16.4.2024 A9-0307/ 001-001

MÓDOSÍTÁSOK 001-001
előterjesztette: Ipari, Kutatási és Energiaügyi Bizottság

Jelentés
Josianne Cutajar **A9-0307/2023**
Irányított biztonsági szolgáltatások

Rendeleti javaslat (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Módosítás 1

AZ EURÓPAI PARLAMENT MÓDOSÍTÁSAI*

a Bizottság javaslatához

2023/0108 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

az (EU) 2019/881 rendeletnek az irányított biztonsági szolgáltatások tekintetében történő módosításáról

(EGT-vonatkozású szöveg)

* Módosítások: az új vagy módosított szöveget félkövér dőlt betűtípus, a törléseket pedig a ▌ jel mutatja.

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 114. cikkére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére[1],

tekintettel a Régiók Bizottsága véleményére,

rendes jogalkotási eljárás keretében[2],

---

[1] ***HL C 349., 2023.9.29., 167. o.***

[2] ***Az Európai Parlament ...-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács ...-i határozata.***

mivel:

(1) Az (EU) 2019/881 európai parlamenti és tanácsi rendelet[1] meghatározza az európai kiberbiztonsági tanúsítási rendszerek létrehozásának keretrendszerét ***az információs és kommunikációs technológiai (IKT)*** termékek, az IKT-szolgáltatások és az IKT-folyamatok megfelelő kiberbiztonsági szintjének az Unióban történő biztosítása céljából, valamint abból a célból, hogy megakadályozza a belső piac széttagoltságát az Unión belüli kiberbiztonsági tanúsítási rendszerek tekintetében.

(1a) Az Unió kibertámadásokkal szembeni rezilienciájának biztosítása és az uniós piac sebezhetőségének megelőzése érdekében ez a rendelet az irányított kiberbiztonsági szolgáltatásokra, azok alkalmazására és megbízhatóságára vonatkozó alapvető követelményeket meghatározó (EU) .../... európai parlamenti és tanácsi rendelettel[2] összhangban kiegészíti a horizontális szabályozási keretet, és átfogó kiberbiztonsági követelményeket állapít meg a digitális elemeket tartalmazó valamennyi termékre vonatkozóan.

(2) Az irányított biztonsági szolgáltatások, azaz az ügyfeleik kiberbiztonsági kockázatkezelésével kapcsolatos tevékenységek végzéséből – ***többek között a biztonsági események felderítéséből, az azokra való reagálásból vagy az azokat követő helyreállításból*** – vagy az azokhoz nyújtott segítségből álló szolgáltatások egyre nagyobb jelentőségre tesznek szert a kiberbiztonsági események megelőzése és hatásaik mérséklése terén. ***Az irányított biztonsági szolgáltatásokat nyújtó szolgáltatók tevékenységei a megelőzéssel, az azonosítással, a védelemmel, a felderítéssel, az elemzéssel, a visszaszorítással, a reagálással és a helyreállítással kapcsolatos szolgáltatásokból állnak, beleértve többek között a kiberfenyegetésekkel kapcsolatos hírszerzés biztosítását, a fenyegetettség proaktív technikák – például a beépített biztonság – révén történő nyomon követését, a kockázatértékelést, a kiterjesztett felderítést, helyreállítást és reagálást.*** Ennek megfelelően az említett szolgáltatások nyújtói az (EU) 2022/2555 európai parlamenti

---

1 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).

2 Az Európai Parlament és a Tanács (EU) […] rendelete [...] (HL ...).

és tanácsi irányelv[1] értelmében kiemelten kritikus ágazathoz tartozó alapvető vagy fontos szervezeteknek minősülnek. Az említett irányelv (86) preambulumbekezdésének megfelelően az irányított biztonsági szolgáltatók olyan területeken, mint az eseményekre való reagálás, behatolási tesztek, biztonsági auditok és tanácsadás, különösen fontos szerepet töltenek be abban, hogy segítsék a szervezeteket az események megelőzésében, észlelésében, az azokra való reagálásban, vagy az eseményt követően a működés helyreállításában. Azonban maguk az irányított biztonsági szolgáltatók is kibertámadások célpontjai, és az ügyfeleik működésébe való szoros integrációjuk miatt különös kockázatot jelentenek. Az (EU) 2022/2555 irányelv értelmében vett alapvető és fontos szervezeteknek ezért fokozott gondossággal kell eljárniuk az irányított biztonsági szolgáltató kiválasztása során.

(3) Az irányított biztonsági szolgáltatók emellett fontos szerepet játszanak az uniós kiberbiztonsági tartalékban is, amelynek fokozatos létrehozását [a kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról szóló] (EU) .../... rendelet támogatja. Az uniós kiberbiztonsági tartalékot a jelentős és nagyszabású kiberbiztonsági események kezelését és az azokat követő azonnali helyreállítást célzó intézkedések támogatására kell felhasználni. [A kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról szóló] (EU) .../... rendelet meghatározza az uniós kiberbiztonsági tartalékot alkotó szolgáltatók kiválasztási eljárását, amelynek többek között figyelembe kell vennie, hogy az érintett szolgáltató rendelkezik-e európai vagy nemzeti kiberbiztonsági tanúsítással. A megbízható szolgáltatók által [a kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról szóló]

[1] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (HL L 333., 2022.12.27., 80. o.).

(EU) .../... rendelet szerint nyújtott releváns szolgáltatások megfelelnek az e rendelet szerinti irányított biztonsági szolgáltatásoknak.

(4) Az irányított biztonsági szolgáltatások tanúsítása nemcsak az uniós kiberbiztonsági tartalék kiválasztási eljárása szempontjából releváns, hanem az ilyen szolgáltatásokat vásárolni szándékozó magán- és állami szervezetek számára is alapvető minőségi mutató. Tekintettel az irányított biztonsági szolgáltatások kritikus jellegére és az általuk kezelt adatok érzékenységére, a tanúsítás fontos iránymutatást és bizonyosságot nyújthat a potenciális ügyfelek számára e szolgáltatások megbízhatóságáról. Az irányított biztonsági szolgáltatásokra vonatkozó európai tanúsítási rendszerek hozzájárulnak az egységes piac széttagoltságának megakadályozásához. E rendelet célja ezért a belső piac működésének javítása.

