Az Európai Unió
Tanácsa

Brüsszel, 2023. április 21.
(OR. en)

8511/23

Intézményközi referenciaszám:
2023/0108 (COD)

CYBER 91
JAI 469
TELECOM 107
DATAPROTECT 109
MI 312
IND 180
CODEC 661

JAVASLAT

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2023. április 19.
Címzett:	Thérèse BLANCHET, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	COM(2023) 208 final
Tárgy:	Javaslat – AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az (EU) 2019/881 rendeletnek az irányított biztonsági szolgáltatások tekintetében történő módosításáról

Mellékelten továbbítjuk a delegációknak a COM(2023) 208 final számú dokumentumot.

Melléklet: COM(2023) 208 final

EURÓPAI
BIZOTTSÁG

Strasbourg, 2023.4.18.
COM(2023) 208 final

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)

INDOKOLÁS

1. A JAVASLAT HÁTTERE

• A javaslat indokai és céljai

Ez az indokolás az (EU) 2019/881 rendeletnek[1] az irányított biztonsági szolgáltatások tekintetében történő módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatot kíséri.

A javasolt célirányos módosítás célja, hogy bizottsági végrehajtási jogi aktusok révén a már a kiberbiztonsági jogszabály hatálya alá tartozó információs és technológiai termékeken (IKT-termékeken), IKT-szolgáltatásokon és IKT-folyamatokon kívül az „irányított biztonsági szolgáltatások” esetében is lehetővé tegye európai kiberbiztonsági tanúsítási rendszerek elfogadását. Az irányított biztonsági szolgáltatások egyre fontosabb szerepet játszanak a kiberbiztonsági események megelőzésében és hatásuk enyhítésében.

Az Európai Unió kiberbiztonsági helyzetének alakulásáról szóló, 2022. május 23-i következtetéseiben[2] a Tanács felszólította az Uniót és tagállamait, hogy fokozzák a kiberbiztonság általános szintjének javítását célzó erőfeszítéseiket, például a megbízható kiberbiztonsági szolgáltatók megjelenésének elősegítésével, és hangsúlyozta, hogy az EU kiberbiztonsági ágazati politikájában kiemelt helyen kell kezelni az ilyen szolgáltatók kiépülésének ösztönzését. A Tanács felkérte továbbá a Bizottságot, hogy tegyen javaslatot arra, hogy milyen módokon lehetne ösztönözni a megbízható kiberbiztonsági szolgáltatások iparágának megjelenését. Az irányított biztonsági szolgáltatások tanúsítása hatékony eszköz az említett szolgáltatások minőségébe vetett bizalom erősítéséhez, és ezáltal elősegíti a megbízható európai kiberbiztonsági szolgáltatások ágazatának kialakulását.

A Bizottság és a főképviselő által 2022. november 10-én „Az EU kibervédelmi politikája” címmel elfogadott közös közlemény[3] bejelentette, hogy a Bizottság fel fogja tárni az uniós szintű kiberbiztonsági tanúsítási rendszerek kialakítási lehetőségeit a kiberbiztonsági ipar és a magánvállalkozások tekintetében. Az irányított biztonsági szolgáltatók szintén fontos szerepet fognak játszani az uniós szintű kiberbiztonsági tartalékban, amelynek fokozatos létrehozását az e rendelettel párhuzamosan javasolt kiberszolidaritásról szóló jogszabály támogatja. Az uniós kiberbiztonsági tartalékot a jelentős és nagyszabású kiberbiztonsági események kezelését és az azokat követő azonnali helyreállítást célzó intézkedések támogatására kell felhasználni. A kiberszolidaritásról szóló jogszabályban említett „megbízható szolgáltatók” által nyújtott releváns kiberbiztonsági szolgáltatások megfelelnek az e javaslatban szereplő „irányított biztonsági szolgáltatásoknak”.

Egyes tagállamok már megkezdték az irányított biztonsági szolgáltatásokra vonatkozó nemzeti tanúsítási rendszerek elfogadását. Az Unió területén alkalmazott különböző kiberbiztonsági tanúsítási rendszerek miatt egyre nagyobb a kockázata annak, hogy az irányított biztonsági szolgáltatások belső piaca széttagolódik. Ez a javaslat a széttagoltság megelőzése érdekében lehetővé teszi az említett szolgáltatásokra vonatkozó európai kiberbiztonsági tanúsítási rendszerek létrehozását.

---

[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] 9364/22.

[3] JOIN(2022) 49 final.

