2025/37

2025.1.15.

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2025/37 RENDELETE

(2024. december 19.)

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 ([1]),

a Régiók Bizottságával folytatott konzultációt követően,

rendes jogalkotási eljárás keretében ([2]),

mivel:

(1) Az (EU) 2019/881 európai parlamenti és tanácsi rendelet ([3]) 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.

(2) Az Unió kibertámadásokkal szembeni rezilienciájának biztosítása és a belső piac sebezhetőségének megelőzése érdekében ez a rendelet az irányított biztonsági szolgáltatásokra, valamint e szolgáltatások alkalmazására és megbízhatóságára vonatkozó biztonsági célkitűzések előírásával az (EU) 2024/2847 európai parlamenti és tanácsi rendelet ([4]) szerinti, a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményeket létrehozó szabályozási keret kiegészítésére törekszik.

(3) Az irányított biztonsági szolgáltatásokat az (EU) 2022/2555 európai parlamenti és tanácsi irányelv ([5]) 6. cikkének 40. pontjában meghatározottak szerinti irányított biztonsági szolgáltatók nyújtják. Ezért az irányított biztonsági szolgáltatások e rendeletben szereplő fogalommeghatározásának összhangban kell lennie az irányított biztonsági szolgáltatók (EU) 2022/2555 irányelvben szereplő fogalommeghatározásával. Ezek a szolgáltatások magukba foglalják az ügyfeleik kiberbiztonsági kockázatkezelésével kapcsolatos tevékenységek végzését vagy az ahhoz nyújtott segítséget, és egyre nagyobb jelentőségre tesznek szert az események megelőzésében és enyhítésében. Ennek megfelelően az említett szolgáltatásokat nyújtó szolgáltatók az (EU) 2022/2555 irányelv értelmében kiemelten kritikus ágazathoz tartozó alapvető vagy fontos szervezeteknek minősülnek. Az említett irányelv (86) preambulumbekezdésében említettek szerint az irányított biztonsági szolgáltatók olyan területeken, mint az eseményekre való reagálás, a behatolásvizsgálat, a biztonsági ellenőrzés és a tanácsadás, különösen fontos szerepet töltenek be abban, hogy segítsék a szervezeteket az események megelőzésére, észlelésére, az azokra való reagálásra, vagy az azokat követő helyreállításra irányuló törekvéseikben. Azonban maguk az irányított biztonsági szolgáltatók is kibertámadások célpontjai, és az ügyfeleik működésébe való szoros integrációjuk miatt különös kockázatot jelentenek. Ezért fontos, hogy az (EU) 2022/2555 irányelv értelmében vett alapvető és fontos szervezetek fokozott gondossággal járjanak el az irányított biztonsági szolgáltatók kiválasztása során.

([1]) HL C 349., 2023.9.29., 167. o.

([2]) Az Európai Parlament 2024. április 24-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2024. december 2-i határozata.

([3]) 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.).

([4]) Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint az (EU) 168/2013 és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet) (HL L, 2024/2847, 2024.11.20., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([5]) 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.).

(4) Az irányított biztonsági szolgáltatások e rendelet szerinti fogalommeghatározása magában foglalja azon irányított biztonsági szolgáltatások nem kimerítő listáját, amelyekre európai kiberbiztonsági tanúsítási rendszerek vonatkozhatnak, mint például az események kezelése, a behatolásvizsgálat, a biztonsági ellenőrzések, és a technikai támogatással kapcsolatos tanácsadás. Az irányított biztonsági szolgáltatások magukban foglalhatják azokat a kiberbiztonsági szolgáltatásokat, amelyek támogatják az eseményekre való felkészültséget, azok megelőzését, észlelését, elemzését, enyhítését, az azokra való reagálást és azokat követő helyreállítást. A kiberfenyegetettség felderítés nyújtása és a technikai támogatással kapcsolatos kockázatértékelés szintén irányított biztonsági szolgáltatásoknak minősülhetnek. A különböző irányított biztonsági szolgáltatásokra külön európai kiberbiztonsági tanúsítási rendszerek vonatkozhatnak. Az ilyen rendszerekkel összhangban kiállított európai kiberbiztonsági tanúsítványoknak az említett szolgáltatásokat nyújtó adott szolgáltató konkrét irányított biztonsági szolgáltatásaira kell vonatkozniuk.