(4a) Az irányított biztonsági szolgáltatások európai tanúsítási rendszereinek e szolgáltatások elterjedéséhez és fokozott versenyhez kell vezetniük, figyelembe véve mind a szolgáltatók, mind a kedvezményezettek sajátos igényeit. E rendszereknek ezért egyensúlyt kell teremteniük célkitűzésük és a szolgáltatók, különösen a mikrovállalkozások vagy a kis- és középvállalkozások (kkv-k) lehetséges szabályozási, adminisztratív és pénzügyi terhei között. Emellett a rendszereknek ösztönözniük kell a tanúsított, irányított biztonsági szolgáltatások igénybevételét azáltal, hogy hozzájárulnak azok hozzáférhetőségéhez, különösen a kisebb szereplők, például a mikrovállalkozások és a kkv-k, valamint a korlátozott kapacitással és erőforrásokkal rendelkező helyi és regionális önkormányzatok számára, amelyeknél azonban nagyobb valószínűséggel fordulnak elő pénzügyi, jogi, reputációs és működési következményekkel járó kiberbiztonsági incidensek.

(4b) Az irányított biztonsági szolgáltatások uniós tanúsítási rendszerének biztosítania kell a biztonságos digitális átállást garantáló és a digitális évtized szakpolitikai programban meghatározott célok eléréséhez hozzájáruló biztonságos és magas színvonalú szolgáltatások rendelkezésre állását, különös tekintettel arra a célra, hogy az uniós vállalkozások 75%-a kezdje használni a számítási felhőt/MI-t/nagy adathalmazokat, hogy a mikrovállalkozások és a kkv-k több mint 90%-a elérje legalább az alapszintű digitális intenzitást, és hogy a kulcsfontosságú közszolgáltatásokat online kínálják.

(4c) A jelenlegi gyorsan fejlődő digitális és technológiai környezetben az oktatási segédanyagok és a formális képzések kínálata eltérő, és az ismeretek különböző módokon szerezhetők meg, formálisan, például egyetemeken vagy tanfolyamokon keresztül, illetve nem formálisan, például az adott területen szerzett munkahelyi képzések vagy hosszú távú munkatapasztalatok révén.

(5) Az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok igénybevételén túlmutatóan az irányított biztonsági szolgáltatások gyakran olyan szolgáltatási funkciókat is biztosítanak, amelyek személyzetük szakmai felkészültségére, szakértelmére és tapasztalatára támaszkodnak. A rendkívül magas szintű szakmai felkészültségnek, szakértelemnek és tapasztalatnak, valamint a megfelelő belső eljárásoknak a biztonsági célkitűzések részét kell képezniük a kiemelkedően magas színvonalú irányított biztonsági szolgáltatások biztosítása érdekében. Annak biztosítása érdekében, hogy az irányított biztonsági szolgáltatások minden szempontból egy ***külön*** tanúsítási rendszer hatálya alá tartozzanak, módosítani kell az (EU) 2019/881 rendeletet. ***Az e rendelet alapján létrehozott tanúsítási rendszerek kidolgozása során figyelembe kell venni az e rendeletben előírt értékelés és felülvizsgálat eredményeit és ajánlásait.***

(5a) A megbízható uniós piac növekedésének elősegítése, valamint a hasonló gondolkodású harmadik országokkal való partnerségek létrehozása érdekében – többek között az (EU).../... európai parlamenti és tanácsi rendeletnek[1] (2023/0109(COD)) az uniós kiberbiztonsági tartalékhoz való hozzáférésre vonatkozó rendelkezéseire figyelemmel – egyszerűsíteni kell az e rendelettel létrehozott keretrendszerben kialakított tanúsítási eljárást a nemzetközi elismertség és a nemzetközi szabványokkal való összhang biztosítása érdekében.

(5b) Az irányított biztonsági szolgáltatások megbízható uniós piacának kialakítása érdekében a szolgáltatóknak és a tagállamoknak együtt kell működniük és hozzá kell járulniuk a kiberbiztonsági munkaerőpiac helyzetére és alakulására vonatkozó adatok gyűjtéséhez.

(5c) A kritikus infrastruktúrák rezilienciájának megerősítésére irányuló, Unió-szerte összehangolt megközelítés a tagállamok kapacitásépítésén alapul. Az Unió

---

1 Az Európai Parlament és a Tanács (EU) […] rendelete [...] (HL...).

azonban szakemberhiánnyal küzd, mivel hiány mutatkozik a képzett szakemberek terén, miközben gyorsan változó fenyegetettségi helyzettel néz szembe, amint azt a Kiberbiztonsági Készségek Akadémiájáról szóló, 2023. április 18-i bizottsági közlemény is elismeri. Ezért a magas színvonalú, alapvető irányított biztonsági szolgáltatások megjelenésének elősegítése és az uniós kiberbiztonsági munkaerő összetételének jobb áttekintése érdekében meg kell erősíteni a tagállamok, a Bizottság, az ENISA és az érdekelt felek – többek között a magánszektor és a tudományos élet – közötti együttműködést a köz- és magánszféra közötti partnerségek kialakítása, a kutatási és innovációs kezdeményezések támogatása, a közös szabványok kidolgozása és kölcsönös elismerése, valamint a kiberbiztonsági készségek tanúsítása révén, többek között a kiberbiztonsági készségek európai keretrendszerén keresztül. Ez várhatóan megkönnyíti a kiberbiztonsági szakemberek Unión belüli mobilitását, valamint a kiberbiztonsági ismereteknek és képzéseknek az oktatási programokba való integrálását, miközben biztosítja a tanulószerződéses gyakorlati képzésekhez és szakmai gyakorlatokhoz való hozzáférést a fiatalok, köztük a hátrányos helyzetű régiókban, például szigeteken, ritkán lakott, vidéki és távoli területeken élők számára. Ezeknek az intézkedéseknek arra is törekedniük kell, hogy több nőt és lányt vonzzanak a területre, és hozzájáruljanak a nemek közötti szakadék kezeléséhez a tudomány, a technológia, a műszaki tudományok és a matematika terén. A magánszektornak arra is törekednie kell, hogy munkahelyi képzést nyújtson a leginkább keresett készségekkel kapcsolatban, bevonva a közigazgatást és az induló vállalkozásokat, valamint a mikrovállalkozásokat és a kkv-kat is.

