Bezpečnostné opatrenia sa prijímajú a realizujú na základe analýzy rizík kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti. Súčasťou analýzy rizík je aj analýza politického rizika tretej strany, pričom politické riziko sa posudzuje najmä vzhľadom na

a) plnenie záväzkov z medzinárodných zmlúv, ktorými je Slovenská republika viazaná a na jej členstvo v medzinárodných organizáciách,
b) možnosť ovplyvňovania a zasahovania do činnosti tretej strany štátom, ktorý nie je členským štátom Európskej únie a Organizácie Severoatlantickej zmluvy (ďalej len „cudzí štát“),
c) analýzu vlastníckej štruktúry a riadiacej štruktúry tretej strany, vrátane vlastníckeho podielu cudzieho štátu a priamych zahraničných investícií do tretej strany,
d) analýzu právnych predpisov a medzinárodných záväzkov cudzieho štátu v oblasti ochrany základných ľudských práv a slobôd, kybernetickej bezpečnosti, boja proti počítačovej kriminalite, ochrany osobných údajov a ochrany informácií,
e) informácie špecifické pre cudzí štát a informácie spravodajskej služby o možných hrozbách pre záujmy Slovenskej republiky.

Politické riziká schvaľuje vláda Slovenskej republiky na základe stanoviska úradu. Stanovisko úradu sa predkladá Bezpečnostnej rade Slovenskej republiky. Politické riziká úrad zverejňuje v jednotnom informačnom systéme kybernetickej bezpečnosti. Úrad v analýze politického rizika zohľadní vyjadrenie Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky, Ministerstva hospodárstva Slovenskej

republiky, Ministerstva vnútra Slovenskej republiky, Slovenskej informačnej služby a Ministerstva obrany Slovenskej republiky z oblasti ich pôsobnosti.

Doterajší odsek 5 sa označuje ako odsek 6.“

Odôvodnenie:

Navrhovaná zmena v porovnaní s vládnym návrhom ponúka presnejšiu definíciu politického rizika. Vládny návrh zákona obsahuje stručný taxatívny výpočet oblastí, ktoré zahŕňa analýza politického rizika. Navrhovaný výpočet zahŕňa širší okruh čiastkových oblastí, ktoré by mal štát zohľadňovať v rámci analýzy politického rizika, čím sa umožňuje lepšie a komplexnejšie posúdenie politického rizika. Navrhovaná zmena tiež lepšie implementuje strategické opatrenia vyplývajúce z EÚ toolboxu kybernetickej bezpečnosti 5G sietí. Odporúčanie Komisie z 26. marca 2019 o kybernetickej bezpečnosti sietí 5G (ďalej len „Odporúčanie“) v recitáli 20 objasňuje „iné“ faktory kybernetickej bezpečnosti nasledovne: „Iné faktory môžu zahŕňať regulačné alebo iné požiadavky, ktoré boli uložené dodávateľom zariadení informačných a komunikačných technológií. Pri posúdení významu týchto faktorov by sa malo okrem iného zohľadniť celkové riziko vplyvu tretej krajiny, najmä v súvislosti s jej modelom riadenia, absenciou dohôd o spolupráci v oblasti bezpečnosti alebo podobných opatrení, ako napr. rozhodnutí o primeranosti, súvisiacich s ochranou údajov medzi Úniou a dotknutou treťou krajinou, alebo či je táto krajina zmluvnou stranou viacstranných, medzinárodných alebo dvojstranných dohôd v oblasti kybernetickej bezpečnosti, boja proti počítačovej kriminalite alebo ochrany údajov..“: Podľa správy o pokroku členských štátov pri implementácii EÚ Toolboxu kybernetickej bezpečnosti 5G sietí medzi konkrétne faktory uplatňované jednotlivými členskými štátmi EÚ patria objektívne faktory, ako napr.:

- pôvod dodávateľov alebo riziko ovplyvňovania zo strany tretích štátov (pri zohľadnení právneho a politického systému tretieho štátu);

- informácie špecifické pre konkrétny tretí štát a spravodajské informácie o možných rizikách a hrozbách.

Napr. v Holandsku vyhláška o bezpečnosti a integrite telekomunikácií z 28. novembra 2019 používa nasledujúce kritériá posúdenia rizika:

- služba alebo výrobok pochádza zo štátu, ktorého právne predpisy ukladajú neštátnym subjektom povinnosť spolupracovať s vládou tohto štátu, alebo ak je poskytovateľom (dodávateľom) služby alebo produktu priamo štátna (štátom vlastnená) spoločnosť,

- služba alebo produkt pochádza zo štátu s aktívnym útočným spravodajským programom zameraným na Holandsko a holandské záujmy, alebo dodávateľ pochádza zo štátu, s ktorým môžu byť vzťahy napäté do takej miery, že sú mysliteľné také vonkajšie aktivity, ktoré môžu mať vplyv na holandské záujmy.