(5) Az irányított biztonsági szolgáltatók fontos szerepet játszhatnak a jelentős eseményekre és a nagyszabású kiberbiztonsági eseményekre való reagálást és a helyreállítás megkezdését támogató uniós intézkedések tekintetében is, megbízható magánszolgáltatók szolgáltatásaira, valamint a kritikus fontosságú szervezetek potenciális sebezhetőségek uniós szinten koordinált biztonsági kockázatértékeléseken alapuló tesztelésére támaszkodva. Az irányított biztonsági szolgáltatások tanúsítása szerepet játszhat az (EU) 2025/38 európai parlamenti és tanácsi rendeletben ([6]) meghatározottak szerinti megbízható irányított biztonsági szolgáltatók kiválasztásában.

(6) Az irányított biztonsági szolgáltatások tanúsítása nemcsak az (EU) 2025/38 rendelet által létrehozott uniós kiberbiztonsági tartalékhoz kapcsolódó kiválasztási eljárás 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 a kezelt adatok érzékenységére, a tanúsítás fontos iránymutatást és bizonyosságot nyújthat a potenciális ügyfelek számára az említett szolgáltatások megbízhatóságáról. Az irányított biztonsági szolgáltatásokra vonatkozó európai kiberbiztonsági tanúsítási rendszerek célja, hogy hozzájáruljanak a belső piac széttagoltságának megakadályozásához. E rendelet célja ezért a belső piac működésének javítása.

(7) Az irányított biztonsági szolgáltatások európai kiberbiztonsági tanúsítási rendszereinek e szolgáltatások elterjedéséhez és az irányított biztonsági szolgáltatók közötti verseny fokozódásához kell vezetniük. Az ilyen szolgáltatók megfelelő szintű műszaki ismereteinek és szakmai feddhetetlenség biztosítására irányuló célkitűzés sérelme nélkül, az ilyen tanúsítási rendszereknek ezért meg kell könnyíteniük a piacra lépést és az irányított biztonsági szolgáltatások nyújtását azáltal, hogy a lehető legnagyobb mértékben egyszerűsítik azokat az esetleges szabályozási, adminisztratív és pénzügyi terheket, amelyekkel a szolgáltatók, különösen a kis- és középvállalkozások (a továbbiakban: kkv-k) – beleértve a mikrovállalkozásokat – szembesülhetnek, amikor irányított biztonsági szolgáltatásokat kínálnak. Emellett az irányított biztonsági szolgáltatások elterjedésének ösztönzése és az azok iránti kereslet ösztönzése érdekében az európai kiberbiztonsági tanúsítási rendszereknek hozzá kell járulniuk azok hozzáférhetőségéhez, különösen a kisebb szereplők, például a kkv-k – beleértve a mikrovállalkozásokat –, valamint a korlátozott kapacitással és erőforrásokkal rendelkező, de a pénzügyi, jogi, reputációs és működést érintő következményekkel járó kiberbiztonsági jogsértéseknek jobban kitett helyi és regionális önkormányzatok számára.

