NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2025/37

z 19. decembra 2024,

ktorým sa mení nariadenie (EÚ) 2019/881, pokiaľ ide o riadené bezpečnostné služby

(Text s významom pre EHP)

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru ([1]),

po porade s Výborom regiónov,

konajúc v súlade s riadnym legislatívnym postupom ([2]),

keďže:

(1) Nariadením Európskeho parlamentu a Rady (EÚ) 2019/881 ([3]) sa stanovuje rámec pre zavádzanie európskych schém certifikácie kybernetickej bezpečnosti na zabezpečenie primeranej úrovne kybernetickej bezpečnosti produktov informačných a komunikačných technológií (ďalej len „IKT“), služieb IKT a procesov IKT v Únii, ako aj na predídenie fragmentácii vnútorného trhu z hľadiska schém certifikácie kybernetickej bezpečnosti v Únii.

(2) S cieľom zabezpečiť odolnosť Únie voči kybernetickým útokom a zabrániť akýmkoľvek zraniteľnostiam na vnútornom trhu je zámerom tohto nariadenia doplniť horizontálny regulačný rámec, ktorým sa stanovujú komplexné požiadavky na kybernetickú bezpečnosť pre produkty s digitálnymi prvkami podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2024/2847 ([4]), a to stanovením bezpečnostných cieľov na riadené bezpečnostné služby, ako aj uplatňovanie a dôveryhodnosť uvedených služieb.

(3) Riadené bezpečnostné služby sú poskytované poskytovateľmi riadených bezpečnostných služieb, ktorí sú vymedzení v článku 6 bode 40 smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 ([5]). Vymedzenie pojmu „riadené bezpečnostné služby“ v tomto nariadení by preto malo byť v súlade s vymedzením pojmu „poskytovatelia riadených bezpečnostných služieb“ v smernici (EÚ) 2022/2555. Uvedené služby spočívajú vo vykonávaní činností súvisiacich s riadením rizika kybernetickej bezpečnosti ich zákazníkov alebo poskytovanie pomoci pri týchto činnostiach a nadobúdajú čoraz väčší význam pri prevencii a zmierňovaní incidentov. V súlade s tým sa poskytovatelia týchto služieb považujú za kľúčové alebo dôležité subjekty patriace do odvetvia s vysokou úrovňou kritickosti podľa smernice (EÚ) 2022/2555. Ako sa uvádza v odôvodnení 86 uvedenej smernice, poskytovatelia riadených bezpečnostných služieb zohrávajú osobitne dôležitú úlohu v pomoci subjektom v ich úsilí o prevenciu, odhaľovanie incidentov, reakciu na ne alebo zotavenie sa z nich, a to v takých oblastiach, ako je reakcia na incidenty, penetračné testovanie, bezpečnostné audity a poradenstvo. Aj samotní poskytovatelia riadených bezpečnostných služieb však boli cieľom kybernetických útokov a ich úzke zapojenie do činnosti ich zákazníkov predstavuje osobitné riziko. Je preto dôležité, aby kľúčové a dôležité subjekty v zmysle smernice (EÚ) 2022/2555 venovali výberu poskytovateľov riadených bezpečnostných služieb zvýšenú pozornosť.

([1]) Ú. v. EÚ C 349, 29.9.2023, s. 167.
([2]) Pozícia Európskeho parlamentu z 24. apríla 2024 (zatiaľ neuverejnená v úradnom vestníku) a rozhodnutie Rady z 2. decembra 2024.
([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) 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 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15).
([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) (Ú. v. EÚ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).
([5]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80).

(4) Vymedzenie pojmu riadených bezpečnostných služieb podľa tohto nariadenia zahŕňa neúplný zoznam riadených bezpečnostných služieb, ktoré by mohli spĺňať podmienky pre európske schémy certifikácie kybernetickej bezpečnosti, ako je riešenie incidentov, penetračné testovanie, bezpečnostné audity, a poradenstvo týkajúce sa technickej podpory. Riadené bezpečnostné služby by mohli zahŕňať služby kybernetickej bezpečnosti, ktoré podporujú pripravenosť, prevenciu, odhaľovanie, analýzu a zmierňovanie incidentov, reakciu na ne a obnovu po nich. Za riadené bezpečnostné služby by sa mohlo považovať aj poskytovanie spravodajských informácií o kybernetických hrozbách a posudzovanie rizík súvisiacich s technickou podporou. Pre jednotlivé riadené bezpečnostné služby by mohli existovať samostatné európske schémy certifikácie kybernetickej bezpečnosti. Európske certifikáty kybernetickej bezpečnosti vydané v súlade s takýmito schémami by sa mali vzťahovať na konkrétne riadené bezpečnostné služby konkrétneho poskytovateľa uvedených služieb.

(5) Poskytovatelia riadených bezpečnostných služieb môžu takisto zohrávať dôležitú úlohu v súvislosti s činnosťami Únie, ktoré podporujú reakciu a počiatočnú obnovu v prípadoch významných incidentov a kybernetických bezpečnostných incidentov veľkého rozsahu, pričom sa spoliehajú na služby od dôveryhodných súkromných poskytovateľov a na testovanie kritických subjektov z hľadiska potenciálnych zraniteľných miest na základe koordinovaných posúdení bezpečnostných rizík na úrovni Únie. Certifikácia riadených bezpečnostných služieb by mohla zohrávať úlohu pri výbere dôveryhodných poskytovateľov riadených bezpečnostných služieb vymedzených v nariadení Európskeho parlamentu a Rady (EÚ) 2025/38 ([6]).

(6) Certifikácia riadených bezpečnostných služieb sa netýka len výberového procesu pre rezervu EÚ na účely kybernetickej bezpečnosti zriadenú nariadením (EÚ) 2025/38, ale je takisto dôležitým ukazovateľom kvality pre súkromné a verejné subjekty, ktoré majú v úmysle si takéto služby zakúpiť. Vzhľadom na kritickosť riadených bezpečnostných služieb a citlivosť spracúvaných údajov by certifikácia mohla poskytnúť potenciálnym zákazníkom dôležité usmernenie a uistenie o dôveryhodnosti týchto služieb. Európske schémy certifikácie kybernetickej bezpečnosti pre riadené bezpečnostné služby majú za cieľ prispievať k predchádzaniu fragmentácii vnútorného trhu. Cieľom tohto nariadenia je teda zlepšiť fungovanie vnútorného trhu.