Pozmeňujúci návrh spresňuje, že politické riziká vyhodnocuje vláda na základe stanoviska úradu a Bezpečnostnej rady, po zohľadnení vyjadrení taxatívne vymedzených orgánov a inštitúcií.

6. V čl. I bod 37 znie:

„37. Za § 24 sa vkladá § 24a, ktorý vrátane nadpisu znie:

„§ 24a
Automatizované poskytovanie informácií

(1) Ak je to vzhľadom na povahu alebo dôležitosť základnej služby potrebné a nedôjde k uzatvoreniu zmluvy podľa § 24 ods. 6, úrad môže rozhodnutím uložiť prevádzkovateľovi základnej služby povinnosť automatizovaným spôsobom vyhodnocovať výskyt kybernetického bezpečnostného incidentu a nahlasovať kybernetický bezpečnostný incident. Na tento účel zverejňuje úrad výstrahy, varovania a ďalšie informácie v jednotnom informačnom systéme kybernetickej bezpečnosti. Náklady spojené s technickým zabezpečením vyhodnocovania a nahlasovania kybernetického bezpečnostného incidentu znáša úrad.

(2) Povinnosť podľa odseku 1 nie je možné uložiť, ak ide o siete a informačné systémy, ktoré sa týkajú zabezpečenia obrany alebo bezpečnosti Slovenskej republiky.

(3) Úrad rozhodnutím podľa odseku 1 určí prevádzkovateľa základnej služby, ktorého sa povinnosť týka, spôsob poskytovania a rozsah informácií, ktoré sa týkajú automatizovaného spôsobu vyhodnocovania výskytu kybernetického bezpečnostného incidentu a nahlasovania kybernetického bezpečnostného incidentu a trvanie tejto povinnosti. Rozhodnutie sa môže týkať len takých informácií, ktoré sú nevyhnutné pre zabezpečenie kybernetickej bezpečnosti a riešenie kybernetického bezpečnostného incidentu, ak tento účel nemožno dosiahnuť inak.

(4) Obsah komunikácie a prenášaných správ a ochrana súkromia podľa osobitného predpisu[28a]) plnením povinností podľa odseku 1 nie sú dotknuté.“

Poznámka pod čiarou k odkazu 28a znie:
„[28a)] 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.“.“

Odôvodnenie:
Navrhovanou úpravou sa v porovnaní s vládnym návrhom spresňuje spôsob a rozsah poskytovania informácií zásadne iba na informácie o kybernetickom bezpečnostnom incidente. Pôvodne navrhovaná povinnosť priamo poskytovať systémové informácie zo sietí a informačných systémov, ktoré tvoria hranicu medzi sieťou, ktorú prevádzkuje prevádzkovateľ základnej služby a sieťou Internet, sa nahrádza iba povinnosťou automatizovaným spôsobom vyhodnocovať a nahlasovať kybernetický bezpečnostný incident.

7. V čl. I bod 38 znie:

„38. Za § 27 sa vkladá § 27a, ktorý vrátane nadpisu znie:

„§ 27a
Obmedzenie používania produktu, procesu, služby alebo tretej strany

(1) Úrad môže rozhodnutím zakázať alebo obmedziť používanie konkrétneho produktu, procesu, služby alebo tretej strany na poskytovanie základnej služby ak zistí, že takéto používanie