(8) Fontos támogatást nyújtani a kkv-knak – beleértve a mikrovállalkozásokat – e rendelet végrehajtásához, valamint az e rendeletben meghatározott követelményeknek megfelelő irányított biztonsági szolgáltatások nyújtásához szükséges speciális kiberbiztonsági készségekkel és szakértelemmel rendelkező személyek felvételéhez. Az (EU) 2021/694 európai parlamenti és tanácsi rendelettel ([7]) létrehozott Digitális Európa program és más releváns uniós programok előírják, hogy a Bizottságnak olyan pénzügyi és technikai támogatást kell kialakítania, amely lehetővé teszi az említett vállalkozások számára, hogy hozzájáruljanak az uniós gazdaság növekedéséhez és a kiberbiztonság közös szintjének megerősítéséhez az Unióban, többek között a Digitális Európa programból és más releváns uniós programokból származó pénzügyi támogatás észszerűsítése, valamint a kkv-k – beleértve a mikrovállalkozásokat – támogatása révén.

(9) Az irányított biztonsági szolgáltatások európai kiberbiztonsági tanúsítási rendszerének hozzá kell járulnia a biztonságos digitális átállást garantáló és az (EU) 2022/2481 európai parlamenti és tanácsi határozattal ([8]) létrehozott digitális évtized 2030 szakpolitikai programban meghatározott célok eléréséhez hozzájáruló biztonságos és magas színvonalú szolgáltatások rendelkezésre állásához, különös tekintettel arra a célra, hogy az uniós vállalkozások 75 %-a kezdje el használni a felhő alapú számítástechnikát, a nagy adathalmazokat vagy a mesterséges

([6]) Az Európai Parlament és a Tanács (EU) 2025/38 rendelete (2024. december 19.) a kiberfenyegetések és -események észlelése, valamint az azokra való felkészülés és reagálás érdekében az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról, és az (EU) 2021/694 rendelet módosításáról (a kiberszolidaritásról szóló rendelet) (HL L, 2025/38, 2025.1.15., ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Az Európai Parlament és a Tanács (EU) 2021/694 rendelete (2021. április 29.) a Digitális Európa program létrehozásáról és az (EU) 2015/2240 határozat hatályon kívül helyezéséről (HL L 166., 2021.5.11., 1. o.).

([8]) Európai Parlament és a Tanács (EU) 2022/2481 határozata (2022. december 14.) a digitális évtized 2030 szakpolitikai program létrehozásáról (HL L 323., 2022.12.19., 4. o.).

intelligenciát, hogy a kkv-k – beleértve a mikrovállalkozásokat – több mint 90 %-a elérje legalább az alapszintű digitális intenzitást, és hogy a kulcsfontosságú közszolgáltatások online elérhetővé váljanak.

(10) Az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok igénybevételén túlmutatóan az irányított biztonsági szolgáltatások gyakran olyan szolgáltatási funkciókat is biztosítanak, amelyek az ilyen szolgáltatásokat nyújtók személyzetének kompetenciájára, szakértelmére és tapasztalatára támaszkodnak. A kiemelkedően magas szintű, említett kompetenciának, szakértelemnek és tapasztalatnak, valamint a megfelelő belső eljárásoknak a biztonsági célkitűzések részét kell képezniük a kiemelkedően magas minőségű irányított biztonsági szolgáltatások biztosítása érdekében. Annak biztosítása érdekében, hogy az irányított biztonsági szolgáltatások minden szempontból külön európai kiberbiztonsági tanúsítási rendszerek hatálya alá tartozzanak, módosítani kell az (EU) 2019/881 rendeletet. Figyelembe kell venni az (EU) 2019/881 rendeletben előírt értékelés és felülvizsgálat eredményeit és ajánlásait.

(11) A megbízható belső piac növekedésének elősegítése és a hasonlóan gondolkodó harmadik országokkal való partnerségek kialakítása érdekében az (EU) 2019/881 rendeletben meghatározott európai kiberbiztonsági tanúsítási kereten belül kialakított tanúsítási eljárást olyan módon kell lefolytatni, hogy az megkönnyítse a nemzetközi elismerést és a nemzetközi szabványokhoz való igazodást.