(5d) ***Megfelelő finanszírozást és erőforrásokat kell biztosítani az (EU) 2019/881 rendelet e rendelettel bevezetett módosításai által az ENISA-ra ruházott további feladatokhoz.***

(5e) ***E rendelet egyes nem alapvető elemeinek kiegészítése érdekében a Bizottságot fel kell hatalmazni arra, hogy az Európai Unió működéséről szóló szerződés 290. cikkének megfelelően jogi aktusokat fogadjon el abból a célból, hogy létrehozza az IKT-termékekre, az IKT-szolgáltatásokra, az IKT-folyamatokra és az irányított biztonsági szolgáltatásokra vonatkozó európai kiberbiztonsági tanúsítási rendszert. Különösen fontos, hogy a Bizottság az előkészítő munkája során megfelelő***

konzultációkat folytasson, többek között szakértői szinten is, és hogy e konzultációkra a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban[1] megállapított elvekkel összhangban kerüljön sor. Így különösen a felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlament és a Tanács a tagállamok szakértőivel egyidejűleg kap kézhez minden dokumentumot, és szakértőik rendszeresen részt vehetnek a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein.

(5e) Az európai adatvédelmi biztossal az (EU) 2018/1725 európai parlamenti és tanácsi rendelet 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos [ÉÉÉÉ/HH/NN]-án/-én véleményt nyilvánított[2],

ELFOGADTA EZT A RENDELETET:

---

1 ***HL L 123, 2016.5.12., 1. o.***

2 ***HL C …, ... o.***

1. cikk

Az (EU) 2019/881 rendelet módosításai

Az (EU) 2019/881 rendelet a következőképpen módosul:

1. Az 1. cikk (1) bekezdése első albekezdésének b) pontja helyébe a következő szöveg lép:

„b) az európai kiberbiztonsági tanúsítási rendszerek létrehozásának keretrendszerét az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok és az irányított biztonsági szolgáltatások megfelelő kiberbiztonsági szintjének az Unóban történő biztosítása céljából, valamint abból a célból, hogy megakadályozza a belső piac széttagoltságát az Unión belüli kiberbiztonsági tanúsítási rendszerek tekintetében.”

2. A 2. cikk a következőképpen módosul:

a) a 9., 10. és 11. pont helyébe a következő szöveg lép:

„9. »európai kiberbiztonsági tanúsítási rendszer«: adott IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások tanúsítására vagy megfelelőségértékelésére alkalmazandó szabályok, műszaki követelmények, szabványok és eljárások uniós szinten meghatározott átfogó rendszere;

10. »nemzeti kiberbiztonsági tanúsítási rendszer«: az adott tanúsítási rendszer hatálya alá tartozó IKT-termékek, IKT-szolgáltatások, IKT-folyamatok és irányított biztonsági szolgáltatások tanúsítására vagy megfelelőségértékelésére alkalmazandó, valamely nemzeti hatóság által kidolgozott és elfogadott szabályok, műszaki követelmények, szabványok és eljárások átfogó rendszere;

11. »európai kiberbiztonsági tanúsítvány«: az illetékes szerv által kibocsátott dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás, IKT-folyamat vagy irányított biztonsági szolgáltatás esetében értékelték, hogy megfelel-e valamely európai kiberbiztonsági tanúsítási rendszer konkrét biztonsági követelményeinek;”

b) a szöveg a következő ponttal egészül ki:

„14a. »irányított biztonsági szolgáltatás«: ***harmadik félnek nyújtott*** kiberbiztonsági kockázatkezeléssel kapcsolatos tevékenységek végzéséből vagy az azokhoz nyújtott segítségből ***vagy tanácsadásból*** álló szolgáltatás, beleértve ***a biztonsági események kezelését,*** a behatolási teszteket, a biztonsági auditokat és tanácsadást is;”

c) a 20., 21. és 22. pont helyébe a következő szöveg lép:

„20. »műszaki előírások«: olyan dokumentum, amely megadja, hogy valamely IKT-terméknek, IKT-szolgáltatásnak, IKT-folyamatnak vagy irányított biztonsági szolgáltatásnak milyen műszaki követelményeket kell teljesítenie vagy arra milyen megfelelőségértékelési eljárások vonatkoznak;

21. »megbízhatósági szint«: az az iránti bizalom alapja, hogy valamely IKT-termék, IKT-szolgáltatás, IKT-folyamat vagy irányított biztonsági szolgáltatás teljesíti egy adott európai kiberbiztonsági tanúsítási rendszer biztonsági követelményeit, megmutatja, hogy valamely IKT-terméket, IKT-szolgáltatást, IKT-folyamatot vagy irányított biztonsági szolgáltatást milyen szinten értékeltek, de a megbízhatósági szint nem méri az érintett IKT-termék, IKT-szolgáltatás, IKT-folyamat vagy irányított biztonsági szolgáltatás biztonságát;

22. »megfelelőségi önértékelés«: az IKT-termékek, IKT-szolgáltatások,IKT-folyamatok vagy irányított biztonsági szolgáltatások gyártói vagy szolgáltatói által végzett olyan tevékenység, amely értékeli, hogy az adott IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások teljesítik-e egy adott európai kiberbiztonsági tanúsítási rendszer biztonsági követelményeit.”***;***

3. A 4. cikk (6) bekezdésének helyébe a következő szöveg lép:

„6. Az ENISA-nak elő kell mozdítania az európai kiberbiztonsági tanúsítás használatát a belső piac széttagoltságának elkerülése érdekében. Az ENISA-nak hozzá kell járulnia egy európai kiberbiztonsági tanúsítási keretrendszernek az e rendelet III. címével összhangban történő létrehozásához és fenntartásához, annak érdekében, hogy a kiberbiztonság tekintetében

átláthatóbbá váljon, hogy mennyire megbízhatóak az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok és az irányított biztonsági szolgáltatások, megerősítve ezzel a digitális belső piacba és annak versenyképességébe vetett bizalmat.”