- **Összhang a szabályozási terület jelenlegi rendelkezéseivel**

Ez a javaslat összhangban áll a kiberbiztonsági jogszabállyal, amelyet egyúttal módosít is. Az említett rendelet rendelkezéseire épül, és azokat úgy igazítja ki, hogy hatályuk az irányított biztonsági szolgáltatásokra is kiterjedjen. A javasolt módosítások a feltétlenül szükséges mértékre korlátozódnak, és nem változtatják meg a kiberbiztonsági jogszabály jellemzőit vagy működését.

A javaslat továbbá összhangban áll 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 szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvvel (NIS 2 irányelv)[4]. Az irányított biztonsági szolgáltatásokat nyújtó szolgáltatók az (EU) 2022/2555 irányelv értelmében kiemelten kritikus ágazathoz tartozó alapvető vagy fontos szervezeteknek minősülnek. Az említett irányelv (86) preambulumbekezdése megállapítja, hogy 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.

E javaslat célja az irányított biztonsági szolgáltatások minőségének javítása és összehasonlíthatóságuk növelése. Ezáltal lehetővé teszi az alapvető és fontos szervezetek számára, hogy az (EU) 2022/2555 irányelvben előírtaknak megfelelően fokozott gondossággal járjanak el az irányított biztonsági szolgáltató kiválasztása során. Ezenkívül a „irányított biztonsági szolgáltatások” e javaslatban szereplő fogalommeghatározása az (EU) 2022/2555 irányelvben szereplő „irányított biztonsági szolgáltatók” fogalommeghatározásából ered, és nagyon hasonló ahhoz. Ezért a javaslat nagy mértékben kiegészíti a NIS 2 irányelvet.

Végezetül ez a javaslat kiegészíti a kiberszolidaritásról szóló jogszabályjavaslatot. A kiberszolidaritásról szóló jogszabályjavaslat meghatározza az uniós szintű kiberbiztonsági tartalékot alkotó szolgáltatók kiválasztásának folyamatát, amelynek *többek között* figyelembe kell vennie, hogy az említett szolgáltatók rendelkeznek-e európai vagy nemzeti kiberbiztonsági tanúsítvánnyal. Az irányított biztonsági szolgáltatásokra vonatkozó jövőbeli tanúsítási rendszerek ezért jelentős szerepet fognak játszani a kiberszolidaritásról szóló jogszabály végrehajtásában.

- **Összhang az Unió egyéb szakpolitikáival**

Ez a javaslat nem érinti a kiberbiztonsági jogszabály és az (EU) 2016/679 rendelet (általános adatvédelmi rendelet)[5], valamint utóbbinak az adatkezelők és adatfeldolgozók által végzett adatkezelési műveletek e rendeletnek való megfelelését igazoló tanúsítási mechanizmusok, adatvédelmi bélyegzők, illetve jelölések létrehozására vonatkozó rendelkezései közötti összhangot. A kiberbiztonsági jogszabály változatlanul nem érinti az adatkezelési műveletek általános adatvédelmi rendelet szerinti tanúsítását, még akkor sem, ha az ilyen műveletek termékekbe és szolgáltatásokba vannak beágyazva.

[4] HL L 333., 2022.12.27., 80. o.
[5] HL L 119., 2016.5.4., 1. o.

Ez a javaslat továbbá nem érinti a kiberbiztonsági jogszabálynak az akkreditálás előírásainak megállapításáról szóló 765/2008/EK rendelettel[6] való összeegyeztethetőségét, különösen a nemzeti akkreditáló testületekre és megfelelőségértékelő szervezetekre, valamint a nemzeti tanúsításfelügyeleti hatóságokra vonatkozó keretrendszer tekintetében.

2. JOGALAP, SZUBSZIDIARITÁS ÉS ARÁNYOSSÁG

• Jogalap

Ez a javaslat módosítja a kiberbiztonsági jogszabályt, amely az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikkén alapul. A kiberbiztonsági jogszabályhoz hasonlóan e javaslatnak is célja a belső piac széttagoltságának elkerülése, nevezetesen azzal, hogy lehetővé teszi az irányított biztonsági szolgáltatásokra vonatkozó európai kiberbiztonsági tanúsítási rendszerek elfogadását. A tagállamok megkezdték az irányított biztonsági szolgáltatásokra vonatkozó nemzeti tanúsítási rendszerek elfogadását. Így fennáll a konkrét kockázata annak, hogy az említett szolgáltatások belső piaca széttagolódik, amit e javaslat kezelni kíván. Ezért az EUMSZ 114. cikke képezi e kezdeményezés releváns jogalapját.

