Republiková únia zamestnávateľov, Digital Park III, Einsteinova 19, 851 01 Bratislava 5
tel.: +421-2-3301 4280, ruz@ruzsr.sk, www.zamestnavatelia.sk

STANOVISKO REPUBLIKOVEJ ÚNIE ZAMESTNÁVATEĽOV

Zákon o kybernetickej bezpečnosti produktov s digitálnymi prvkami (zákon o kybernetickej odolnosti) a o zmene a doplnení niektorých zákonov

https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/LP/2026/316

Materiál v pripomienkovom konaní do 26.06.2026

Stručný popis podstaty materiálu najmä jeho relevancie z pohľadu RÚZ

Materiál predkladá do medzirezortného pripomienkového konania Národný bezpečnostný úrad na základe Plánu legislatívnych úloh vlády Slovenskej republiky na rok 2025

Cieľom a obsahom materiálu je najmä:
Účelom návrhu zákona je implementácia nariadenia Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami. Návrh zákona ustanovuje kompetencie, práva a povinnosti úradu ako orgánu dohľadu nad trhom pre produkt s digitálnymi prvkami (ďalej len „dohľad nad trhom"). Implementáciou nariadenia (EÚ) 2024/2847 sa najmä spresňuje samotný výkon dohľadu nad trhom a s ním súvisiace práva a povinnosti úradu ako orgánu dohľadu nad trhom a hospodárskych subjektov ako subjektov dohľadu nad trhom. Úrad bude v rámci výkonu dohľadu nad trhom uprednostňovať výkon dohľadu nad trhom na diaľku (monitorovanie dodržiavania povinností hospodárskych subjektov v online prostredí), ale na základe podnetov alebo na základe vlastných zistení môže pristúpiť k výkonu dohľad nad trhom aj na mieste priamo u hospodárskeho subjektu. Samotný výkon dohľadu nad trhom bude zabezpečovaný príslušníkmi úradu a zamestnancami úradu. Okrem nich sa môžu na dohľade nad trhom v prípade potreby podieľať aj iné fyzické osoby (odborníci) v postavení tzv. poverených osôb. Za nedodržanie povinností vyplývajúcich hospodárskym subjektom z nariadenia (EÚ) 2024/2847 a z tohto návrhu zákona bude úrad ukladať sankcie v podobe ukladania pokút vyplývajúcich z nariadenia (EÚ) 2024/2847 a ukladania opatrení vyplývajúcich z nariadenia (EÚ) 2019/1020.

Návrh zákona má nadobudnúť účinnosť dňa 01.01.2027, okrem vymedzených ustanovení, ktoré nadobudnú účinnosť neskôr

Postoj RÚZ k materiálu

Účelom návrhu zákona je implementácia nariadenia Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami. RÚZ k návrhu predkladá nižšie uvedené pripomienky.

Pripomienky RÚZ k predkladanému materiálu

1. Zásadná pripomienka k čl. I., - návrh zákona ako celku

Požadujeme doplniť legislatívnu techniku tak, aby zákon nepreberal neúplne ani odchylne definície CRA; pri pojmoch „produkt s digitálnymi prvkami", „hospodársky subjekt", „výrobca", „dovozca", „distribútor", „podstatná úprava", „zraniteľnosť", „aktívne zneužívaná zraniteľnosť" a „obdobie podpory" buď použiť presné znenie oficiálneho slovenského znenia CRA, alebo uviesť explicitný odkaz na čl. 3 CRA.

Odôvodnenie:
Telekomunikačné prostredie obsahuje kombináciu produktov, služieb, konfigurácií, vlastného softvéru, zákazníckych zariadení a sieťových prvkov. Nejednoznačná definícia môže spôsobiť neprimerané prenesenie povinností výrobcu na subjekt, ktorý je iba používateľom, integrátorom alebo distribútorom.

2. Zásadná pripomienka k čl. I., §3 a čl. IV

Navrhujeme doplniť alebo upraviť účinnosť § 3 tak, aby právny a technický režim prijímania oznámení podľa čl. 14 CRA bol zabezpečený najneskôr od 11. septembra 2026; súčasne upraviť prechodné ustanovenia pre produkty uvedené na trh pred 11. decembrom 2027.

Optimálnejšie nastaviť účinnosť zákona na deň účinnosti nariadenia CRA (11.december 2027) a osobitne skoršiu účinnosť pre plnenie oznamovaných povinností podľa čl. 14 CRA.