4. Az 8. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„1. Az ENISA-nak támogatnia kell és elő kell mozdítania az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok és az irányított biztonsági szolgáltatások e rendelet III. címében meghatározott kiberbiztonsági tanúsítására vonatkozó uniós szakpolitika kidolgozását és végrehajtását, az alábbiak révén:

a) a kapcsolódó területeken folytatott szabványosítás fejleményeinek folyamatos nyomon követése és az európai kiberbiztonsági tanúsítási rendszerek fejlesztéséhez használandó megfelelő műszaki előírásokra vonatkozó ajánlások az 54. cikk (1) bekezdésének c) pontja alapján az olyan esetekre, amikor nem állnak rendelkezésre szabványok;

b) javaslati európai kiberbiztonsági tanúsítási rendszerek (a továbbiakban: javasolt tanúsítási rendszerek) kidolgozása IKT-termékekre, IKT-szolgáltatásokra, IKT-folyamatokra és irányított biztonsági szolgáltatásokra vonatkozóan a 49. cikkel összhangban;

c) az elfogadott európai kiberbiztonsági tanúsítási rendszerek értékelése a 49. cikk (8) bekezdésével összhangban;

d) részvétel az 59. cikk (4) bekezdése szerinti kölcsönös felülvizsgálatban;

e) a Bizottság támogatása az európai kiberbiztonsági tanúsítási csoport titkárságának a 62. cikk (5) bekezdése alapján történő biztosításában.”;

b) a (3) bekezdés helyébe a következő szöveg lép:

„3. Az ENISA-nak az IKT-termékek, az IKT-szolgáltatások, az IKT-

folyamatok és az irányított biztonsági szolgáltatások kiberbiztonsági követelményeire vonatkozó iránymutatásokat kell összeállítania és közzétennie, valamint bevált gyakorlatokat kialakítania, formális, strukturált és átlátható módon együttműködve a nemzeti kiberbiztonsági tanúsító hatóságokkal és az ágazattal.”;

c) a (5) bekezdés helyébe a következő szöveg lép:

„5. Az ENISA-nak elő kell segítenie a kockázatkezelésre és az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok és az irányított biztonsági szolgáltatások biztonságára vonatkozó európai és nemzetközi szabványok kidolgozását.”

5. A 46. cikk (1) és (2) bekezdésének helyébe a következő szöveg lép:

„1. Létrejön az európai kiberbiztonsági tanúsítási keretrendszer, annak érdekében, hogy az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok és az irányított biztonsági szolgáltatások digitális egységes piacának létrehozása céljából a kiberbiztonság szintjének az Unión belüli javítása és az európai kiberbiztonsági tanúsítási rendszerekre vonatkozó, uniós szinten összehangolt megközelítés lehetővé tétele útján javuljanak a belső piac működésének feltételei.

2. Az európai kiberbiztonsági tanúsítási keretrendszer meghatároz egy mechanizmust az európai kiberbiztonsági tanúsítási rendszerek létrehozására. A mechanizmus tanúsítja, hogy az e rendszerekkel összhangban értékelt IKT-termékek, IKT-szolgáltatások és IKT-folyamatok megfelelnek az adott biztonsági követelményeknek, az e termékek, szolgáltatások és folyamatok által tárolt vagy továbbított vagy kezelt adatok, vagy az általuk ellátott funkciók vagy kínált szolgáltatások rendelkezésre állásának, hitelességének, sértetlenségének vagy titkosságának azok teljes életciklusa alatti védelme céljából. Ezen túlmenően tanúsítja, hogy az említett rendszerekkel összhangban értékelt irányított biztonsági szolgáltatások megfelelnek az adott biztonsági követelményeknek az említett szolgáltatások nyújtásával összefüggésben hozzáférhető, kezelt, tárolt vagy továbbított adatok rendelkezésre állásának, hitelességének, sértetlenségének és titkosságának védelme céljából, és hogy az említett szolgáltatásokat folyamatosan a szükséges szakmai felkészültséggel,

szakértelemmel és tapasztalattal, továbbá rendkívül magas szintű releváns műszaki ismeretekkel és szakmai feddhetetlenséggel rendelkező személyzet nyújtja.”

6. Az 47. cikk (2) és (3) bekezdésének helyébe a következő szöveg lép:

„(2) Az uniós gördülő munkaprogramnak magában kell foglalnia különösen azon IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy ezek kategóriáinak, valamint azon irányított biztonsági szolgáltatások jegyzékét, amelyek alkalmasak arra, hogy valamely európai kiberbiztonsági tanúsítási rendszer hatálya alá vonják őket. ***Ezzel összefüggésben a Bizottság mélyreható értékelést készíthet a meglévő képzési pályákról az azonosított készséghiányok áthidalása érdekében, valamint javaslatot tehet a szakképzett munkaerő és a készségtípusok iránti igények kezelésére.***

(3) Bármely konkrét IKT-terméknek, IKT-szolgáltatásnak és IKT-folyamatnak vagy ezek kategóriáinak, valamint irányított biztonsági szolgáltatásnak az uniós gördülő munkaprogramban való szerepeltetését igazolni kell a következő indokok közül egy vagy több alapján:

a) olyan nemzeti kiberbiztonsági tanúsítási rendszerek rendelkezésre állása és kidolgozása, amelyek hatálya IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások egy konkrét kategóriájára kiterjed, különösen a széttagoltság veszélyére tekintettel;

b) vonatkozó uniós vagy tagállami jog vagy szakpolitikák;

c) piaci kereslet;

ca) a technológiai fejlődés, valamint a nemzetközi kiberbiztonsági tanúsítási rendszerek és a nemzetközi és ipari szabványok rendelkezésre állása és fejlesztése.

d) változások a kiberfenyegetettségi helyzetben;

e) az európai kiberbiztonsági tanúsítási csoport általi valamely konkrét rendszer javaslati szintű kidolgozására irányuló kérelem.”