a) neumožňuje alebo zásadným spôsobom sťažuje udržanie kybernetickej bezpečnosti, a tým ohrozuje život alebo zdravie osôb, hospodárske fungovanie štátu, verejný poriadok, bezpečnosť alebo majetok osôb, alebo
b) ohrozuje bezpečnostné záujmy Slovenskej republiky.
(2) Konanie podľa odseku 1 úrad začne z vlastného podnetu alebo na základe odôvodneného podnetu iného orgánu verejnej moci Slovenskej republiky. Oznámenie o začatí konania úrad zverejní najmenej na 30 dní v jednotnom informačnom systéme kybernetickej bezpečnosti a na svojom webovom sídle a počas tejto doby nemôže vydať rozhodnutie.
(3) Úrad pred vydaním rozhodnutia podľa odseku 1 vždy vykoná vo vzťahu k produktu, procesu, službe alebo k tretej strane analýzu rizík podľa § 20 ods. 5 na základe vyjadrenia Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky, Ministerstva hospodárstva Slovenskej republiky, Ministerstva vnútra Slovenskej republiky, Slovenskej informačnej služby a Ministerstva obrany Slovenskej republiky z oblasti ich pôsobnosti. Návrh rozhodnutia predkladá Bezpečnostnej rade Slovenskej republiky a vláde Slovenskej republiky. Od stanoviska vlády Slovenskej republiky sa úrad nemôže odchýliť.
(4) Úrad vydá rozhodnutie podľa odseku 1 iba v prípade, ak prevádzkovateľ základnej služby alebo tretia strana nedostatky podľa odseku 1 neodstráni v primeranej lehote určenej úradom.
(5) Prevádzkovateľ základnej služby je povinný zdržať sa používania konkrétneho produktu, procesu, služby alebo tretej strany uvedenej v rozhodnutí podľa odseku 1 na poskytovanie základnej služby alebo ich používanie obmedziť.
(6) Rozhodnutie podľa odseku 1 sa vyhlási zverejnením v Zbierke zákonov Slovenskej republiky[28b]) a účinky nadobúda dňom vyhlásenia. Ak je vyhlásené rozhodnutie podľa odseku 1 zmenené alebo zrušené, na právny akt, ktorým sa rozhodnutie podľa odseku 1 zmenilo alebo zrušilo, sa prvá veta použije rovnako.
(7) Ak úrad rozhodnutím podľa odseku 1 zakáže alebo obmedzí používanie konkrétneho produktu, procesu, služby alebo tretej strany na poskytovanie základnej služby, v rozhodnutí podľa odseku 1 zároveň určí primeranú dobu zákazu alebo obmedzenia používania konkrétneho produktu, procesu, služby alebo tretej strany, ktorá nemôže byť dlhšia ako dva roky. O zákaze alebo obmedzení podľa prvej vety môže úrad rozhodnúť aj opakovane.
(8) Ak ide o produkt, proces, službu alebo tretiu stranu, ktorú prevádzkovateľ základnej služby začal používať pred zverejnením rozhodnutia podľa odseku 1, je prevádzkovateľ základnej služby povinný zdržať sa používania alebo obmedziť používanie produktu, procesu, služby alebo tretej strany uvedenej v rozhodnutí podľa odseku 1 v primeranej lehote určenej v rozhodnutí, ktorá nie je kratšia ako dva roky a dlhšia ako päť rokov. Zároveň je prevádzkovateľ základnej služby povinný najneskôr do 6 mesiacov od zverejnenia rozhodnutia podľa odseku 1 vykonať primerané bezpečnostné opatrenia na riadenie rizík podľa odseku 3.“

Poznámka pod čiarou k odkazu 28b znie:
„[28b]) § 13 písm. f) 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.“.“

Odôvodnenie:
Podľa ust. § 5 ods. 1 písm. ae) Národný bezpečnostný úrad posudzuje bezpečnostné riziká tretej strany, ktorých posúdenie predkladá