(7) Európske schémy certifikácie kybernetickej bezpečnosti pre riadené bezpečnostné služby by mali viesť k využívaniu týchto služieb a k zvýšeniu hospodárskej súťaže medzi poskytovateľmi riadených bezpečnostných služieb. Bez toho, aby bol dotknutý cieľ zabezpečiť dostatočnú a primeranú úroveň relevantných technických znalostí a profesijnej integrity takýchto poskytovateľov, takéto schémy certifikácie by preto mali uľahčiť vstup na trh a ponuku riadených bezpečnostných služieb tým, že sa v čo najväčšej možnej miere zjednoduší potenciálna regulačná, administratívna a finančná záťaž, s ktorou by sa poskytovatelia, najmä malé a stredné podniky (ďalej len „MSP“), vrátane mikropodnikov, mohli stretnúť pri ponúkaní riadených bezpečnostných služieb. V záujme podpory využívania riadených bezpečnostných služieb a stimulácie dopytu po nich by tieto európske schémy certifikácie kybernetickej bezpečnosti okrem toho mali prispievať k prístupnosti týchto služieb, najmä pre menšie subjekty, ako sú MSP vrátane mikropodnikov, ako aj pre miestne a regionálne orgány, ktoré majú obmedzené kapacity a zdroje, avšak sú náchylnejšie na narušenie kybernetickej bezpečnosti, čo má finančné, právne, reputačné a prevádzkové dôsledky.

(8) Je dôležité poskytovať podporu MSP, vrátane mikropodnikov, pri vykonávaní tohto nariadenia a pri nábore pracovníkov so špecializovanými zručnosťami a odbornými znalosťami v oblasti kybernetickej bezpečnosti potrebnými na poskytovanie riadených bezpečnostných služieb v súlade s požiadavkami stanovenými v tomto nariadení. V programe Digitálna Európa zriadenom nariadením Európskeho parlamentu a Rady (EÚ) 2021/694 ([7]) a iných príslušných programoch Únie sa stanovuje, že Komisia zavedie finančnú a technickú podporu, ktorá uvedeným podnikom umožní prispievať k rastu hospodárstva Únie a k posilneniu spoločnej úrovne kybernetickej bezpečnosti v Únii, a to aj zjednodušením finančnej podpory z programu Digitálna Európa a iných relevantných programov Únie a podporou MSP, vrátane mikropodnikov.

(9) Európske schémy certifikácie kybernetickej bezpečnosti pre riadené bezpečnostné služby by mali prispievať k dostupnosti zabezpečených a vysokokvalitných služieb, ktoré zaručujú bezpečný prechod na digitálnu technológiu, a k dosiahnutiu cieľov stanovených v politickom programe Digitálne desaťročie 2030 zriadenom rozhodnutím Európskeho parlamentu a Rady (EÚ) 2022/2481 ([8]), najmä pokiaľ ide o cieľ, aby 75 % podnikov v Únii

([6]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2025/38 z 19. decembra 2024, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne a ktorým sa mení nariadenie (EÚ) 2021/694 (akt o kybernetickej solidarite) (Ú. v. EÚ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/694 z 29. apríla 2021, ktorým sa zriaďuje program Digitálna Európa a zrušuje rozhodnutie (EÚ) 2015/2240 (Ú. v. EÚ L 166, 11.5.2021, s. 1).

([8]) Rozhodnutie Európskeho parlamentu a Rady (EÚ) 2022/2481 zo 14. decembra 2022, ktorým sa zriaďuje politický program digitálne desaťročie do roku 2030 (Ú. v. EÚ L 323, 19.12.2022, s. 4).

začalo používať cloudové služby, veľké dáta alebo umelú inteligenciu, aby viac ako 90 % MSP, vrátane mikropodnikov, dosiahlo aspoň základnú úroveň digitálnej intenzity a aby boli kľúčové verejné služby dostupné online.

(10) Riadené bezpečnostné služby často poskytujú okrem zavádzania produktov IKT, služieb IKT alebo procesov IKT aj ďalšie služby, ktoré sú závislé od zručností, odborných znalosti a skúseností zamestnancov poskytovateľov takýchto služieb. Na zabezpečenie veľmi vysokej kvality poskytovaných riadených bezpečnostných služieb by súčasťou bezpečnostných cieľov mala byť veľmi vysoká úroveň uvedených zručností, odborných znalostí a skúseností, ako aj vhodné interné postupy. V záujme zabezpečenia toho, aby sa špecializované európske schémy certifikácie kybernetickej bezpečnosti vzťahovali na všetky aspekty riadených bezpečnostných služieb, je teda potrebné zmeniť nariadenie (EÚ) 2019/881. Mali by sa zohľadniť výsledky a odporúčania hodnotenia a preskúmania stanovené v nariadení (EÚ) 2019/881.

(11) S cieľom uľahčiť rast spoľahlivého vnútorného trhu a zároveň vytvoriť partnerstvá s podobne zmýšľajúcimi tretími krajinami, by sa mal proces certifikácie zavedený v európskom rámci certifikácie kybernetickej bezpečnosti stanovenom nariadením (EÚ) 2019/881 implementovať spôsobom, ktorý uľahčuje medzinárodné uznávanie a súlad s medzinárodnými normami.