7. Az 49. cikk ***a következőképpen módosul***:

a) a (7) bekezdés helyébe a következő szöveg lép:

„(7) A Bizottság ***felhatalmazást kap arra, hogy*** az ENISA által kidolgozott javasolt rendszer alapján ***a 65a. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el abból a célból, hogy kiegészítse ezt a rendeletet*** az IKT-termékekre, az IKT-szolgáltatásokra, az IKT-folyamatokra és az irányított biztonsági szolgáltatásokra vonatkozó, az 51., az 52. és az 54. cikkben meghatározott követelményeknek megfelelő európai kiberbiztonsági tanúsítási rendszerekről szóló rendelkezésekkel***.";***

b) a szöveg a következő bekezdéssel egészül ki:

„7a. Az ilyen felhatalmazáson alapuló jogi aktusok elfogadása előtt a Bizottság az ENISA-val együttműködve hatásvizsgálatot végez és tesz közzé a javasolt európai kiberbiztonsági tanúsítási rendszerről. A hatásvizsgálat elkészítése során a Bizottság nyilvános konzultációkat folytat és konzultál az SCCG-vel és az ECCG-vel.";

8. Az 51. cikk a következőképpen módosul:

a) a cím helyébe a következő szöveg lép:

„Az IKT-termékekre, IKT-szolgáltatásokra és IKT-folyamatokra vonatkozó európai kiberbiztonsági tanúsítási rendszerek biztonsági célkitűzései"

b) a bevezető mondat helyébe a következő szöveg lép:

„Az IKT-termékekre, IKT-szolgáltatásokra és IKT-folyamatokra vonatkozó európai kiberbiztonsági tanúsítási rendszereket úgy kell kialakítani, hogy – értelemszerűen – teljesítsék legalább az alábbi biztonsági célkitűzéseket:"***;***

9. A rendelet a következő cikkel egészül ki:

„Az irányított biztonsági szolgáltatásokra vonatkozó európai kiberbiztonsági tanúsítási rendszerek biztonsági célkitűzései

Az irányított biztonsági szolgáltatásokra vonatkozó európai kiberbiztonsági tanúsítási rendszereket úgy kell kialakítani, hogy – értelemszerűen – teljesítsék legalább az alábbi biztonsági célkitűzéseket:

a) annak biztosítása, hogy az irányított biztonsági szolgáltatásokat a szükséges szakmai felkészültséggel, szakértelemmel és tapasztalattal nyújtják, beleértve

azt is, hogy az e szolgáltatások nyújtásáért felelős személyzet az adott területen rendkívül magas szintű műszaki ismeretekkel és szakmai felkészültséggel, elegendő és megfelelő tapasztalattal, valamint a legmagasabb szintű szakmai feddhetetlenséggel rendelkezik;

b) annak biztosítása, hogy a szolgáltató megfelelő belső eljárásokkal rendelkezik annak biztosítására, hogy az irányított biztonsági szolgáltatások mindenkor rendkívül magas színvonalúak legyenek;

c) az irányított biztonsági szolgáltatások nyújtásával összefüggésben hozzáférhető, tárolt, továbbított vagy más módon kezelt adatok védelme a véletlenszerű vagy jogosulatlan hozzáféréssel, tárolással, nyilvánosságra hozatallal, megsemmisítéssel, egyéb kezeléssel, elvesztéssel, megváltoztatással vagy hozzáférhetetlenséggel szemben;

d) annak biztosítása, hogy fizikai vagy műszaki biztonsági esemény bekövetkeztekor az adatok, a szolgáltatások és a funkciók rendelkezésre állása, valamint az adatokhoz, a szolgáltatásokhoz és a funkciókhoz való hozzáférés mihamarabb helyreáll;

e) annak biztosítása, hogy a feljogosított személyek, programok vagy gépek kizárólag a hozzáférési jogaik tárgyát képező adatokhoz, szolgáltatásokhoz vagy funkciókhoz férhetnek hozzá;

f) annak nyilvántartása és megállapíthatóvá tétele, hogy ki, mikor és mely adatokat, szolgáltatásokat vagy funkciókat vette igénybe, használt vagy egyéb módon kezelt;

g) annak biztosítása, hogy az irányított biztonsági szolgáltatások nyújtása során alkalmazott IKT-termékek, IKT-szolgáltatások és IKT-folyamatok [és hardverek] alapértelmezetten és tervezetten biztonságosak, ***és naprakész szoftverrel és hardverrel vannak ellátva,*** esetükben nem állnak fenn közismert sebezhetőségek, és tartalmazzák a legújabb biztonsági frissítéseket.

10. Az 52. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) Az európai kiberbiztonsági tanúsítási rendszerek az IKT-termékekre, az

IKT-szolgáltatásokra, az IKT-folyamatokra és az irányított biztonsági szolgáltatásokra a következő megbízhatósági szintek közül egy vagy több szintet határozhatnak meg. „alapvető”, „jelentős” és „magas”. A megbízhatósági szintnek a biztonsági események valószínűsége és hatása szempontjából arányban kell állnia az IKT-termék, az IKT-szolgáltatás, az IKT-folyamat vagy az irányított biztonsági szolgáltatás rendeltetés szerinti használatához kapcsolódó kockázat szintjével.”;

b) a (3) bekezdés helyébe a következő szöveg lép:

„(3) A releváns európai kiberbiztonsági tanúsítási rendszernek meg kell határoznia a minden egyes megbízhatósági szintnek megfelelő biztonsági követelményeket, ideértve a megfelelő biztonsági funkciókat és az IKT-termékre, az IKT-szolgáltatásra, az IKT-folyamatra vagy az irányított biztonsági szolgáltatásra alkalmazandó értékelés megfelelő szigorúságát és mélységét.”;

c) az (5), (6) és (7) bekezdés helyébe a következő szöveg lép:

„(5) Az „alap” megbízhatósági szintet feltüntető európai kiberbiztonsági tanúsítvány vagy uniós megfelelőségi nyilatkozat arra vonatkozóan szolgál biztosítékkal, hogy azok az IKT-termékek, IKT-szolgáltatások, IKT-folyamatok és irányított biztonsági szolgáltatások, amelyekre vonatkozóan az említett tanúsítványt vagy az említett uniós megfelelőségi nyilatkozatot kibocsátották, teljesítik a vonatkozó biztonsági követelményeket – többek között a biztonsági funkciókat – és olyan szintű értékelésen estek át, amely a biztonsági eseményekkel és támadásokkal kapcsolatos alapvető, ismert kockázatok minimalizálására törekszik. Az elvégzendő értékelési tevékenységeknek magukban kell foglalniuk legalább a műszaki dokumentáció áttekintését. Ha az ilyen áttekintés nem megfelelő, egyenlő hatású helyettesítő értékelési tevékenységeket kell végezni.