Bezpečnostnej rade SR. Naproti tomu vládou navrhované znenie ust. § 27a predpokladá posúdenie rizika iba vo vzťahu k produktu, procesu, službe. Preto navrhujeme výslovne doplniť aj posudzovanie rizika samotnej tretej strany (dodávateľa), nielen produktov, procesov a služieb. V EÚ Toolboxe totiž boli členské štáty EÚ vyzvané:
- posilniť bezpečnostné požiadavky na operátorov mobilných sietí (napr. zaviesť kontroly prístupu, pravidlá bezpečnej prevádzky, monitorovanie, obmedzenia outsourcingu konkrétnych úloh a funkcií atď.);
- posúdiť rizikový profil dodávateľov a následne uplatniť príslušné obmedzenia pre dodávateľov považovaných za vysoko rizikových;
- zaistiť, aby mal každý operátor vhodnú stratégiu viacerých dodávateľov, aby sa obmedzila akákoľvek závislosť od jedného dodávateľa (alebo dodávateľov s podobným rizikovým profilom), zabezpečiť primeranú rovnováhu dodávateľov na vnútroštátnej úrovni a vyhnúť sa závislosti od dodávateľov považovaných za vysoko rizikových.
Vo vzťahu k poslednej uvedenej povinnosti sa napr. v Taliansku vyžaduje vypracovanie projektu diverzifikácie, ktorý zahŕňa „vertikálnu" diverzifikáciu (použitie systémov od rôznych dodávateľov v oblasti hardvéru a softvéru) a „horizontálnu" diverzifikáciu (použitie rôznych softvérových riešení). Niekoľko členských štátov medzičasom zaviedlo opatrenia, ktoré napríklad požadujú, aby operátori predložili svoje vlastné stratégie diverzifikácie a zabezpečili prijatie opatrení na zvýšenie ich odolnosti a bezpečnostnej spoľahlivosti.
Túto povinnosť naším pozmeňujúcim návrhom navrhujeme zakotviť osobitne vo vzťahu k tým prevádzkovateľom základných služieb, ktorých sa dotkne zákaz alebo obmedzenie používania konkrétnych produktov, procesov, služieb alebo tretích strán.
Ďalej navrhujeme, aby podnet na začatie konania o posúdení rizika a zákaze produktov, procesov, služieb alebo tretích strán mohol úradu predložiť aj iný orgán verejnej moci SR, t.j. aby konanie nezačínalo iba na podnet, resp. ex offo z moci samotného úradu.
Tiež navrhujeme doplniť dobu maximálne dvoch rokov, na ktorú môže dôjsť k obmedzeniu používania rizikového produktu, procesu, služby či dodávateľa, a to aj opakovane. V prípade už využívaných produktov, procesov, služieb alebo tretích strán sa stanovuje minimálna doba dvoch rokov a maximálna doba piatich rokov, počas ktorej sa ešte produkty môžu používať. Zároveň však bude musieť prevádzkovateľ základnej služby do šiestich mesiacov vypracovať aj plán diverzifikácie, aby počas plynutia určenej doby minimalizoval riziko a závislosť od rizikového produktu, procesu, služby či dodávateľa.
Vypúšťajú sa vo vládnom návrhu obsiahnuté ustanovenia § 27b a 27c o blokovaní, a to z dôvodu neprimerane koncipovanej širokej navrhovanej pôsobnosti úradu. Blokovanie ako riešenie kybernetického bezpečnostného incidentu, ako nástroja jeho riešenia v podobe aplikácie ustanovenia § 27 v platnom znení zostáva v platnosti.

8. **V čl. I bode 41** v § 29 ods. 3 v poznámke pod čiarou k odkazu 31b) sa slová „STN EN ISO/IEC 17024" nahrádzajú slovami „STN EN ISO/IEC 17024 (015258)" a slová „(ISO/IEC 17024) (01 5258)" sa nahrádzajú slovami „Vestník Úradu pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky č. 3/13.".

Odôvodnenie: *Ide o legislatívnu úpravu, ktorou sa v poznámke pod čiarou spresňuje citácia slovenskej technickej normy doplnením odkazu na Vestník Úradu pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky č. 3/13. Podľa § 4 ods. 1 písm. b) zákona č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov sa vo Vestníku zverejňujú oznámenia o slovenskej technickej norme vhodnej na posudzovanie zhody.*

9. V čl. I bod 43 znie:

„43. V § 29 odsek 6 znie:

„(6) Úrad môže kedykoľvek vykonať audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby, alebo požiadať certifikovaného audítora kybernetickej bezpečnosti, aby vykonal takýto audit u prevádzkovateľa základnej služby s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom.“.“

Odôvodnenie: *Precizuje sa platný text z dôvodu, aby nevznikala neodôvodnená povinnosť vykonať audit do dvoch rokov aj pre tých prevádzkovateľov základnej služby, ktorým bol v tomto čase nariadený audit úradom.*

10. V čl. I bod 45, § 31 ods. 2 písmeno d) sa slová „§ 24a ods. 1 a 2“ nahrádzajú slovami „§24a ods. 1“.

Odôvodnenie: *Ide o legislatívno-technickú úpravu vzhľadom na zmenu obsahu ods. 2.*