(12) Az Unió szakemberhiánnyal küzd, mivel hiány mutatkozik a képzett szakemberek terén, miközben gyorsan változó fenyegetettségi helyzettel néz szembe, amint azt „A kiberbiztonsági szakemberhiány megszüntetése az EU versenyképességének, növekedésének és rezilienciájának növelése érdekében (a Kiberbiztonsági Készségek Akadémiája)” című, 2023. április 18-i bizottsági közlemény is elismeri. Az oktatási források és a formális képzés fajtái eltérőek, és az ismeretek különböző módokon szerezhetők meg: formálisan, például egyetemeken vagy tanfolyamokon, vagy informálisan, például munkahelyi képzésen vagy az adott területen szerzett munkatapasztalaton keresztül. Ezért a magas színvonalú irányított biztonsági szolgáltatások megjelenésének elősegítése és az uniós kiberbiztonsági munkaerő összetételének jobb áttekintése érdekében fontos, hogy megerősödjön a tagállamok, a Bizottság, az (EU) 2019/881 rendelettel létrehozott Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) és az érdekelt felek – többek között a magánszektor és a tudományos élet szereplői – közötti együttműködés 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 keretén keresztül. Az ilyen együttműködés várhatóan megkönnyíti a kiberbiztonsági szakemberek Unión belüli mobilitását, valamint a kiberbiztonsági ismereteknek és képzésnek az oktatási programokba való integrálását, miközben biztosítja a tanulószerződéses gyakorlati képzésekhez és szakmai gyakorlatokhoz való hozzáférést a fiatalok számára, beleértve a hátrányos helyzetű régiókban, például szigeteken, ritkán lakott, vidéki és távoli területeken élőket is. Fontos, hogy az ilyen együttműködés arra irányuljon, hogy több nőt és lányt vonzzanak a területre, és hozzájáruljon a nemek közötti szakadék kezeléséhez a tudományok, a technológia, a műszaki tudományok és a matematika terén, valamint hogy a magánszektor célja a közigazgatás és az induló innovatív vállalkozások, valamint a kkv-k – beleértve a mikrovállalkozásokat – bevonásával olyan munkahelyi képzés biztosítása legyen, amely a leginkább keresett készségeket célozza. Fontos továbbá, hogy a szolgáltatók és a tagállamok együttműködjenek és hozzájáruljanak a kiberbiztonsági munkaerőpiac helyzetére és alakulására vonatkozó adatok gyűjtéséhez.

(13) Az ENISA fontos szerepet játszik a javaslati európai kiberbiztonsági tanúsítási rendszerek kidolgozásában. Az Unió általános költségvetési tervezetének elkészítésekor a Bizottságnak az (EU) 2019/881 rendelet 29. cikkében meghatározott eljárással összhangban értékelnie kell az ENISA létszámtervéhez szükséges költségvetési forrásokat.

(14) Ez a rendelet az (EU) 2019/881 rendelet célzott módosításáról rendelkezik, annak érdekében, hogy lehetővé tegye az európai kiberbiztonsági tanúsítási rendszerek irányított biztonsági szolgáltatásokra vonatkozó létrehozását. Ennek során pontosítja és egyértelműbbé teszi az említett rendelet valamennyi európai kiberbiztonsági tanúsítási rendszer kidolgozására és működésére vonatkozó bizonyos rendelkezéseit, azok átláthatóságának és nyitottságának biztosítása érdekében. Ez utóbbi módosítások, amelyek az (EU) 2019/881 rendelet pontosítására vagy egyértelműbbé tételére korlátozódnak - különös tekintettel a javasolt tanúsítási rendszerek továbbításakor az ENISA által nyújtandó információkra, az egyes tanúsítási rendszerek esetében létrehozott eseti munkacsoportokra és az európai kiberbiztonsági tanúsítási rendszerekről történő tájékoztatásra és konzultációra vonatkozó módosításokra - semmilyen módon nem érinthetik az említett rendelet 67. cikke szerinti szélesebb körű értékelést és felülvizsgálatot, különösen az említett rendelet kiberbiztonsági tanúsítási keretrendszerre vonatkozó címe hatásának, eredményességének és hatékonyságának értékelését. Az említett cím értékelésének és felülvizsgálatának az érdekelt felekkel folytatott széles körű konzultáción, valamint az érintett eljárások teljes körű és alapos elemzésén kell alapulnia.