(6) A »jelentős« megbízhatósági szintet feltüntető európai kiberbiztonsági tanúsítvány arra vonatkozóan szolgál biztosítékkal, hogy azok az IKT-termékek, IKT-szolgáltatások, IKT-folyamatok és irányított biztonsági szolgáltatások, amelyekre vonatkozóan az említett tanúsítványt

kibocsátották, teljesítik a vonatkozó biztonsági követelményeket – többek között a biztonsági funkciókat – és olyan szintű értékelésen estek át, amely az ismert kiberbiztonsági kockázatok, valamint a korlátozott szakértelemmel és erőforrásokkal rendelkező elkövetők által végrehajtott biztonsági események és kiberbiztonsági támadások minimalizálására törekszik. Az elvégzendő értékelési tevékenységeknek legalább az alábbiakat kell magukban foglalniuk: a közismert sebezhetőségek hiánya megállapításának felülvizsgálata és az annak megállapítására szolgáló tesztelés, hogy az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok vagy az irányított biztonsági szolgáltatások megfelelően működtetik-e a szükséges biztonsági funkciókat. Ha ezen értékelési tevékenységek egyike sem megfelelő, egyenlő hatású helyettesítő értékelési tevékenységeket kell végezni.

(7) A »magas« megbízhatósági szintet feltüntető európai kiberbiztonsági tanúsítvány arra vonatkozóan szolgál biztosítékkal, hogy azon IKT-termékek, IKT-szolgáltatások, IKT-folyamatok és irányított biztonsági szolgáltatások, amelyekre vonatkozóan az említett tanúsítványt kibocsátották, teljesítik a vonatkozó biztonsági követelményeket – többek között a biztonsági funkciókat – és olyan szintű értékelésen estek át, amely a jelentős szakértelemmel és erőforrásokkal rendelkező elkövetők által, a tudomány legutolsó állása szerinti technológiával végrehajtott kibertámadások minimalizálására törekszik. Az elvégzendő értékelési tevékenységeknek legalább az alábbiakat kell magukban foglalniuk: a közismert sebezhetőségek hiánya megállapításának felülvizsgálata; az annak megállapítására szolgáló tesztelés, hogy az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok vagy az irányított biztonsági szolgáltatások megfelelően, a legfejlettebb technika szerint működtetik-e a szükséges biztonsági funkciókat; valamint behatolásvizsgálatok révén annak értékelése, hogy azok mennyire ellenállóak a jól képzett elkövetők által végrehajtott támadásokkal szemben. Ha ezen értékelési tevékenységek egyike sem megfelelő, egyenlő hatású helyettesítő értékelési tevékenységeket kell végezni.”

11. Az 53. cikk (1), (2) és (3) bekezdése helyébe a következő szöveg lép:

„(1) Egy európai kiberbiztonsági tanúsítási rendszer lehetővé teheti, hogy az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok vagy az irányított biztonsági szolgáltatások gyártójának vagy nyújtójának kizárólagos felelőssége mellett megfelelőségi önértékelésre kerüljön sor. Megfelelőségi önértékelés csak az »alap« megbízhatósági szintnek megfelelő, alacsony kockázatot jelentő IKT-termékek, IKT-szolgáltatások, IKT-folyamatok és irányított biztonsági szolgáltatások esetében engedhető meg.

(2) Az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok vagy az irányított biztonsági szolgáltatások gyártója vagy nyújtója uniós megfelelőségi nyilatkozatot állíthat ki arról, hogy megtörtént annak bizonyítása, hogy a tanúsítási rendszer követelményei teljesülnek. E nyilatkozat kiállításával az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok vagy az irányított biztonsági szolgáltatások gyártója vagy nyújtója felelősséget vállal azért, hogy az IKT-termék, az IKT-szolgáltatás, az IKT-folyamat vagy az irányított biztonsági szolgáltatás megfelel az adott tanúsítási rendszer által előírt követelményeknek.

(3) Az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok vagy az irányított biztonsági szolgáltatások gyártójának vagy nyújtójának az alkalmazandó európai kiberbiztonsági tanúsítási rendszerben meghatározott ideig az 58. cikkben említett nemzeti kiberbiztonsági tanúsító hatóság rendelkezésére kell bocsátania az uniós megfelelőségi nyilatkozatot, a műszaki dokumentációt és az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok vagy az irányított biztonsági szolgáltatások tanúsítási rendszernek való megfelelésével kapcsolatos összes egyéb releváns információt. Az uniós megfelelőségi nyilatkozat másolati példányát meg kell küldeni a nemzeti kiberbiztonsági tanúsító hatóságnak és az ENISA-nak.”

12. Az 54. cikk (1) bekezdése a következőképpen módosul:

a) az a) pont helyébe a következő szöveg lép:

„a) a tanúsítási rendszer tárgya és hatálya, ideértve a hatálya alá tartozó IKT-termékek, IKT-szolgáltatások, IKT-folyamatok és irányított biztonsági

szolgáltatások típusát vagy kategóriáit;”

b) a j) pont helyébe a következő szöveg lép:

„j) az IKT-termékeknek, az IKT-szolgáltatásoknak, az IKT-folyamatoknak és az irányított biztonsági szolgáltatásoknak az európai kiberbiztonsági tanúsítványok vagy az uniós megfelelőségi nyilatkozatok követelményeinek való megfelelése nyomon követésének szabályai, ideértve a meghatározott kiberbiztonsági követelményeknek való folyamatos megfelelés bizonyítására szolgáló mechanizmusokat is;”

c) az l) pont helyébe a következő szöveg lép:

„l) az annak következményeire vonatkozó szabályok, ha a tanúsított vagy uniós megfelelőségi nyilatkozat hatálya alá tartozó IKT-termékek, IKT-szolgáltatások, IKT-folyamatok és irányított biztonsági szolgáltatások nem felelnek meg a tanúsítási rendszer követelményeinek;”

d) az o) pont helyébe a következő szöveg lép:

„o) az azonos típusú vagy kategóriájú IKT-termékekre, IKT-szolgáltatásokra, IKT-folyamatokra és irányított biztonsági szolgáltatásokra kiterjedő nemzeti vagy nemzetközi kiberbiztonsági tanúsítási rendszerek, biztonsági követelmények, értékelési kritériumok és módszerek, valamint megbízhatósági szintek azonosítása;”

e) a q) pont helyébe a következő szöveg lép:

„q) az uniós megfelelőségi nyilatkozatnak, a műszaki dokumentációnak, valamint minden egyéb releváns információnak az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok vagy az irányított biztonsági szolgáltatások gyártója vagy nyújtója általi rendelkezésre bocsátásának időtartama;”.