11. V čl. I bod 48 znie:

„48. V § 31 sa za odsek 5 vkladajú nové odseky 6 až 9, ktoré znejú:
„(6) Úrad uloží pokutu od 300 eur do 100 000 eur výrobcovi alebo poskytovateľovi produktov, služieb alebo procesov, ktorý sa dopustí správneho deliktu tým, že podľa čl. 53 nariadenia (EÚ) 2019/881 vydá EÚ vyhlásenie o zhode, ktoré je v rozpore s požiadavkami ustanovenými v Európskom systéme certifikácie kybernetickej bezpečnosti.
(7) Úrad uloží pokutu od 300 eur do 100 000 eur výrobcovi alebo poskytovateľovi certifikovaných produktov, služieb alebo procesov alebo výrobcovi alebo poskytovateľovi produktov, služieb a procesov, pre ktoré je vydané EÚ vyhlásenie o zhode, ktorý sa dopustí správneho deliktu tým, že nezverejní v elektronickej podobe alebo neaktualizuje doplňujúce informácie o kybernetickej bezpečnosti podľa čl. 55 ods. 1 písm. a) až d) nariadenia (EÚ) 2019/881.
(8) Úrad uloží pokutu od 300 eur do 100 000 eur orgánu posudzovania zhody, držiteľovi európskeho certifikátu kybernetickej bezpečnosti alebo vydavateľovi EÚ vyhlásení o zhode, ktorý sa dopustí správneho deliktu tým, že
a) neposkytne vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti informácie potrebné na plnenie svojich úloh podľa čl. 58 ods. 8 písm. a) nariadenia (EÚ) 2019/881,

b) znemožní vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti viesť vyšetrovanie v podobe auditu podľa čl. 58 ods. 8 písm. b) nariadenia (EÚ) 2019/881.
(9) Úrad uloží pokutu od 300 eur do 100 000 eur orgánu posudzovania zhody alebo držiteľovi európskeho certifikátu kybernetickej bezpečnosti, ktorý sa dopustí správneho deliktu tým, že neumožní vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti prístup do priestorov podľa čl. 58 ods. 8 písm. d) nariadenia (EÚ) 2019/881.“.

Doterajšie odseky 6 až 12 sa označujú ako odseky 10 až 16.“

Odôvodnenie: *Namiesto techniky odkazu na príslušné články sa navrhuje technika odkazu na články nariadenia priamo v texte predpisu. V ods. 7 sa slovo „údaje“ nahrádza slovom „informácie“. Ide o legislatívnu úpravu, ktorou sa zosúlaďuje navrhovaný právny text s čl. 55 ods. 1 úvodnej vety nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 („...zverejňuje tieto doplňujúce informácie o kybernetickej bezpečnosti“) a súčasne s ďalšími navrhovanými ustanoveniami (odsekmi) v § 31, v ktorých sa používa termín „informácie“.*

12. V čl. I bod 52 znie:

„52. V § 32 sa odsek 1 dopĺňa písmenami g) a h), ktoré znejú:

„g) certifikačné schémy a postupy v systéme certifikácie kybernetickej bezpečnosti,
h) bezpečnostné opatrenia, ak si to vyžadujú právne záväzné akty a odporúčania Európskej únie pre oblasť kybernetickej bezpečnosti.“.“

Odôvodnenie: *Nadväzujúca úprava vzhľadom na vypustenie blokovania.*

13. V čl. I bod 53 znie:

„53. V § 33 ods. 1 sa slová „§ 17 ods. 6, § 21 ods. 4 a § 27“ nahrádzajú slovami „§ 17, § 21 a § 27“.“

Odôvodnenie: *Nadväzujúca úprava vzhľadom na vypustenie § 27b a 27c. Vo vzťahu k ust. § 27a sa naopak predpokladá aplikácia správneho poriadku a súdna preskúmateľnosť.*

14. V čl. I bod 58 znie:

„58. V prílohe č. 1 v sektore „3. Digitálna infraštruktúra“ sa v stĺpci „Prevádzkovateľ služieb“ vkladá nový riadok, ktorý znie: „poskytovateľ služieb webhostingu, DNS hostingu alebo mailhostingu“.“

Odôvodnenie: *Navrhovaná zmena v porovnaní s vládnym návrhom zužuje reguláciu v sektore digitálna infraštruktúra a odstraňuje prevádzkovateľa obchodu na internete s možnosťou vyhľadávania, objednávania a nákupu tovarov a služieb ako prevádzkovateľa služby v prílohe č. 1 zákona.*

Meno a priezvisko poslanca NR SR	Podpis
1. JURAJ KRÚPA	
2. PETER VOKÁL	
3. PETER KREMSKÝ	
4. Marcel Mihalík	
5. Lucia Ďuriková	
6. Richard Vašečka	
7. GYÖRGY GYIMESI	
8. ANNA ANDREJUVOVÁ	
9. Milan KUKLIAK	
10. Milan Vetrák	
11. Jaromír SIBL	
12. Monika Kozelová	
13. MAREK ŠEFČÍK	
14. MILAN POTOCKÝ	
15. Andrej Hamrík	
16. TOMÁŠ ŠUDÍK	
17. MILAN LAURENČÍK	
18.	
19.	