(15) Mivel e rendelet célját, nevezetesen az irányított biztonsági szolgáltatásokra vonatkozó európai kiberbiztonsági tanúsítási rendszerek létrehozásának lehetővé tételét a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban annak terjedelme és hatásai miatt e cél jobban megvalósítható, az Unió intézkedéseket hozhat a szubszidiaritásnak az Európai Unióról szóló szerződés 5. cikkében foglalt elvével összhangban. Az arányosságnak az említett cikkben foglalt elvével összhangban ez a rendelet nem lépi túl az e cél eléréséhez szükséges mértéket.

(16) (16) Az európai adatvédelmi biztossal az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([9]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos 2024. január 10-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., a 10. és a 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 vagy 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 cikk a következő ponttal egészül ki:

„14a. »irányított biztonsági szolgáltatás«: olyan, harmadik félnek nyújtott szolgáltatás, amely a kiberbiztonsági kockázatkezeléssel kapcsolatos tevékenységek – például események kezelése, behatolásvizsgálat, biztonsági ellenőrzések és technikai támogatással kapcsolatos tanácsadás, többek között szakértői tanácsadás – elvégzéséből vagy az azokhoz nyújtott segítségből áll;”

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

„20. »műszaki előírás«: 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;

([9]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o.).

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, és megmutatja, hogy valamely IKT-terméket, IKT-szolgáltatást, IKT-folyamatot vagy irányított biztonsági szolgáltatást milyen szinten értékeltek, de 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 vagy 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 a következőképpen módosul:

i. a bevezető fordulat 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:”;

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

„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;”

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 helyébe a következő szöveg lép:

„*46. cikk*

Az európai kiberbiztonsági tanúsítási keretrendszer

(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, valamint annak tanúsítására, 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 vagy az azokon keresztül tárolt vagy továbbított vagy kezelt adatok, vagy az általuk vagy az azokon keresztül ellátott funkciók vagy az általuk vagy az azokon keresztül 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 kompetenciával, szakértelemmel és tapasztalattal, kielégítő és megfelelő szintű releváns műszaki ismeretekkel és szakmai feddhetetlenséggel rendelkező személyzet nyújtja."

6. A 47. cikk a következőképpen módosul:

a) a (2) bekezdés helyébe a következő szöveg lép:

„(2) Az uniós gördülő munkaprogramnak magában kell foglalnia különösen azon IKT-termékek, IKT-szolgáltatások, IKT-folyamatok és irányított biztonsági szolgáltatások vagy ezek kategóriáinak jegyzékét, amelyek alkalmasak arra, hogy valamely európai kiberbiztonsági tanúsítási rendszer hatálya alá vonják őket.";

b) a (3) bekezdés következőképpen módosul:

ii. a bevezető fordulat helyébe a következő szöveg lép:

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

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

„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, és különösen a széttagoltság veszélyére tekintettel;"

iii. a bekezdés a következő ponttal egészül ki:

„ca) a technológiai fejlődés, valamint a nemzetközi kiberbiztonsági tanúsítási rendszerek, a nemzetközi és az ipar által használt szabványok rendelkezésre állása és fejlesztése;".

7. A 49. cikk a következőképpen módosul:

a) az (1)–(4) bekezdés helyébe a következő szöveg lép:

„(1) Az ENISA-nak a Bizottság 48. cikk szerinti kérése alapján ki kell dolgoznia egy olyan javasolt tanúsítási rendszert, amely megfelel az 51., az 51a., az 52. és az 54. cikkben meghatározott alkalmazandó követelményeknek.