(12) Únia čelí nedostatku talentov, ktorý sa vyznačuje nedostatkom kvalifikovaných odborníkov, a rýchlo sa vyvíjajúcej panoráme hrozieb, ako sa uznáva v oznámení Komisie z 18. apríla 2023 s názvom „Riešenie nedostatku odborníkov v oblasti kybernetickej bezpečnosti s cieľom posilniť konkurencieschopnosť, rast a odolnosť EÚ (Akadémia kybernetických zručností)“. Vzdelávacie zdroje a formy formálnej odbornej prípravy sa líšia a vedomosti možno získať rôznymi spôsobmi: formálne, napríklad na univerzite alebo na kurzoch, alebo neformálne, napríklad prostredníctvom odbornej prípravy na pracovisku alebo na základe pracovných skúseností v príslušnej oblasti. S cieľom uľahčiť vznik vysokokvalitných riadených bezpečnostných služieb a získať lepší prehľad o zložení pracovnej sily v oblasti kybernetickej bezpečnosti v Únii je preto dôležité, aby sa posilnila spolupráca medzi členskými štátmi, Komisiou, Agentúrou Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) a zainteresovanými stranami vrátane súkromného sektora a akademickej obce prostredníctvom rozvoja verejno-súkromných partnerstiev, podpory výskumných a inovačných iniciatív, vývoja a vzájomného uznávania spoločných noriem a certifikácie zručností v oblasti kybernetickej bezpečnosti, a to aj prostredníctvom európskeho rámca zručností v oblasti kybernetickej bezpečnosti. Táto spolupráca by tiež uľahčila mobilitu odborníkov v oblasti kybernetickej bezpečnosti v rámci Únie, ako aj začlenenie znalostí a odbornej prípravy v tejto oblasti do vzdelávacích programov, a zároveň by mladým ľuďom vrátane osôb žijúcich v znevýhodnených regiónoch, ako sú ostrovy, riedko osídlené, vidiecke a vzdialené oblasti, zabezpečila prístup k učňovskej príprave a stážam. Je dôležité, aby cieľom takejto spolupráce bolo prilákať viac žien a dievčat do tohto odboru a prispievať k riešeniu rodových rozdielov vo vede, technológii, inžinierstve a matematike a aby sa súkromný sektor zameral na poskytovanie odbornej prípravy na pracovisku zameranej na zručnosti, ktoré sú najžiadanejšie, a to so zapojením verejnej správy a startupov, ako aj MSP, vrátane mikropodnikov. Takisto je dôležité, aby poskytovatelia a členské štáty spolupracovali a prispievali k zberu údajov o situácii a vývoji na trhu práce v oblasti kybernetickej bezpečnosti.

(13) Agentúra ENISA zohráva významnú úlohu pri príprave kandidátskych európskych schém certifikácie kybernetickej bezpečnosti. Komisia by pri príprave návrhu všeobecného rozpočtu Únie mala posúdiť potrebné rozpočtové zdroje pre plán pracovných miest agentúry ENISA v súlade s postupom stanoveným v článku 29 nariadenia (EÚ) 2019/881.

(14) V tomto nariadení sa stanovujú cielené zmeny nariadenia (EÚ) 2019/881 s cieľom umožniť zavádzanie európskych schém certifikácie kybernetickej bezpečnosti pre riadené bezpečnostné služby. Zároveň sa v ňom špecifikujú a objasňujú určité ustanovenia uvedeného nariadenia týkajúce sa prípravy a fungovania všetkých európskych schém certifikácie kybernetickej bezpečnosti s cieľom zabezpečiť ich transparentnosť a otvorenosť. Týmito zmenami, ktoré sa obmedzujú na spresnenie alebo objasnenie nariadenia (EÚ) 2019/881, najmä zmenami týkajúcimi sa informácií, ktoré má agentúra ENISA poskytovať pri prenose kandidátskej schémy, ad hoc pracovných skupín zriadených pre každú kandidátsku schému a informácií a konzultácií v súvislosti s európskymi schémami certifikácie kybernetickej bezpečnosti, by v žiadnom prípade nemalo byť dotknuté širšie hodnotenie a preskúmanie uvedeného nariadenia podľa článku 67 uvedeného nariadenia, najmä hodnotenia vplyvu, účinnosti a efektívnosti hlavy uvedeného nariadenia týkajúcej sa európskeho rámca certifikácie kybernetickej bezpečnosti. Hodnotenie a preskúmanie týkajúce sa uvedenej hlavy by mali vychádzať zo širokej konzultácie so zainteresovanými stranami a úplnej a dôkladnej analýzy príslušných postupov.

(15) Keďže cieľ tohto nariadenia, a to umožniť zavedenie európskych schém certifikácie kybernetickej bezpečnosti pre riadené bezpečnostné služby, nie je možné uspokojivo dosiahnuť na úrovni členských štátov, ale z dôvodov jeho rozsahu a účinkov ho možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej Únii. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie tohto cieľa.

(16) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([9]) sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal svoje stanovisko 10. januára 2024,

PRIJALI TOTO NARIADENIE:

Článok 1

Zmeny nariadenia (EÚ) 2019/881

Nariadenie (EÚ) 2019/881 sa mení takto:

1. V článku 1 ods. 1 prvom pododseku sa písmeno b) nahrádza takto:

„b) rámec pre zavádzanie európskych schém certifikácie kybernetickej bezpečnosti na zabezpečenie primeranej úrovne kybernetickej bezpečnosti produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb v Únii, ako aj na predídenie fragmentácii vnútorného trhu z hľadiska schém certifikácie kybernetickej bezpečnosti v Únii.“

2. Článok 2 sa mení takto:

a) Body 9, 10 a 11 sa nahrádzajú takto:

„9. ‚európska schéma certifikácie kybernetickej bezpečnosti‘ je komplexný súbor pravidiel, technických požiadaviek, noriem a postupov, ktoré sú stanovené na úrovni Únie a ktoré sa uplatňujú na certifikáciu alebo posudzovanie zhody konkrétnych produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb;

10. ‚vnútroštátna schéma certifikácie kybernetickej bezpečnosti‘ je komplexný súbor pravidiel, technických požiadaviek, noriem a postupov vypracovaných a prijatých vnútroštátnym orgánom verejnej moci a uplatňovaných pri certifikácii alebo posudzovaní zhody produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb v rozsahu pôsobnosti príslušnej schémy;

11. ‚európsky certifikát kybernetickej bezpečnosti‘ je dokument, ktorý vydal príslušný orgán a ktorým sa potvrdzuje, že daný produkt IKT, služba IKT, proces IKT alebo riadená bezpečnostná služba boli predmetom hodnotenia, pokiaľ ide o súlad s konkrétnymi bezpečnostnými požiadavkami stanovenými v európskej schéme certifikácie kybernetickej bezpečnosti;“.

b) Vkladá sa tento bod:

„14a. ‚riadená bezpečnostná služba‘ je služba poskytovaná tretej strane, ktorej predmetom je vykonávanie činností súvisiacich s riadením rizika kybernetickej bezpečnosti alebo poskytovanie pomoci pri týchto činnostiach, ako je riešenie incidentu, penetračné testovanie, bezpečnostné audity a konzultácie vrátane odborného poradenstva súvisiaceho s technickou podporou;“.

c) Body 20, 21 a 22 sa nahrádzajú takto:

„20. ‚technická špecifikácia‘ je dokument, v ktorom sa predpisujú technické požiadavky, ktoré musí spĺňať produkt IKT, služba IKT, proces IKT alebo riadená bezpečnostná služba, alebo postupy posudzovania zhody týkajúce sa produktu IKT, služby IKT, procesu IKT alebo riadenej bezpečnostnej služby;

([9]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

21. ‚úroveň záruky' je základ pre presvedčenie, že produkt IKT, služba IKT, proces IKT alebo riadená bezpečnostná služba spĺňa bezpečnostné požiadavky konkrétnej európskej schémy certifikácie kybernetickej bezpečnosti a uvádza úroveň, na akej sa produkt IKT, služba IKT, proces IKT alebo riadená bezpečnostná služba hodnotili, ale ako taký nemeria bezpečnosť produktu IKT, služby IKT, procesu IKT alebo riadenej bezpečnostnej služby;

22. ‚posúdenie zhody samohodnotením' je činnosť vykonávaná výrobcom alebo poskytovateľom/dodávateľom produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb, ktorou sa hodnotí, či tieto produkty IKT, služby IKT, procesy IKT alebo riadené bezpečnostné služby spĺňajú požiadavky konkrétnej európskej schémy certifikácie kybernetickej bezpečnosti."

3. V článku 4 sa odsek 6 nahrádza takto:

„6. Agentúra ENISA presadzuje používanie európskej certifikácie kybernetickej bezpečnosti, aby predišla fragmentácii vnútorného trhu. Agentúra ENISA prispieva k zriadeniu a udržiavaniu európskeho rámca certifikácie kybernetickej bezpečnosti v súlade s hlavou III tohto nariadenia, aby sa posilnila transparentnosť kybernetickej bezpečnosti produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb, a tým sa posilnila dôvera v digitálny vnútorný trh a jeho konkurencieschopnosť."

4. Článok 8 sa mení takto:

a) Odsek 1 sa mení takto:

i) úvodná časť sa nahrádza takto:

„1. Agentúra ENISA podporuje a presadzuje tvorbu a vykonávanie politiky Únie v oblasti certifikácie kybernetickej bezpečnosti produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb v zmysle hlavy III tohto nariadenia, a to tak, že:";

ii) písmeno b) sa nahrádza takto:

„b) vypracúva kandidátske európske schémy certifikácie kybernetickej bezpečnosti (ďalej len ‚kandidátske schémy') produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb v súlade s článkom 49;".

b) Odsek 3 sa nahrádza takto:

„3. Agentúra ENISA zostavuje a uverejňuje usmernenia a vypracúva osvedčené postupy, ktoré sa týkajú požiadaviek kybernetickej bezpečnosti na produkty IKT, služby IKT, procesy IKT a riadené bezpečnostné služby, a to v spolupráci s vnútroštátnymi orgánmi pre certifikáciu kybernetickej bezpečnosti a s príslušným odvetvím formálnym, štandardizovaným a transparentným spôsobom."

c) Odsek 5 sa nahrádza takto:

„5. Agentúra ENISA uľahčuje zavádzanie a využívanie európskych i medzinárodných noriem v oblasti riadenia rizika a v oblasti bezpečnosti produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb."

5. Článok 46 sa nahrádza takto:

„*Článok 46*

Európsky rámec certifikácie kybernetickej bezpečnosti

1. V záujme vytvorenia digitálneho jednotného trhu s produktmi IKT, službami IKT, procesmi IKT a riadenými bezpečnostnými službami sa zriadi európsky rámec certifikácie kybernetickej bezpečnosti s cieľom zlepšiť podmienky fungovania vnútorného trhu zvýšením úrovne kybernetickej bezpečnosti v Únii a umožnením harmonizovaného prístupu na úrovni Únie k európskym schémam certifikácie kybernetickej bezpečnosti.

2. Európskym rámcom certifikácie kybernetickej bezpečnosti sa zabezpečuje mechanizmus zavádzania európskych schém certifikácie kybernetickej bezpečnosti a osvedčovania, že produkty IKT, služby IKT a procesy IKT vyhodnotené v súlade s týmito schémami spĺňajú špecifikované bezpečnostné požiadavky s cieľom chrániť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo funkcií či služieb, ktoré tieto produkty, služby a procesy poskytujú alebo sprístupňujú, a to počas ich celého životného cyklu. Ďalej sa ním

osvedčuje, že riadené bezpečnostné služby vyhodnotené v súlade s takýmito schémami spĺňajú špecifikované bezpečnostné požiadavky s cieľom chrániť dostupnosť, pravosť, integritu a dôvernosť údajov, ktoré sa sprístupňujú, spracúvajú, uchovávajú alebo prenášajú v súvislosti s poskytovaním týchto služieb, a že tieto služby sa nepretržite poskytujú s využitím požadovaných zručností, odborných znalostí a skúseností zamestnancov, ktorí majú dostatočnú a primeranú úroveň relevantných technických vedomostí a profesijnej bezúhonnosti.“

6. Článok 47 sa mení takto:

a) Odsek 2 sa nahrádza takto:

„2. Priebežný pracovný program Únie obsahuje najmä zoznam produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb alebo ich kategórií, ktoré sú spôsobilé mať prospech zo zahrnutia do rozsahu pôsobnosti európskej schémy certifikácie kybernetickej bezpečnosti.“

b) Odsek 3 sa mení takto:

i) úvodná časť sa nahrádza takto:

„3. Zahrnutie konkrétneho produktu IKT, služby IKT, procesu IKT alebo riadených bezpečnostných služieb alebo ich kategórií do priebežného pracovného programu Únie sa zakladá na jednom či viacerých z týchto dôvodov:“;

ii) písmeno a) sa nahrádza takto:

„a) dostupnosť a rozvoj vnútroštátnych schém certifikácie kybernetickej bezpečnosti, ktoré sa vzťahujú na konkrétnu kategóriu produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb, a najmä pokiaľ ide o riziko fragmentácie;“

iii) vkladá sa toto písmeno:

„ca) technologický vývoj a dostupnosť a rozvoj medzinárodných schém certifikácie kybernetickej bezpečnosti a medzinárodných a priemyselných noriem;“.

7. Článok 49 sa mení takto:

a) Odseky 1 až 4 sa nahrádzajú takto:

„1. Na žiadosť Komisie podľa článku 48 vypracuje agentúra ENISA kandidátsku schému, ktorá spĺňa platné požiadavky stanovené v článkoch 51, 51a, 52 a 54.