13. Az 56. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) A 49. cikk alapján elfogadott európai kiberbiztonsági tanúsítási rendszerek keretében tanúsított IKT-termékekről, IKT-szolgáltatásokról, IKT-folyamatokról és irányított biztonsági szolgáltatásokról vélelmezni

kell, hogy megfelelnek az e rendszerek által támasztott követelményeknek.”;

b) a (3) bekezdés a következőképpen módosul:

i. az első albekezdés helyébe a következő szöveg lép:

„A Bizottság az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok és az irányított biztonsági szolgáltatások Unión belüli megfelelő szintű kiberbiztonságának biztosítása és a belső piac működésének javítása érdekében rendszeresen értékeli az elfogadott európai kiberbiztonsági tanúsítási rendszerek hatékonyságát és alkalmazását, valamint azt, hogy valamely konkrét európai kiberbiztonsági rendszert a vonatkozó uniós jog útján kötelezővé kell-e tenni. Az első ilyen értékelést 2023. december 31-ig el kell végezni, az ezt követő értékeléseket pedig legalább kétévenként. A Bizottság az említett értékelés eredményeitől függően azonosítja a valamely létező tanúsítási rendszer hatálya alá tartozó azon IKT-termékeket, IKT-szolgáltatásokat, IKT-folyamatokat és irányított biztonsági szolgáltatásokat, amelyeket kötelező tanúsítási rendszer hatálya alá kell vonni.”;

ii. a harmadik albekezdés a következőképpen módosul:

aa) az a) pont helyébe a következő szöveg lép:

„a) figyelembe veszi az intézkedéseknek az ilyen IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások gyártóira vagy nyújtóira és a felhasználókra gyakorolt hatásait ezen intézkedések költségei, valamint a megcélzott IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások várható magasabb biztonsági szintjéből eredő társadalmi vagy gazdasági előnyök tekintetében;”

bb) a d) pont helyébe a következő szöveg lép:

„d) figyelembe veszi a végrehajtási határidőket, az átmeneti intézkedéseket és időszakokat, tekintettel különösen az

intézkedésnek az IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások gyártóira vagy szolgáltatóira gyakorolt lehetséges hatására, ***beleértve a mikrovállalkozások és a kkv-k sajátos érdekeit és igényeit is***;

iii. a szöveg a következő albekezdéssel egészül ki:

„E cikk harmadik albekezdésének d) pontja tekintetében a Bizottság megfelelő pénzügyi támogatást biztosít a meglévő uniós programok szabályozási keretében, különösen a mikrovállalkozások és a kkv-k – köztük az irányított biztonsági szolgáltatások területén tevékenykedő induló innovatív vállalkozások – pénzügyi terheinek enyhítése érdekében.”;

c) a (7) és a (8) bekezdés helyébe a következő szöveg lép:

„(7) Az IKT-termékeiket, IKT-szolgáltatásaikat, IKT-folyamataikat vagy irányított biztonsági szolgáltatásaikat tanúsítási mechanizmusnak alávető természetes vagy jogi személyek kötelesek az 58. cikkben említett nemzeti kiberbiztonsági tanúsító hatóság – amennyiben az európai kiberbiztonsági tanúsítványt e hatóság állította ki –, vagy a 60. cikkben említett megfelelőségértékelő szervezet rendelkezésére bocsátani a tanúsítás lefolytatásához szükséges összes információt.

(8) Az európai kiberbiztonsági tanúsítvány jogosultjának tájékoztatnia kell a (7) bekezdésben említett hatóságot vagy szervezetet minden olyan, a tanúsított IKT-termék, IKT-szolgáltatás, IKT-folyamat vagy irányított biztonsági szolgáltatás biztonságát érintő, utólag észlelt sebezhetőségről vagy rendellenességről, amely hatással lehet az említett termék, szolgáltatás vagy folyamat tanúsítással összefüggő követelményeknek való megfelelésére. Ez a hatóság vagy szervezet az említett információt köteles indokolatlan késedelem nélkül továbbítani az érintett nemzeti kiberbiztonsági tanúsító hatóságnak.”

14. Az 57. cikk (1) és (2) bekezdésének helyébe a következő szöveg lép:

„(1) E cikk (3) bekezdésének sérelme nélkül a nemzeti kiberbiztonsági tanúsítási

rendszerek és az IKT-termékekre, IKT-szolgáltatásokra, IKT-folyamatokra és irányított biztonsági szolgáltatásokra vonatkozó olyan kapcsolódó eljárások, amelyek egy európai kiberbiztonsági tanúsítási rendszer hatálya alá tartoznak, a 49. cikk (7) bekezdése alapján elfogadott felhatalmazáson alapuló jogi aktusban meghatározott időponttól nem bírnak joghatással. A nemzeti kiberbiztonsági tanúsítási rendszerek és az IKT-termékekre, IKT-szolgáltatásokra, IKT-folyamatokra és irányított biztonsági szolgáltatásokra vonatkozó olyan kapcsolódó eljárások, amelyek nem tartoznak egy európai kiberbiztonsági tanúsítási rendszer hatálya alá, továbbra is fennmaradnak.

(2) A tagállamok a már valamely hatályos európai kiberbiztonsági tanúsítási rendszer hatálya alá tartozó IKT-termékekre, IKT-szolgáltatásokra, IKT-folyamatokra és irányított biztonsági szolgáltatásokra nem vezethetnek be új nemzeti kiberbiztonsági tanúsítási rendszereket.”