(2) Az ENISA az európai kiberbiztonsági tanúsítási csoport 48. cikk (2) bekezdése szerinti kérése alapján kidolgozhat egy olyan javasolt tanúsítási rendszert, amely megfelel az 51., az 51a., az 52. és az 54. cikkben meghatározott alkalmazandó követelményeknek. E kérés visszautasítása esetén az ENISA köteles azt megindokolni. E kérés elutasításáról az igazgatótanács dönthet.

(3) A javasolt tanúsítási rendszer kidolgozása során az ENISA-nak hivatalos, nyílt, átlátható és inkluzív konzultációs folyamat keretében kellő időben konzultálnia kell valamennyi érdekelt féllel. Amikor a (6) bekezdés szerint továbbítja a javasolt tanúsítási rendszert a Bizottságnak, az ENISA tájékoztatást nyújt arról, hogy miként felelt meg e bekezdésnek.

(4) Minden egyes javasolt tanúsítási rendszer tekintetében az ENISA a 20. cikk (4) bekezdésével összhangban eseti munkacsoportot hoz létre, az ENISA számára konkrét tanácsadás nyújtása és szakértelem biztosítása céljából. Ezen eseti munkacsoportokban – adott esetben és a 20. cikk (4) bekezdésében előírt eljárások és mérlegelési jogkör sérelme nélkül – a tagállamok közigazgatási szervei, az uniós intézmények, szervek, hivatalok és ügynökségek, valamint a magánszektor szakértői is részt vesznek.";

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

„(7) A Bizottság az ENISA által kidolgozott javasolt tanúsítási 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 51a., az 52. és az 54. cikkben meghatározott releváns követelményeknek megfelelő európai kiberbiztonsági tanúsítási rendszerekről rendelkezik. E végrehajtási jogi aktusokat a 66. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni."

8. A rendelet a következő cikkel egészül ki:

„49a. cikk

Tájékoztatás és konzultáció az európai kiberbiztonsági tanúsítási rendszerekről

(1) A Bizottság nyilvánosan hozzáférhetővé teszi az ENISA-hoz intézett, a 48. cikkben említettek szerinti, javasolt tanúsítási rendszer kidolgozására vagy egy létező európai kiberbiztonsági tanúsítási rendszer felülvizsgálatára irányuló kérésére vonatkozó információkat.

(2) A javasolt tanúsítási rendszer ENISA általi, 49. cikk szerinti kidolgozása során az Európai Parlament, a Tanács vagy mindkettő felkérheti a Bizottságot - mint az európai kiberbiztonsági tanúsítási csoport elnökét - és az ENISA-t, hogy negyedévente nyújtson be releváns információkat a javasolt tanúsítási rendszer tervezetéről. Az Európai Parlament vagy a Tanács kérésére az ENISA – a Bizottsággal egyetértésben és a 27. cikk sérelme nélkül – az előírt titoktartási szintnek megfelelő és adott esetben korlátozott módon az Európai Parlament és a Tanács rendelkezésére bocsáthatja a javasolt tanúsítási rendszer tervezetének vonatkozó részeit.

(3) Az uniós intézmények közötti párbeszéd fokozása, valamint a hivatalos, nyílt, átlátható és inkluzív konzultációs folyamathoz való hozzájárulás érdekében az Európai Parlament, a Tanács vagy mindkettő felkérheti a Bizottságot és az ENISA-t, hogy vitassák meg az IKT-termékekre, az IKT-szolgáltatásokra, az IKT-folyamatokra vagy az irányított biztonsági szolgáltatásokra vonatkozó európai kiberbiztonsági tanúsítási rendszerek működésével kapcsolatos kérdéseket.

(4) A Bizottság e rendeletnek a 67. cikk szerinti értékelése során adott esetben figyelembe veszi az Európai Parlament és a Tanács által az e cikk (3) bekezdésében említett kérdésekkel kapcsolatban kifejtett véleményekből eredő elemeket.”

9. 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:”.