Odôvodnenie:
CRA stanovuje skoršiu aplikáciu čl. 14. Národný zákon, ktorý aktivuje oznamovací mechanizmus až od 1. januára 2027, môže vytvoriť implementačnú medzeru a právnu neistotu pre výrobcov, dovozcov, distribútorov a osoby plniace oznamovacie povinnosti.

3. Zásadná pripomienka k čl. I., §3
Navrhujeme výslovne ustanoviť, že použitie národného jednotného informačného systému kybernetickej bezpečnosti nesmie zakladať duplicitu voči jednotnej platforme podľa CRA a musí byť technicky, procesne a právne interoperabilné s platformou podľa čl. 16 CRA.

Odôvodnenie:
Oznamovanie aktívne zneužívaných zraniteľností a závažných incidentov s vplyvom na bezpečnosť produktu má podľa CRA prebiehať súčasne voči CSIRT určenému za koordinátora a ENISA prostredníctvom jednotnej reporting platformy. Národná úprava musí predísť duplicite a nejasnosti, ktorý kanál je právne rozhodujúci.

4. Zásadná pripomienka k čl. I., §3
Navrhujeme doplniť, že oznamovacie povinnosti podľa tohto zákona sa majú vykonávať spôsobom, ktorý nevytvára duplicitu voči oznamovacím povinnostiam podľa zákona o kybernetickej bezpečnosti, transpozície smernice (EÚ) 2022/2555 (NIS 2), všeobecného nariadenia o ochrane údajov (GDPR), zákona o elektronických komunikáciách alebo iných sektorových predpisov. Ak hospodársky subjekt oznámil incident alebo zraniteľnosť príslušnému orgánu prostredníctvom určeného mechanizmu, úrad má v maximálnej možnej miere využiť už oznámené údaje a nepožadovať opakované oznamovanie totožných informácií.

Odôvodnenie:
Podniky poskytujúce elektronické komunikačné siete a služby už podliehajú viacerým incident reporting režimom. Duplicitné hlásenia zvyšujú administratívnu záťaž, môžu viesť k nejednotným interpretáciám toho istého incidentu a odčerpávajú odborné kapacity, ktoré majú byť prioritne využité na technické riešenie incidentu alebo zraniteľnosti.

5. Zásadná pripomienka k čl. I., §3
Navrhujeme presnejšie formulovať § 3 – oznamovacia povinnosť podľa čl. 14 CRA sa vzťahuje len na výrobcu, pre ostatných je len na dobrovoľnej báze.

6. Zásadná pripomienka k čl. I., §5 vloženie nového odseku
Navrhujeme doplniť splnomocnenie alebo povinnosť NBÚ vydať metodické usmernenie, ktoré vysvetlí, čo sa v telekomunikačnom prostredí považuje a nepovažuje za podstatnú úpravu produktu s digitálnymi prvkami.

Odôvodnenie:
Bežný provisioning, konfigurácia služby, bezpečnostná konfigurácia podľa dokumentácie výrobcu, distribúcia výrobcom dodanej bezpečnostnej aktualizácie alebo zákaznícke nastavenia by nemali automaticky viesť k tomu, že telekomunikačný podnik bude považovaný za výrobcu.

7. Zásadná pripomienka k čl. I., §5
Navrhujeme doplniť výslovné záruky proporcionality, nevyhnutnosti a ochrany obchodného tajomstva, duševného vlastníctva, zdrojového kódu, SBOM, bezpečnostných konfigurácií a informácií o kritickej infraštruktúre pri výkone dohľadu nad trhom.

Odôvodnenie:

Návrh umožňuje požadovať technickú dokumentáciu vrátane prístupu k zabudovanému softvéru. V telekomunikačnom sektore môže ísť o vysoko citlivé informácie o sieťovej architektúre, zraniteľnostiach, vendor dokumentácii, konfiguráciách a bezpečnostných mechanizmoch.

8. Zásadná pripomienka k čl. I., §5 odsek 1, písmeno b)

Navrhujeme doplniť v § 5 ods. 1 že sa oprávnenia orgánu dozoru podľa písm. b) uplatňujú voči kontrolovanému subjektu. Považujeme napr. za nejasné, či odstránenie obsahu z online rozhrania sa má a môže vzťahovať všeobecne na akýkoľvek hospodársky subjekt.