2. Na žiadosť ECCG podľa článku 48 ods. 2 môže agentúra ENISA vypracovať kandidátsku schému, ktorá spĺňa platné požiadavky stanovené v článkoch 51, 51a, 52 a 54. Ak agentúra ENISA takúto žiadosť zamietne, musí toto zamietnutie odôvodniť. Každé rozhodnutie o zamietnutí takejto žiadosti prijíma správna rada.

3. Keď agentúra ENISA vypracúva kandidátsku schému, vedie včas so všetkými príslušnými zainteresovanými stranami formálne, otvorené, transparentné a inkluzívne konzultácie. Agentúra ENISA pri zasielaní kandidátskej schémy Komisii podľa odseku 6 poskytne informácie o spôsobe, akým dosiahla súlad s týmto odsekom.

4. Pre každú kandidátsku schému agentúra ENISA zriadi ad hoc pracovnú skupinu v súlade s článkom 20 ods. 4, ktorej účelom je poskytovať agentúre ENISA špecifické poradenstvo a odborné znalosti. Uvedené ad hoc pracovné skupiny v príslušných prípadoch a bez toho, aby boli dotknuté postupy a diskrečná právomoc stanovené v článku 20 ods. 4, zahŕňajú expertov z verejnej správy členských štátov, inštitúcií, orgánov, úradov a agentúr Únie a súkromného sektora.“

b) Odsek 7 sa nahrádza takto:

„7. Komisia môže na základe kandidátskej schémy pripravenej agentúrou ENISA prijať vykonávacie akty, v ktorých sa stanoví európsku schému certifikácie kybernetickej bezpečnosti produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb, ktorý spĺňa príslušné požiadavky stanovené v článkoch 51, 51a, 52 a 54. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 66 ods. 2.“

8. Vkladá sa tento článok:

„Článok 49a

Informácie a konzultácie týkajúce sa európskych schém certifikácie kybernetickej bezpečnosti

1. Komisia zverejní informácie o svojej žiadosti adresovanej agentúre ENISA, aby vypracovala kandidátsku schému alebo preskúmala existujúcu európsku schému certifikácie kybernetickej bezpečnosti uvedenú v článku 48.

2. Počas prípravy kandidátskej schémy agentúrou ENISA podľa článku 49 môže Európsky parlament, Rada alebo obaja požiadať Komisiu ako predsedu ECCG a agentúru ENISA, aby štvrťročne predkladali relevantné informácie o návrhu kandidátskej schémy. Na žiadosť Európskeho parlamentu alebo Rady môže agentúra ENISA po dohode s Komisiou a bez toho, aby bol dotknutý článok 27, sprístupniť Európskemu parlamentu a Rade príslušné časti návrhu kandidátskej schémy spôsobom, ktorý je primeraný požadovanej úrovni dôvernosti, a v prípade potreby obmedzeným spôsobom.

3. S cieľom posilniť dialóg medzi inštitúciami Únie a prispieť k formálnemu, otvorenému, transparentnému a inkluzívnemu konzultačnému procesu môže Európsky parlament, Rada alebo obaja vyzvať Komisiu a agentúru ENISA, aby prediskutovali záležitosti týkajúce sa fungovania európskych schém certifikácie kybernetickej bezpečnosti produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb.

4. Komisia pri hodnotení tohto nariadenia podľa článku 67 vo vhodných prípadoch zohľadní prvky vyplývajúce zo stanovísk Európskeho parlamentu a Rady k záležitostiam uvedeným v odseku 3 tohto článku.“

9. Článok 51 sa mení takto:

a) Názov sa nahrádza takto:

„Bezpečnostné ciele európskych schém certifikácie kybernetickej bezpečnosti pre produkty IKT, služby IKT a procesy IKT“.

b) Úvodná veta sa nahrádza takto:

„Európska schéma certifikácie kybernetickej bezpečnosti pre produkty IKT, služby IKT alebo procesy IKT musí byť navrhnutá tak, aby podľa potreby splnila aspoň tieto bezpečnostné ciele:“.

10. Vkladá sa tento článok:

„Článok 51a

Bezpečnostné ciele európskych schém certifikácie kybernetickej bezpečnosti pre riadené bezpečnostné služby

Európska schéma certifikácie kybernetickej bezpečnosti pre riadené bezpečnostné služby musí byť navrhnutý tak, aby podľa potreby splnil aspoň tieto bezpečnostné ciele:

a) aby riadené bezpečnostné služby boli poskytované s využitím požadovaných zručností, odborných znalostí a skúseností vrátane toho, aby zamestnanci zodpovední za poskytovanie uvedených služieb mali dostatočnú a primeranú úroveň technických vedomostí a zručností v danej konkrétnej oblasti, dostatočné a primerané skúsenosti a najvyšší stupeň profesijnej bezúhonnosti;

b) aby mal poskytovateľ zavedené vhodné interné postupy zabezpečujúce poskytovanie riadených bezpečnostných služieb vždy na dostatočnej a primeranej úrovni kvality;

c) aby sa údaje, ktoré sa sprístupňujú, uchovávajú, prenášajú alebo inak spracúvajú v súvislosti s poskytovaním riadených bezpečnostných služieb, chránili pred náhodným alebo neoprávneným prístupom, ukladaním, zverejnením, zničením, iným spracovaním alebo stratou, zmenou či nedostatočnou dostupnosťou;

d) aby bola v prípade fyzického alebo technického incidentu včas obnovená dostupnosť údajov, služieb a funkcií a prístup k nim;

e) aby oprávnené osoby, programy alebo zariadenia mali prístup výlučne k tým údajom, službám alebo funkciám, na ktoré sa vzťahujú ich prístupové práva;

f) aby sa uchovával záznam a bol k dispozícii na posudzovanie údajov, služieb alebo funkcií, ktoré boli predmetom prístupu, použité alebo inak spracúvané, kedy a kým;

g) aby produkty IKT, služby IKT a procesy IKT , ktoré sa používajú pri poskytovaní riadených bezpečnostných služieb, boli bezpečné už v štádiu návrhu a štandardne a aby prípadne obsahovali najnovšie bezpečnostné aktualizácie a neobsahovali verejne známe zraniteľnosti.“

11. Článok 52 sa mení takto:

a) Odsek 1 sa nahrádza takto:

„1. Európska schéma certifikácie kybernetickej bezpečnosti môže uvádzať jednu alebo viacero z týchto úrovní záruky pre produkty IKT, služby IKT, procesy IKT a riadené bezpečnostné služby: ‚základná‘, ‚významná‘ alebo ‚vysoká‘. Úroveň záruky zodpovedá úrovni rizika spojeného s plánovaným využívaním daného produktu IKT, služby IKT, procesu IKT alebo riadenej bezpečnostnej služby z hľadiska pravdepodobnosti a vplyvu incidentu.“

b) Odsek 3 sa nahrádza takto:

„3. Bezpečnostné požiadavky zodpovedajúce každej úrovni záruky sa uvádzajú v príslušnej európskej schéme certifikácie kybernetickej bezpečnosti vrátane zodpovedajúcich bezpečnostných funkcií a zodpovedajúcej prísnosti a hĺbky hodnotenia, ktorým má produkt IKT, služba IKT, proces IKT alebo riadená bezpečnostná služba prejsť.“

c) Odseky 5, 6 a 7 sa nahrádzajú takto:

„5. Európsky certifikát kybernetickej bezpečnosti alebo EÚ vyhlásenie o zhode, v ktorom sa odkazuje na úroveň záruky ‚základný‘, poskytuje uistenie, že produkty IKT, služby IKT, procesy IKT alebo riadené bezpečnostné služby, pre ktoré je vydaný uvedený certifikát alebo uvedené EÚ vyhlásenie o zhode, spĺňajú zodpovedajúce bezpečnostné požiadavky vrátane bezpečnostných funkcií a že boli hodnotené na úrovni určenej na minimalizovanie známych základných rizík incidentov a kybernetických útokov. Hodnotiace činnosti, ktoré sa majú vykonať, zahŕňajú aspoň preskúmanie technickej dokumentácie. V prípade, keď takéto preskúmanie nie je vhodné, vykonajú sa náhradné hodnotiace činnosti s rovnocenným účinkom.

6. Európsky certifikát kybernetickej bezpečnosti, v ktorom sa odkazuje na úroveň záruky ‚významná‘, poskytuje uistenie, že produkty IKT, služby IKT, procesy IKT alebo riadené bezpečnostné služby, pre ktoré je vydaný uvedený certifikát, spĺňajú zodpovedajúce bezpečnostné požiadavky vrátane bezpečnostných funkcií a že boli hodnotené na úrovni určenej na minimalizovanie známych kybernetickobezpečnostných rizík a rizík incidentov a kybernetických útokov, ktoré vykonávajú subjekty s obmedzenými zručnosťami a zdrojmi. Hodnotiace činnosti, ktoré sa majú vykonať, zahŕňajú aspoň: preskúmanie na preukázanie neexistencie verejne známych zraniteľností a skúšku na preukázanie, že produkty IKT, služby IKT, procesy IKT alebo riadené bezpečnostné služby správne plnia potrebné bezpečnostné funkcie. V prípade, keď takéto hodnotiace činnosti nie sú vhodné, vykonajú sa náhradné hodnotiace činnosti s rovnocenným účinkom.

7. Európsky certifikát kybernetickej bezpečnosti, v ktorom sa odkazuje na úroveň záruky ‚vysoký‘, poskytuje uistenie, že produkty IKT, služby IKT, procesy IKT alebo riadené bezpečnostné služby, pre ktoré je vydaný uvedený certifikát, spĺňajú zodpovedajúce bezpečnostné požiadavky vrátane bezpečnostných funkcií a že boli hodnotené na úrovni určenej na minimalizovanie rizika najpokročilejších kybernetických útokov, ktoré vykonávajú subjekty so značnými zručnosťami a zdrojmi. Hodnotiace činnosti, ktoré sa majú vykonať, zahŕňajú aspoň: Hodnotiace činnosti, ktoré sa majú vykonať, zahŕňajú aspoň: skúšku na preukázanie, že produkty IKT, služby IKT, procesy IKT alebo riadené bezpečnostné služby správne plnia najpokročilejšie potrebné bezpečnostné funkcie a posúdenie ich odolnosti proti zručným útočníkom prostredníctvom penetračného testovania. V prípade, keď takéto hodnotiace činnosti nie sú vhodné, vykonajú sa náhradné hodnotiace činnosti s rovnocenným účinkom.“

12. V článku 53 sa odseky 1, 2 a 3 nahrádzajú takto:

„1. Európska schéma certifikácie kybernetickej bezpečnosti môže povoliť posúdenie zhody samohodnotením, za ktoré nesie výhradnú zodpovednosť výrobca alebo poskytovateľ produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb. Posúdenie zhody samohodnotením je povolené iba v súvislosti s produktmi IKT, službami IKT, procesmi IKT alebo riadenými bezpečnostnými službami, ktoré predstavujú nízke riziko zodpovedajúce úrovni záruky ‚základný'.

2. Výrobca alebo poskytovateľ/dodávateľ produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb môže vydať EÚ vyhlásenie o zhode, ktorým potvrdí, že sa preukázalo splnenie požiadaviek stanovených v schéme. Vydaním takéhoto vyhlásenia preberá výrobca alebo poskytovateľ/dodávateľ produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb zodpovednosť za súlad produktu IKT, služby IKT, procesu IKT alebo riadenej bezpečnostnej služby s požiadavkami stanovenými v uvedenej schéme.

3. Výrobca alebo poskytovateľ/dodávateľ produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb uchováva EÚ vyhlásenie o zhode, technickú dokumentáciu a všetky ďalšie relevantné informácie, ktoré sa týkajú zhody produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb so schémou, k dispozícii pre vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti vymedzený podľa článku 58 počas obdobia stanoveného v príslušnej európskej schéme certifikácie kybernetickej bezpečnosti. Kópia EÚ vyhlásenia o zhode sa predloží vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti a agentúre ENISA."