10. 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) hogy az irányított biztonsági szolgáltatásokat a szükséges kompetenciával, szakértelemmel és tapasztalattal nyújtsák, beleértve azt is, hogy az e szolgáltatások nyújtásával megbízott személyzet az adott területen kielégítő és megfelelő műszaki ismeretekkel és kompetenciával, kielégítő és megfelelő tapasztalattal, valamint a legmagasabb szintű szakmai feddhetetlenséggel rendelkezzen;

b) hogy a szolgáltató megfelelő belső eljárásokkal rendelkezzen annak biztosítására, hogy az irányított biztonsági szolgáltatások mindenkor kielégítő és megfelelő színvonalúak legyenek;

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

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

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

f) hogy tartsák nyilván és értékelés céljából tegyék hozzáférhetővé, hogy ki, mikor és mely adatokat, szolgáltatásokat vagy funkciókat vett igénybe, használt vagy kezelt egyéb módon;

g) hogy az irányított biztonsági szolgáltatások nyújtása során alkalmazott IKT-termékek, IKT-szolgáltatások és IKT-folyamatok tervezetten és alapértelmezetten biztonságosak legyenek, és adott esetben tartalmazzák a legújabb biztonsági frissítéseket, és esetükben ne álljanak fenn közismert sebezhetőségek.”

11. 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: »alap«, »jelentős« és »magas«. A megbízhatósági szintnek az 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), a (6) és a (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 vagy 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 az eseményekkel és a kiberbiztonsági 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 vagy 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 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 vagy 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.”

12. 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 vagy 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. cikk szerint kijelölt 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.”

13. 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 vagy irányított biztonsági szolgáltatások típusát vagy kategóriáit;”

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

„g) az 51. és az 51a. cikkben említett alkalmazandó biztonsági célkitűzések elérésének igazolása érdekében az alkalmazandó konkrét értékelési kritériumok és módszerek, beleértve az értékelés típusait is;”

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

„j) az IKT-termékeknek, az IKT-szolgáltatásoknak, az IKT-folyamatoknak vagy 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;”

d) 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 vagy irányított biztonsági szolgáltatások nem felelnek meg a tanúsítási rendszer követelményeinek;”

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

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

f) 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;”.

14. 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 2025. február 4-től 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 értékelések 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:

— 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;”,

— 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, ideértve a kkv-k – beleértve a mikrovállalkozásokat is – sajátos érdekeit és igényeit;”

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. cikk szerint kijelölt 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, folyamat vagy irányított biztonsági szolgáltatás tanúsítással összefüggő követelményeknek való megfelelésére. Ez a hatóság vagy szervezet az említett információt köteles indokolatlan késedelem nélkül továbbítani az érintett nemzeti kiberbiztonsági tanúsító hatóságnak.”

15. 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.”

16. 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, hogy bizonyos IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások valószínűleg nem felelnek meg e rendelet vagy egyes európai kiberbiztonsági tanúsítási rendszerek követelményeinek; valamint;"

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."

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

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

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

„(2) Az értékelésben fel kell mérni továbbá az e rendelet III. címében foglalt rendelkezések hatását, eredményességét és hatékonyságát, beleértve az európai kiberbiztonsági tanúsítási rendszerek elfogadásához vezető eljárásokat és az azok alapját képző tényeket, tekintettel 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 irányuló célkitűzésekre.

(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 belső piacra való belépésének megelőzése érdekében, amelyek nem felelnek meg az alapszintű kiberbiztonsági követelményeknek."

19. A melléklet e rendelet mellékletének megfelelően módosul.

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 Brüsszelben, 2024. december 19-én.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*
R. METSOLA	BÓKA J.

MELLÉKLET

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

1. A 2–5. pont helyébe a következő szöveg lép:

„2. A megfelelőségértékelő szervezet olyan harmadik fél, amely független az általa értékelt szervezettől vagy IKT-termékektől, IKT-szolgáltatásoktól, IKT-folyamatoktól vagy irányított biztonsági szolgáltatásoktól.