9. Zásadná pripomienka k čl. I., §5 odsek 1, písmeno f)

Navrhujeme doplniť do § 5 ods. 4 písm. f), že právo odoberať vzorky produktu s digitálnymi prvkami alebo jeho časti je dovolené len ak to povaha produktu umožňuje

10. Zásadná pripomienka k čl. I., §6

Pri poverených osobách požadujeme doplniť požiadavky na nezávislosť, preukázateľnú odbornú spôsobilosť, bezpečnostný režim, mlčanlivosť, zákaz konfliktu záujmov a vylúčenie osôb s konkurenčným alebo dodávateľským konfliktom voči kontrolovanému subjektu.

Odôvodnenie:

Externá poverená osoba môže pri dohľade získať prístup k informáciám, ktoré majú povahu obchodného tajomstva, bezpečnostnej dokumentácie alebo informácií súvisiacich s kontinuitou elektronických komunikačných služieb.

11. Zásadná pripomienka k čl. I., §8

Pri opatreniach podľa § 8 navrhujeme doplniť povinnosť posúdiť dopad na kontinuitu elektronických komunikačných služieb, kritickú infraštruktúru, tiesňové volania, podnikových zákazníkov a verejný záujem..

Navrhujeme doplniť v § 8 výslovne aj požiadavku, aby sa opatrenia ukladali primerané povahe identifikovaného rizika a v súlade s princípom ako je uvedené v nariadení CRA t.j. opatrenia ako je zákaz sprístupnenia alebo uvedenia na trh alebo stiahnutie z trhu by mali byť ukladané až potom, ak hospodársky subjekt neprijme vhodné nápravné opatrenia v určenej lehote alebo ak nesúlad alebo riziko pretrváva (vid čl. 54 ods. 5, čl. 58 nariadenia CRA, čl. 19 nariadenia 2019/1020, rovnaký princíp upravený aj v zákone č. 128/2002 Z.z.) a pri zohľadnení dopadov na kľúčové subjekty uvedené v článku 3 ods. 1 smernice (EÚ) 2022/2555 a iný verejný záujem.

Celkovo je nejasné akým spôsobom bude úrad postupovať pri výkone dohľadu podľa nariadenia 2029/1020 a súčasne úprave v čl. 52 až 60 CRA .

V § 8 ods. 1 písm a) a § 10 – povinnosť uviesť produkt s digitálnymi prvkami do súladu s osobitným predpisom1) by sa mala uložiť a smerovať primárne voči hospodárskemu subjektu, ktorý je výrobcom ako sa predpokladá v čl. 58 nariadenia 2024/2847.

Odôvodnenie:

Zákaz sprístupňovania, zákaz uvedenia do prevádzky, stiahnutie alebo spätné prevzatie zariadení môže v telekomunikačnom prostredí vyvolať sekundárny bezpečnostný a spoločenský dopad, ktorý môže byť závažnejší než samotné produktové riziko.

12. Zásadná pripomienka k čl. I., §8

Navrhujeme doplniť, že opatrenia podľa tohto zákona sa ukladajú vo vzťahu ku konkrétnemu produktu s digitálnymi prvkami a jeho súladu s požiadavkami podľa Nariadenia (EÚ) 2024/2847. Opatrenia podľa tohto zákona nemožno ukladať výlučne z dôvodu krajiny pôvodu produktu, sídla výrobcu, vlastníckej štruktúry výrobcu, jeho obchodnej značky alebo všeobecnej rizikovosti dodávateľa, ak nie je preukázaný nesúlad konkrétneho produktu alebo konkrétne kyberneticko-bezpečnostné riziko podľa tohto zákona. Tým nie sú dotknuté opatrenia podľa osobitných predpisov upravujúcich kybernetickú bezpečnosť, národnú bezpečnosť, bezpečnosť dodávateľského reťazca alebo ochranu kritických služieb.

Odôvodnenie:

Rizikovosť dodávateľa, krajina pôvodu, vlastnícka kontrola alebo väzby na tretí štát patria systematicky do režimu riadenia kybernetických rizík a bezpečnosti dodávateľského reťazca podľa zákona o kybernetickej bezpečnosti, transpozície smernice (EÚ) 2022/2555 (NIS 2) alebo osobitných bezpečnostných predpisov. Návrh zákona o kybernetickej odolnosti by nemal vytvárať implicitný základ na plošné zákazy dodávateľov alebo výmenu už nasadených technológií bez osobitného právneho základu, individuálneho posúdenia rizika, proporcionality a prechodných období.