• Szubszidiaritás (nem kizárólagos hatáskör esetén)

Az irányított biztonsági szolgáltatásokra vonatkozó európai kiberbiztonsági tanúsítási rendszerek elfogadásának lehetővé tételére és a belső piac széttagoltságának elkerülésére irányuló célkitűzés nem érhető el nemzeti szinten, és csak uniós szinten valósítható meg. Emellett a javasolt módosítás tárgyát képező irányított biztonsági szolgáltatásokat olyan szolgáltatók nyújtják, amelyek legnagyobb potenciális ügyfeleikhez hasonlóan az Unió egész területén működnek. Az uniós szintű fellépés ezért egyszerre szükséges és a nemzeti szintű fellépésnél hatékonyabb megoldás.

• Arányosság

A javaslat a kiberbiztonsági jogszabály célirányos módosítása. Célja eléréséhez a feltétlenül szükséges mértékre korlátozódik, nevezetesen arra, hogy az IKT-termékeken, az IKT-szolgáltatásokon és az IKT-folyamatokon kívül az irányított biztonsági szolgáltatásokra vonatkozó európai kiberbiztonsági tanúsítási rendszerek elfogadását is lehetővé tegye. A javasolt módosítás mindenekelőtt kiigazítja az európai kiberbiztonsági tanúsítási keretrendszer alkalmazási körét oly módon, hogy az magában foglalja a „irányított biztonsági szolgáltatásokat” is, tartalmazza az említett szolgáltatásoknak a NIS 2 irányelvvel összhangban álló fogalommeghatározását, valamint módosítja az európai kiberbiztonsági tanúsítás biztonsági célkitűzéseit annak érdekében, hogy azok igazodjanak az „irányított biztonsági szolgáltatásokhoz”. A többi módosítás technikai jellegű, és azt hivatott biztosítani, hogy a vonatkozó cikkek a „irányított biztonsági szolgáltatásokra” is kiterjedjenek. A javasolt kezdeményezés tehát arányos a célkitűzéssel.

• A jogi aktus típusának megválasztása

Mivel a javaslat az (EU) 2019/881 rendelet módosítására irányul, a megfelelő jogi eszköz a rendelet.

[6] HL L 218., 2008.8.13., 30. o.

3. AZ *UTÓLAGOS* ÉRTÉKELÉSEK, AZ ÉRDEKELT FELEKKEL FOLYTATOTT KONZULTÁCIÓK ÉS A HATÁSVIZSGÁLATOK EREDMÉNYEI

- **A jelenleg hatályban lévő jogszabályok *utólagos* értékelése / célravezetőségi vizsgálata**

Tárgytalan.

- **Az érdekelt felekkel folytatott konzultációk**

Célzott konzultációkra került sor a tagállamokkal és az ENISA-val. E konzultációk során a tagállamok ismertették az irányított biztonsági szolgáltatások tanúsításával kapcsolatos jelenlegi tevékenységeiket és meglátásaikat. Az ENISA kifejtette véleményét és ismertette a tagállamokkal és az érdekelt felekkel folytatott megbeszélések eredményeit. A tagállamoktól és az ENISA-tól kapott észrevételek és információk beépítésre kerültek a javaslatba.

- **Szakértői vélemények összegyűjtése és felhasználása**

Tárgytalan.

- **Hatásvizsgálat**

Hatásvizsgálatra nincs szükség, ezért annak elkészítése alól mentességet kértek, mivel a javaslat a kiberbiztonsági jogszabályt csak nagyon korlátozott mértékben és célzott módon módosítja. A javaslat felhatalmazná a Bizottságot arra, hogy végrehajtási jogi aktusok révén tanúsítási rendszereket fogadjon el az IKT-termékeken, az IKT-szolgáltatásokon és az IKT-folyamatokon kívül – amelyek már a jogi aktus hatálya alá tartoznak – az „irányított biztonsági szolgáltatásokra” vonatkozóan is. A javaslat értelmében a módosítás azonban csak akkor jár joghatással, amikor az említett tanúsítási rendszereket már – egy későbbi szakaszban – elfogadták. Ezenkívül a módosítás nem változtatná meg a tanúsítási rendszerek önkéntes jellegét.

- **Célravezető szabályozás és egyszerűsítés**

Tárgytalan.

- **Alapjogok**

A javaslatnak nincs semmilyen előrelátható hatása az alapjogok védelmére.

4. KÖLTSÉGVETÉSI VONZATOK

Nincsenek.