15. Az 58. cikk a következőképpen módosul:

a) a (7) bekezdés a következőképpen módosul:

i. az a) és a b) pont helyébe a következő szöveg lép:

„a) más illetékes piacfelügyeleti hatóságokkal együttműködve felügyelik és betartatják az IKT-termékeknek, az IKT-szolgáltatásoknak, az IKT-folyamatoknak és az irányított biztonsági szolgáltatásoknak az illetékességi területükön kiadott európai kiberbiztonsági tanúsítványok követelményeinek való megfelelése nyomon követésére vonatkozó, az 54. cikk (1) bekezdésének j) pontja alapján az európai kiberbiztonsági tanúsítási rendszerekbe foglalt szabályokat;

b) betartatják az IKT-termékeknek, az IKT-szolgáltatásoknak, az IKT-folyamatoknak vagy az irányított biztonsági szolgáltatásoknak az illetékességi területükön letelepedett és megfelelőségi önértékelést végző gyártóira vagy nyújtóira vonatkozó kötelezettségeket és nyomon követik az azoknak való megfelelést, így különösen betartatják az 53. cikk (2) és (3) bekezdésében, valamint az alkalmazandó európai kiberbiztonsági tanúsítási rendszerben

megállapított, az említett gyártókra és szolgáltatókra vonatkozó kötelezettségeket és nyomon követik az azoknak való megfelelést;”

ii. a h) pont helyébe a következő szöveg lép:

„h) együttműködnek a többi nemzeti kiberbiztonsági tanúsító hatósággal és más hatóságokkal, többek között azáltal, hogy megosztják az azzal kapcsolatos információkat, ha bizonyos IKT-termékek, IKT-szolgáltatások, IKT-folyamatok és irányított biztonsági szolgáltatások nem felelnek meg e rendelet vagy egyes európai kiberbiztonsági tanúsítási rendszerek követelményeinek; és”;

b) a (9) bekezdés helyébe a következő szöveg lép:

„(9) A nemzeti kiberbiztonsági tanúsító hatóságoknak együtt kell működniük egymással és a Bizottsággal, különösen az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok és az irányított biztonsági szolgáltatások kiberbiztonságára vonatkozó kiberbiztonsági tanúsítással és műszaki kérdésekkel kapcsolatos információk, tapasztalatok és bevált gyakorlatok cseréje révén.”

16. Az 59. cikk (3) bekezdése b) és c) pontjának helyébe a következő szöveg lép:

„b) az IKT-termékek, IKT-szolgáltatások, IKT-folyamatok és irányított biztonsági szolgáltatások európai kiberbiztonsági tanúsítványoknak való megfelelésének nyomon követésére szolgáló szabályoknak az 58. cikk (7) bekezdésének a) pontja alapján történő felügyeletére és betartatására szolgáló eljárásokat;

c) az IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások gyártóira vagy nyújtóira vonatkozó kötelezettségeknek az 58. cikk (7) bekezdésének b) pontja alapján történő nyomon követésére és betartatására szolgáló eljárásokat;”

16a. A rendelet a következő cikkel egészül ki:

„65a. cikk

A felhatalmazás gyakorlása

(1) A felhatalmazáson alapuló jogi aktusok elfogadására vonatkozóan a

Bizottság részére adott felhatalmazás feltételeit ez a cikk határozza meg.

(2) A Bizottságnak a 49. cikk (7) bekezdése szerinti, felhatalmazáson alapuló jogi aktusok elfogadására vonatkozó felhatalmazása ötéves időtartamra szól [a módosított rendelet hatálybalépésének napja]-tól/-től kezdődő hatállyal. A Bizottság legkésőbb kilenc hónappal az ötéves időtartam letelte előtt jelentést készít a felhatalmazásról. A felhatalmazás hallgatólagosan meghosszabbodik a korábbival megegyező időtartamra, amennyiben az Európai Parlament vagy a Tanács nem ellenzi a meghosszabbítást legkésőbb három hónappal minden egyes időtartam letelte előtt.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja az 49. cikk (7) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az Európai Unió Hivatalos Lapjában való kihirdetését követő napon, vagy a benne megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

(4) A felhatalmazáson alapuló jogi aktus elfogadása előtt a Bizottság a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban megállapított elvekkel összhangban konzultál az egyes tagállamok által kijelölt szakértőkkel.

(5) A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul és egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.

(6) A 49. cikk (7a) bekezdése értelmében elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha az Európai Parlamentnek és a Tanácsnak a jogi aktusról való értesítését követő három hónapon belül sem az Európai Parlament, sem a Tanács nem emelt ellene kifogást, illetve ha az említett időtartam lejártát megelőzően mind az Európai Parlament, mind a Tanács arról tájékoztatta a Bizottságot, hogy nem fog kifogást emelni. Az Európai Parlament vagy a Tanács kezdeményezésére ez az időtartam két hónappal meghosszabbodik.;”

17. A 67. cikk helyébe a következő szöveg lép:

„67 cikk

Értékelés és felülvizsgálat

(1) A Bizottság 2024. június 28-ig, majd azt követően háromévente értékeli az ENISA és munkamódszerei hatását, eredményességét és hatékonyságát, hogy szükséges-e módosítani az ENISA megbízatását, hogy egy ilyen módosítás milyen pénzügyi vonzatokkal járna. Az értékelésben figyelembe kell venni minden olyan visszajelzést, amelyet az ENISA a tevékenységével kapcsolatban kapott. Amennyiben a Bizottság megítélése szerint az ENISA működése kitűzött céljai, megbízatása és feladatai tekintetében a továbbiakban nem indokolt, javasolhatja e rendeletnek az ENISA-ra vonatkozó rendelkezései tekintetében történő módosítását.

(2) Az értékelésben fel kell mérni az e rendelet III. címében foglalt rendelkezések hatását, eredményességét és hatékonyságát az IKT-termékek, az IKT-szolgáltatások, az IKT-folyamatok és az irányított biztonsági szolgáltatások Unión belüli megfelelő szintű kiberbiztonságának biztosítására és a belső piac működésének javítására vonatkozó célkitűzések tekintetében,

(3) A Bizottság a következőket is értékeli:

a) az európai kiberbiztonsági tanúsítási rendszerekről való konzultációhoz, valamint azok előkészítéséhez és elfogadásához vezető eljárások hatékonysága és eredményessége, továbbá ezen eljárások javításának és felgyorsításának módjai;

b) hogy szükség van-e alapvető kiberbiztonsági követelményekre a belső piachoz való hozzáférés tekintetében olyan IKT-termékek, IKT-szolgáltatások, IKT-folyamatok és irányított biztonsági szolgáltatások uniós piacra való belépésének megelőzése érdekében, amelyek nem felelnek meg az alapszintű kiberbiztonsági követelményeknek.

(4) A Bizottság az értékelésről szóló jelentést 2024. június 28-ig, majd azt követően háromévente következtetéseivel együtt megküldi az Európai Parlamentnek, a Tanácsnak, és az igazgatótanácsnak. A jelentés megállapításait közzé kell tenni.

2. cikk

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt ...,

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*