13. Zásadná pripomienka k čl. I., §8

Ak opatrenie podľa tohto zákona môže mať významný dopad na dostupnosť, kontinuitu alebo bezpečnosť elektronických komunikačných sietí alebo elektronických komunikačných služieb, navrhujeme doplniť povinnosť úradu pred uložením opatrenia primerane konzultovať jeho dopady s Úradom pre reguláciu elektronických komunikácií a poštových služieb, ak tým nie je zmarený účel opatrenia alebo bezprostredne ohrozený verejný záujem.

Odôvodnenie:
Zákaz používania, zákaz sprístupňovania, stiahnutie alebo spätné prevzatie technológie v telekomunikačnej sieti môže mať širší dopad než bežné stiahnutie spotrebného výrobku z trhu. Pri zásahu do siete je potrebné zohľadniť dostupnosť služieb, tiesňové volania, podnikových zákazníkov, verejné služby, kontinuitu kritickej infraštruktúry a čas potrebný na bezpečnú migráciu alebo náhradu technológie.

14. Zásadná pripomienka k čl. I., - vloženie nového ustanovenia

Navrhujeme doplniť odporúčanie alebo sektorové usmernenie, aby obstarávanie produktov s digitálnymi prvkami obsahovalo povinnosť dodávateľa preukázať súlad s CRA, support period, CVD politiku, spôsob bezpečnostných aktualizácií, EU vyhlásenie o zhode, CE označenie a dostupnosť relevantnej technickej dokumentácie.

Odôvodnenie:
Telekomunikačný podnik bude vo veľkej miere závislý od výrobcov a dodávateľov. CRA má priamy dopad na RFP/RFI, zmluvy, vendor management, SLA pre zraniteľnosti a požiadavky na dokumentáciu.

15. Zásadná pripomienka k čl. I., §11

Navrhujeme doplniť jasné kritériá, kedy hospodársky subjekt hradí náklady vzoriek, skúšok a ďalších úkonov, vrátane limitov primeranosti a pravidiel pri spornom alebo čiastočnom zistení nesúladu.

Odôvodnenie:
Testovanie sieťových prvkov, bezpečnostných zariadení alebo špecializovaného softvéru môže byť nákladné. Bez limitov môže vzniknúť neprimeraná ekonomická záťaž, najmä ak záver dohľadu nebude jednoznačný.

16. Zásadná pripomienka k čl. I., §12

Navrhujeme doplniť režim klasifikácie a zdieľania citlivých informácií pri výmene medzi NBÚ, CSIRT, ENISA, Komisiou, colnými orgánmi a inými orgánmi dohľadu.

Navrhujeme doplniť v § 12 výslovne aj odkaz na osobitný predpis (nariadenie 2024/2847 a ďalšie vykonávacie predpisy), ktoré upravujú výnimky, kedy sa informácie neposkytujú.

Taktiež navrhujeme doplniť do § 6 ods. 9 výslovne, že „Povinnosť zachovávať mlčanlivosť trvá aj po ukončení služobného vzťahu alebo obdobného vzťahu; v prípade prizvanej osoby povinnosť zachovávať mlčanlivosť trvá aj po vykonaní úkonu vo všeobecnom záujme."

Odôvodnenie:
Informácie o aktívne zneužívaných zraniteľnostiach, topológii produktov a mitigáciách môžu byť samy osebe zneužiteľné. Návrh má preto jasne upraviť ochranu, rozsah a účel sprístupnenia.

17. Zásadná pripomienka k čl. I., §13

Navrhujeme zachovať sankčný rámec podľa CRA, ale doplniť transparentnú metodiku posudzovania závažnosti, opakovanosti, miery zavinenia, prijatých nápravných opatrení, spolupráce subjektu a dopadu na trh a kontinuitu služieb.

Odôvodnenie:

Pokuty viazané na celosvetový obrat sú materiálne významné. Pri formálnom alebo technicky spornom nesúlade je potrebná predvídateľnosť, proporcionalita a možnosť efektívnej nápravy pred sankčnou eskaláciou.

18. Zásadná pripomienka k čl. I., §13

Navrhujeme doplniť princíp prednosti nápravy pred sankciou. Pri menej závažnom, formálnom alebo technicky spornom porušení má úrad pred uložením pokuty spravidla vyzvať hospodársky subjekt na nápravu a určiť primeranú lehotu, ak tým nie je bezprostredne ohrozená kybernetická bezpečnosť, zdravie, bezpečnosť osôb alebo iný významný verejný záujem. Zároveň doplniť možnosť upustiť od uloženia pokuty, ak hospodársky subjekt porušenie bezodkladne odstránil, poskytol súčinnosť a porušenie nespôsobilo významné kybernetické-bezpečnostné riziko.