13. V článku 54 sa odsek 1 mení takto:

a) Písmeno a) sa nahrádza takto:

„a) predmet úpravy a rozsah pôsobnosti danej certifikačnej schémy vrátane typu alebo kategórií produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb, na ktoré sa vzťahuje;".

b) Písmeno g) sa nahrádza takto:

„g) konkrétne hodnotiace kritériá a metódy, ktoré sa majú použiť, vrátane typov hodnotenia, s cieľom preukázať, že sa dosiahli platné bezpečnostné ciele uvedené v článkoch 51 a 51a;".

c) Písmeno j) sa nahrádza takto:

„j) pravidlá monitorovania súladu produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb s požiadavkami európskych certifikátov kybernetickej bezpečnosti alebo EÚ vyhlásení o zhode vrátane mechanizmov na preukázanie trvalého súladu so stanovenými požiadavkami kybernetickej bezpečnosti;".

d) Písmeno l) sa nahrádza takto:

„l) pravidlá týkajúce sa dôsledkov pre produkty IKT, služby IKT, procesy IKT alebo riadené bezpečnostné služby, ktoré boli certifikované alebo pre ktoré bolo vydané EÚ vyhlásenie o zhode, ale ktoré nespĺňajú požiadavky schémy;".

e) Písmeno o) sa nahrádza takto:

„o) určenie vnútroštátnych alebo medzinárodných schém certifikácie kybernetickej bezpečnosti, ktoré sa vzťahujú na rovnaký typ alebo kategóriu produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb, bezpečnostných požiadaviek, kritérií a metód hodnotenia a úrovní záruky;".

f) Písmeno q) sa nahrádza takto:

„q) obdobie, počas ktorého výrobca alebo poskytovateľ/dodávateľ produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb má uchovávať k dispozícii EÚ vyhlásenie o zhode, technickú dokumentáciu a všetky ďalšie relevantné informácie;".

14. Článok 56 sa mení takto:

a) Odsek 1 sa nahrádza takto:

„1. Produkty IKT, služby IKT, procesy IKT a riadené bezpečnostné služby certifikované v rámci európskej schémy certifikácie kybernetickej bezpečnosti prijatej podľa článku 49 sa považujú za vyhovujúce požiadavkám danej schémy."

b) Odsek 3 sa mení takto:

i) prvý pododsek sa nahrádza takto:

„Komisia pravidelne posúdi účinnosť a využívanie prijatých európskych schém certifikácie kybernetickej bezpečnosti a či sa niektorá konkrétna európska schéma certifikácie kybernetickej bezpečnosti má stať záväzným prostredníctvom príslušného práva Únie s cieľom zaistiť primeranú úroveň kybernetickej bezpečnosti produktov IKT, služieb IKT, procesov IKT a od 4. februára 2025 riadených bezpečnostných služieb v Únii a zlepšiť fungovanie vnútorného trhu. Prvé takéto posúdenie sa vykoná do 31. decembra 2023 a následné posúdenia sa potom vykonávajú aspoň každé dva roky. Komisia na základe výsledkov uvedených posúdení určí produkty IKT, služby IKT, procesy IKT a riadené bezpečnostné služby, na ktoré sa vzťahuje existujúca certifikačná schéma a na ktoré sa má vzťahovať povinná certifikačná schéma.“;

ii) tretí pododsek sa mení takto:

— písmeno a) sa nahrádza takto:

„a) zohľadní vplyv opatrení na výrobcov alebo poskytovateľov/dodávateľov takýchto produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb a na užívateľov z hľadiska nákladov uvedených opatrení a spoločenských alebo ekonomických prínosov vyplývajúcich z predpokladanej zvýšenej úrovne bezpečnosti cielených produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb;“,

— písmeno d) sa nahrádza takto:

„d) zohľadní všetky lehoty na vykonávanie, prechodné opatrenia a obdobia, najmä s ohľadom na možný vplyv daného opatrenia na výrobcov alebo poskytovateľov/dodávateľov produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb vrátane osobitných záujmov a potrieb malých a stredných podnikov, vrátane mikropodnikov;“.

c) Odseky 7 a 8 sa nahrádzajú takto:

„7. Fyzická či právnická osoba, ktorá predkladá produkty IKT, služby IKT, procesy IKT alebo riadené bezpečnostné služby na certifikáciu, sprístupní vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti vymedzenému podľa článku 58, ak tento orgán vydáva európsky certifikát kybernetickej bezpečnosti, alebo orgánu posudzovania zhody uvedenému v článku 60 všetky informácie potrebné pre certifikáciu.

8. Držiteľ európskeho certifikátu kybernetickej bezpečnosti informuje orgán uvedený v odseku 7 o všetkých následne zistených zraniteľnostiach alebo nezrovnalostiach týkajúcich sa bezpečnosti certifikovaného produktu IKT, služby IKT, procesu IKT alebo riadenej bezpečnostnej služby, ktoré môžu mať vplyv na ich súlad s požiadavkami týkajúcimi sa certifikácie. Uvedený orgán bez zbytočného odkladu postúpi uvedené informácie dotknutému vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti.“

15. V článku 57 sa odseky 1 a 2 nahrádzajú takto:

„1. Bez toho, aby bol dotknutý odsek 3 tohto článku, vnútroštátne schémy certifikácie kybernetickej bezpečnosti a súvisiace postupy týkajúce sa produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb, na ktoré sa vzťahuje európska schéma certifikácie kybernetickej bezpečnosti, strácajú účinnosť k dátumu stanovenému vo vykonávacom akte prijatom podľa článku 49 ods. 7. Vnútroštátne schémy certifikácie kybernetickej bezpečnosti a súvisiace postupy týkajúce sa produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb, na ktoré sa európska schéma certifikácie kybernetickej bezpečnosti nevzťahuje, existujú naďalej.

2. Členské štáty nezavedú nové vnútroštátne schémy certifikácie kybernetickej bezpečnosti produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb, na ktoré sa už vzťahuje platná európska schéma certifikácie kybernetickej bezpečnosti.“

16. Článok 58 sa mení takto:

a) Odsek 7 sa mení takto:

i) písmená a) a b) sa nahrádzajú takto:

„a) dozerajú nad pravidlami uvedenými v európskych schémach certifikácie kybernetickej bezpečnosti podľa článku 54 ods. 1 písm. j), ktoré sa týkajú monitorovania súladu produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb s požiadavkami európskych certifikátov kybernetickej bezpečnosti, ktoré boli vydané na ich príslušných územiach, a tieto pravidlá presadzujú, a to v spolupráci s ďalšími príslušnými orgánmi dohľadu nad trhom;

b) monitorujú dodržiavanie povinností výrobcov alebo poskytovateľov/dodávateľov produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb, ktorí sú usadení na ich príslušných územiach a vykonávajú posúdenie zhody samohodnotením, a tieto povinnosti presadzujú, a najmä monitorujú dodržiavanie povinností takýchto výrobcov alebo poskytovateľov/dodávateľov stanovených v článku 53 ods. 2 a 3 a v príslušnej európskej schéme certifikácie kybernetickej bezpečnosti, a tieto povinnosti presadzujú;“

ii) písmeno h) sa nahrádza takto:

„h) spolupracujú s inými vnútroštátnymi orgánmi pre certifikáciu kybernetickej bezpečnosti alebo inými orgánmi verejnej moci, čo zahŕňa poskytovanie informácií o možnom nesúlade produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb s požiadavkami tohto nariadenia alebo s požiadavkami konkrétnych európskych schém certifikácie kybernetickej bezpečnosti; a“.

b) Odsek 9 sa nahrádza takto:

„9. Vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti navzájom i s Komisiou spolupracujú, najmä si vymieňajú informácie, skúsenosti a osvedčené postupy, pokiaľ ide o certifikáciu kybernetickej bezpečnosti a technické otázky súvisiace s kybernetickou bezpečnosťou produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb.“

17. V článku 59 ods. 3 sa písmená b) a c) nahrádzajú takto:

„b) postupy dozoru a presadzovania pravidiel monitorovania súladu produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb s európskymi certifikátmi kybernetickej bezpečnosti podľa článku 58 ods. 7 písm. a);

c) postupy monitorovania a presadzovania povinností výrobcov a poskytovateľov/dodávateľov produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb podľa článku 58 ods. 7 písm. b);“.

18. V článku 67 sa odseky 2 a 3 nahrádzajú takto:

„2. V hodnotení sa zároveň posúdi vplyv, účinnosť a efektívnosť ustanovení hlavy III tohto nariadenia vrátane postupov vedúcich k prijatiu európskych schém certifikácie kybernetickej bezpečnosti a ich dátových základní, a to z hľadiska cieľov zabezpečiť primeranú úroveň kybernetickej bezpečnosti produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb v Únii a zlepšiť fungovanie vnútorného trhu.

3. V hodnotení sa posúdi, či sú základné požiadavky kybernetickej bezpečnosti na prístup na vnútorný trh potrebné na to, aby sa zabránilo vstupu produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb, ktoré nespĺňajú základné požiadavky kybernetickej bezpečnosti, na vnútorný trh.“

19. Príloha sa mení v súlade s prílohou k tomuto nariadeniu.

Článok 2

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 19. decembra 2024

Za Európsky parlament	*Za Radu*
predsedníčka	*predseda*
R. METSOLA	BÓKA J.

PRÍLOHA

Príloha k nariadeniu (EÚ) 2019/881 sa mení takto:

1. Body 2 až 5 sa nahrádzajú takto:

„2. Orgán posudzovania zhody je orgánom tretej strany, ktorá je nezávislá od organizácie alebo produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb, ktoré posudzuje.

3. Za orgán posudzovania zhody možno považovať subjekt, ktorý patrí do obchodného alebo profesijného združenia, ktoré zastupuje podniky, ktoré sa podieľajú na navrhovaní, produkcii, poskytovaní, inštalácii, používaní alebo údržbe produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb, ktoré tento subjekt posudzuje, ak sa preukáže jeho nezávislosť a absencia konfliktu záujmov.

4. Orgány posudzovania zhody, ich vrcholový manažment a osoby zodpovedné za výkon úloh posudzovania zhody nesmú byť návrhármi, výrobcami, dodávateľmi, subjektmi, ktoré vykonávajú inštaláciu alebo údržbu, obstarávateľmi, vlastníkmi ani užívateľmi posudzovaného produktu IKT, služby IKT, procesu IKT alebo riadenej bezpečnostnej služby, ani splnomocnenými zástupcami žiadnej z uvedených strán. Uvedený zákaz nevylučuje používanie posudzovaných produktov IKT, ktoré sú potrebné na vykonávanie činností orgánu posudzovania zhody, ani používanie takých produktov IKT na osobné účely.

5. Orgány posudzovania zhody, ich vrcholový manažment a osoby zodpovedné za vykonávanie úloh posudzovania zhody sa nesmú priamo podieľať na navrhovaní, zhotovovaní alebo výrobe, dodávaní alebo poskytovaní, marketingu, inštalácii, používaní alebo údržbe posudzovaných produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb, ani zastupovať strany, ktoré sa na takýchto činnostiach podieľajú. Orgány posudzovania zhody, ich vrcholový manažment a osoby zodpovedné za vykonávanie úloh posudzovania zhody sa nesmú podieľať na žiadnych činnostiach, ktoré môžu ovplyvniť ich nezávislý úsudok alebo bezúhonnosť v súvislosti s ich činnosťami posudzovania zhody. Uvedený zákaz sa vzťahuje najmä na poradenské služby.“

2. Bod 10 sa mení takto:

a) Úvodná časť sa nahrádza takto:

„10. Orgán posudzovania zhody má neustále, pre každý postup posudzovania zhody a pre každý druh a každú kategóriu alebo podkategóriu produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb v potrebnej miere k dispozícii:“.

b) Písmeno c) sa nahrádza takto:

„c) postupy na výkon činností, ktorými sa náležite zohľadňuje veľkosť každého podniku, odvetvie, v ktorom podnik pôsobí, jeho štruktúra, stupeň zložitosti technológie daného produktu IKT, služby IKT, procesu IKT alebo riadenej bezpečnostnej služby a hromadný či sériový charakter produkčného procesu.“

3. Body 19 a 20 sa nahrádzajú takto:

„19. Orgány posudzovania zhody spĺňajú požiadavky príslušnej harmonizovanej normy v zmysle vymedzenia v článku 2 bode 9 nariadenia (ES) č. 765/2008 pre akreditáciu orgánov posudzovania zhody, ktoré vykonávajú certifikáciu produktov IKT, služieb IKT, procesov IKT alebo riadených bezpečnostných služieb.

20. Orgány posudzovania zhody zabezpečia, aby skúšobné laboratóriá používané na účely posudzovania zhody spĺňali požiadavky príslušnej harmonizovanej normy v zmysle vymedzenia v článku 2 bode 9 nariadenia (ES) č. 765/2008 pre akreditáciu laboratórií, ktoré vykonávajú skúšky.“

V súvislosti s týmto aktom bolo urobené vyhlásenie, ktoré možno nájsť v Ú. v. EÚ C, 2025/307, 15.1.2024, ELI: http://data.europa.eu/eli/C/2025/307/oj.