3. Megfelelőségértékelő szervezetnek tekinthető olyan szervezet is, amely az általa értékelt IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások tervezésében, gyártásában, nyújtásában, összeszerelésében, használatában vagy karbantartásában részt vevő vállalkozásokat képviselő vállalkozói szövetséghez vagy szakmai egyesüléshez tartozik, feltéve, hogy bizonyítottan független és esetében bizonyítottan nem áll fenn összeférhetetlenség.

4. A megfelelőségértékelő szervezetek, azok felső vezetése és a megfelelőségértékelési feladatok elvégzéséért felelős személyek nem lehetnek tervezői, gyártói, nyújtói, üzembe helyezői, vásárlói, tulajdonosai, felhasználói vagy karbantartói az értékelt IKT-terméknek, IKT-szolgáltatásnak, IKT-folyamatnak vagy irányított biztonsági szolgáltatásnak, valamint nem lehetnek az említett felek meghatalmazott képviselői sem. Ez a tilalom nem zárja ki a megfelelőségértékelő szervezet működéséhez szükséges, értékelt IKT-termékek használatát, sem az ilyen IKT-termékek személyes célra történő használatát.

5. A megfelelőségértékelő szervezetek, azok felső vezetése és a megfelelőségértékelési feladatok elvégzéséért felelős személyek nem vehetnek részt közvetlenül az értékelt IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások tervezésében, gyártásában és kivitelezésében, biztosításában, értékesítésében, üzembe helyezésében, használatában és karbantartásában, valamint nem képviselhetnek az ilyen tevékenységekben részt vevő feleket. A megfelelőségértékelő szervezetek, azok felső vezetése és a megfelelőségértékelési feladatok elvégzéséért felelős személyek nem vehetnek részt olyan tevékenységben sem, amely megfelelőségértékelési tevékenységük tekintetében veszélyeztetné döntéshozói függetlenségüket vagy feddhetetlenségüket. Ez a tilalom különösen érvényes a szaktanácsadási szolgáltatásokra.”

2. A 10. pont a következőképpen módosul:

a) a bevezető fordulat helyébe a következő szöveg lép:

„10. A megfelelőségértékelő szervezetnek minden megfelelőségértékelési eljárás és az IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások minden típusa, kategóriája és alkategóriája tekintetében mindenkor rendelkeznie kell a szükséges:”;

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

„c) olyan, tevékenységeinek elvégzésére szolgáló eljárásokkal, amelyek kellően figyelembe veszik az adott vállalkozás méretét, az ágazatot, amelyben a vállalkozás a tevékenységét folytatja, a vállalkozás szerkezetét, az érintett IKT-termék, IKT-szolgáltatás, IKT-folyamat vagy irányított biztonsági szolgáltatás műszaki összetettségének fokát, valamint azt, hogy tömeg- vagy sorozatgyártásról van-e szó.”

3. A 19. és a 20. pont helyébe a következő szöveg lép:

„19. A megfelelőségértékelő szervezeteknek meg kell felelniük az IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások tanúsítását végző megfelelőségértékelő szervezetek akkreditálása tekintetében a vonatkozó, a 765/2008/EK rendelet 2. cikkének 9. pontjában meghatározottak szerinti harmonizált szabvány követelményeinek.

20. A megfelelőségértékelő szervezeteknek biztosítaniuk kell, hogy a megfelelőségértékelések céljára használt vizsgálati laboratóriumok megfeleljenek a vizsgálatokat végző laboratóriumok akkreditálása tekintetében a vonatkozó, a 765/2008/EK rendelet 2. cikkének 9. pontjában meghatározottak szerinti harmonizált szabvány követelményeinek.”

E rendelet tekintetében egy nyilatkozat megtételére került sor, amely a HL következő számában található: HL C, 2025/307, 2025.1.15., ELI: http://data.europa.eu/eli/C/2025/307/oj.