Odôvodnenie:

Cieľom dohľadu má byť predovšetkým uvedenie produktu do súladu a odstránenie rizika, nie sankcionovanie ako prvý nástroj. Nový regulačný rámec bude spojený s viacerými aplikačnými a technickými otázkami. Pri sporných alebo formálnych nedostatkoch je primerané najskôr umožniť efektívnu nápravu, pokiaľ nejde o situáciu s bezprostredným alebo závažným rizikom.

19. Zásadná pripomienka k čl. I., §13

Navrhujeme doplniť do § 13 pri ukladaní pokút, že pokutu nemožno uložiť, ak bola za to isté porušenie povinností uložená podľa iných právnych predpisov (nejasné, akým spôsobom sa bude aplikovať napr. čl. 52 ods. 14 ak by mal mať oprávnenie na výkon dohľadu v tej istej veci iný orgán dohľadu podľa iného právneho predpisu).

Navrhujeme taktiež upraviť a zosúladiť lehotu v akej môže orgán dohľadu uložiť pokutu s lehotou (3 roky od porušenia povinnosti), ktorá je upravená v zákone č. 128/2002 Z.z. o štátnej kontrole vnútorného trhu vo veciach spotrebiteľa.

20. Zásadná pripomienka k čl. I., §14

Mali by sa aplikovať pravidlá správneho poriadku aj v prípade postupu § 2 ods. 2 psím o) (kompetencie úradu rozhodovať aj v odvolacom konaní), kde v odvolacom konaní rozhoduje orgán vyššej inštancie resp. predseda úradu na základe návrhu ním ustanovenej osobitnej komisie v prípade rozkladu.

Taktiež navrhujeme v §14 výpočet ust, na ktoré sa nevzťahuje správny poriadok upraviť tak, aby sa vypustiť § 6 (správy poriadok sa vzťahoval aj na prípad, ak úrad vykonáva dohľad na diaľku). V čl. 54 ods. 1 CRA sa výslovne uvádza odkaz na čl. 18 nariadenia 2019/1020 (hospodársky má mať vždy právo vyjadriť sa k zisteniam pred uložením opatrenia, rozhodnutia).

21. Zásadná pripomienka k čl. I., - vloženie nového ustanovenia

Do návrhu zákona navrhujeme doplniť, že samotné poskytovanie konektivity, prenosu signálov, prístupu k internetu, smerovania, prepájania alebo inej technickej konektivity sa nepovažuje za uvedenie alebo sprístupnenie produktu s digitálnymi prvkami na trh, ak podnik vo vzťahu ku konkrétnemu produktu nevystupuje ako výrobca, dovozca, distribútor, splnomocnený zástupca alebo osoba vykonávajúca podstatnú úpravu produktu.

Odôvodnenie:

CRA je produktová regulácia. Podnik poskytujúci elektronické komunikačné siete alebo služby môže v konkrétnom prípade vystupovať ako distribútor, integrátor alebo výrobca produktu, avšak nemá byť považovaný za hospodársky subjekt s povinnosťami výrobcu len preto, že prevádzkuje sieť alebo poskytuje službu. Výslovné vymedzenie znižuje riziko neprimeraného rozšírenia pôsobnosti zákona na služby, ktoré sú regulované osobitnými predpismi.

22. Zásadná pripomienka k čl. I., - vloženie nového ustanovenia

Doplniť, že hospodársky subjekt plní povinnosti podľa tohto zákona len v rozsahu svojej konkrétnej roly vo vzťahu ku konkrétnemu produktu s digitálnymi prvkami a len v rozsahu informácií, dokumentov a technických možností, ktoré má právne a fakticky k dispozícii. Podnik nesmie byť sankcionovaný za neposkytnutie dokumentácie, zdrojového kódu, software bill of materials (SBOM) alebo technických informácií, ktoré má výlučne výrobca, dovozca, distribútor alebo iný subjekt v dodávateľskom reťazci a ku ktorým podnik nemá právny alebo technický prístup.

Odôvodnenie:
Telekomunikačný podnik často používa sieťové prvky, bezpečnostné zariadenia, koncové zariadenia, softvér alebo cloudové komponenty tretích strán. Nemusí mať zdrojový kód, úplnú technickú dokumentáciu, SBOM ani oprávnenie poskytnúť dodávateľskú dokumentáciu úradu. Povinnosti a sankcie musia byť viazané na reálnu rolu subjektu v dodávateľskom reťazci a na rozsah jeho faktickej kontroly nad produktom.

Zdroj:

https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/LP/2026/316