5. EGYÉB ELEMEK

- **Végrehajtási tervek, valamint a nyomon követés, az értékelés és a jelentéstétel szabályai**

A javaslat által módosítandó rendelkezések értékelésére a kiberbiztonsági jogszabálynak a jogszabály 67. cikkével összhangban a Bizottság által elvégzendő időszakos értékelése részeként kerül majd sor. Az értékelés egyebek mellett felméri a kiberbiztonsági tanúsítási keretrendszerre vonatkozó rendelkezések hatását, eredményességét és hatékonyságát az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok Unión belüli megfelelő szintű kiberbiztonságának biztosítására és a belső piac működésének javítására vonatkozó célkitűzések tekintetében is. A javaslat tartalmaz egy olyan módosítást, amely biztosítja, hogy

az értékelés az irányított biztonsági szolgáltatásokra is kiterjedjen. A Bizottság továbbá jelentést küld az értékelésről és következtetéseiről az Európai Parlamentnek, a Tanácsnak és az ENISA igazgatótanácsának, és nyilvánosságra hozza a jelentés megállapításait.

- **A javaslat egyes rendelkezéseinek részletes magyarázata**

A javaslat két cikket tartalmaz. Az 1. cikk az (EU) 2019/881 rendelet módosításait tartalmazza, a 2. cikk pedig a hatálybalépésre vonatkozik. Az 1. cikk célzott módosításokat tartalmaz a kiberbiztonsági jogszabályban foglalt európai kiberbiztonsági tanúsítási keretrendszer hatályának oly módon történő módosítása érdekében, hogy az kiterjedjen az „irányított biztonsági szolgáltatásokra” is (a kiberbiztonsági jogszabály 1. és 46. cikke). Tartalmazza az említett szolgáltatások fogalommeghatározását, amely nagyon közel áll a NIS 2 irányelv szerinti „irányított biztonsági szolgáltató” fogalommeghatározásához (a kiberbiztonsági jogszabály 2. cikke). Emellett egy új, 51a. cikkel egészíti ki a rendeletet, amely az európai kiberbiztonsági tanúsítás „irányított biztonsági szolgáltatásokhoz” igazított biztonsági célkitűzéseire vonatkozik. Végül a javaslat számos technikai módosítást tartalmaz annak biztosítása érdekében, hogy a vonatkozó cikkek az „irányított biztonsági szolgáltatásokra” is kiterjednek.

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)

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,

tekintettel a Régiók Bizottságának véleményére,

rendes jogalkotási eljárás keretében,

mivel:

(1) Az (EU) 2019/881 európai parlamenti és tanácsi rendelet[7] meghatározza az európai kiberbiztonsági tanúsítási rendszerek létrehozásának keretrendszerét az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok 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) Az irányított biztonsági szolgáltatások, azaz az ügyfeleik kiberbiztonsági kockázatkezelésével kapcsolatos tevékenységek végzéséből vagy az azokhoz nyújtott segítségből álló szolgáltatások egyre nagyobb jelentőségre tesznek szert a kiberbiztonsági események megelőzése és hatásaik mérséklése terén. Ennek megfelelően az említett szolgáltatások nyújtói az (EU) 2022/2555 európai parlamenti és tanácsi irányelv[8] 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

---

[7] 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.).

[8] 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.).

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] (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 átaluk 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.

(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 tanúsítási rendszer hatálya alá tartozzanak, módosítani kell az (EU) 2019/881 rendeletet.

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,

ELFOGADTA EZT A RENDELETET:

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 Unióban 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«: kiberbiztonsági kockázatkezeléssel kapcsolatos tevékenységek végzéséből vagy az azokhoz nyújtott segítségből álló szolgáltatás, beleértve a biztonsági eseményekre való reagálást, 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. A 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) az (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. A 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.

(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:

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;

d) változások a kiberfenyegetettségi helyzetben;

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

7. A 49. cikk (7) bekezdésének helyébe a következő szöveg lép:

„(7) A Bizottság az ENISA által kidolgozott javasolt rendszer alapján végrehajtási jogi aktusokat fogadhat el, amelyekben 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 rendelkezik. E végrehajtási jogi aktusokat a 66. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.”

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:

„51a. cikk

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, 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 az »alap«, a »jelentős« és a »magas« megbízhatósági szintek közül egy vagy több szintet határozhatnak meg. 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 – többek között a kkv-kra – gyakorolt lehetséges hatására;”

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 végrehajtási 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;"

17. A 67. cikk (2) és (3) bekezdésének helyébe a következő szöveg lép:

„(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 is.

(3) Az értékelésben fel kell mérni, 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."

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 Strasbourgban, -án/-én.

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