Az Európai Unió
Tanácsa

Brüsszel, 2026. május 22.
(OR. en)

9399/26

Intézményközi referenciaszámok:
2026/0011 (COD)
2026/0012 (COD)

LIMITE

CYBER 229
JAI 606
DATAPROTECT 161
TELECOM 239
MI 489
IND 342
CADREFIN 220
FIN 697
BUDGET 19
CSC 316
CODEC 937

FELJEGYZÉS

Küldi:	a Tanács Főtitkársága
Címzett:	az Állandó Képviselők Bizottsága/a Tanács
Tárgy:	Javaslat – Az Európai Parlament és a Tanács rendelete az Európai Uniós Kiberbiztonsági Ügynökségről (ENISA), az európai kiberbiztonsági tanúsítási keretrendszerről és az IKT-ellátási lánc biztonságáról, valamint az (EU) 2019/881 rendelet hatályon kívül helyezéséről (2. kiberbiztonsági jogszabály) Javaslat – Az Európai Parlament és a Tanács irányelve az (EU) 2022/2555 irányelvnek az egyszerűsítési intézkedések és [a 2. kiberbiztonsági jogszabályra irányuló javaslattal] való összehangolás tekintetében történő módosításáról – Jelentés az elért eredményekről

Az elnökség a Tanács előkészítő szervei által eddig elvégzett munka és a javaslat vizsgálatával kapcsolatos aktuális helyzet ismertetése céljából jelentést készített az Európai Uniós Kiberbiztonsági Ügynökségről (ENISA), az európai kiberbiztonsági tanúsítási keretrendszerről és az IKT-ellátási lánc biztonságáról, valamint az (EU) 2019/881 rendelet hatályon kívül helyezéséről szóló európai parlamenti és tanácsi rendeletre (2. kiberbiztonsági jogszabály) irányuló javaslattal kapcsolatban elért eredményekről.

BEVEZETÉS

1. 2026. január 20-án a Bizottság az EU kiberbiztonsági rezilienciájának és képességeinek megerősítése céljából új kiberbiztonsági csomagra tett javaslatot. A csomag egyik tagja az Európai Uniós Kiberbiztonsági Ügynökségről (ENISA), az európai kiberbiztonsági tanúsítási keretrendszerről és az IKT-ellátási lánc biztonságáról szóló **rendelet**, amely hatályon kívül helyezi az (EU) 2019/881 rendeletet (a kiberbiztonsági jogszabályt). Ezt a rendeletet (a „2. kiberbiztonsági jogszabályt") kiegészíti egy **irányelv**, amely az (EU) 2022/2555 irányelvnek (NIS 2 irányelv) az egyszerűsítési intézkedések és [a 2. kiberbiztonsági jogszabályra irányuló javaslattal] való összehangolás tekintetében történő módosításáról szól.

2. A javaslat benyújtását megelőzően a Tanács az ENISA-ról szóló 2024. december 6-i következtetéseiben[1] felkérte a Bizottságot, hogy vizsgálja meg és erősítse tovább az ENISA által a kiberreziliencia javítása terén uniós szinten és a tagállamok között megvalósuló operatív együttműködés támogatásában betöltött szerepet, figyelembe véve a tagállamok e területen meglévő hatásköreit. Emellett felszólította a Bizottságot annak biztosítására is, hogy az ENISA-nak a tagállamok támogatására vonatkozó megbízatása célzott és egyértelműen meghatározott legyen, tartalmazzon konkrét stratégiai célkitűzéseket és rangsorolt feladatokat, a többi szereplő tekintetében fennálló feladatok és hatáskörök pontosabb megosztása mellett. Arra sürgette továbbá a Bizottságot, hogy éljen a kiberbiztonsági jogszabály értékelése által kínált lehetőséggel, és tárja fel, hogy az uniós kiberbiztonsági tanúsítási rendszerek kidolgozása tekintetében miként rendelkezhetnénk egy egyszerűbb, kockázatalapú, valamint átláthatóbb és gyorsabb megközelítéssel. Emellett a kiberbiztonság jövőjéről szóló, 2024. május 21-i következtetéseiben[2] a Tanács hangsúlyozta az IKT-ellátási láncok biztonságának garantálása iránti elkötelezettségét, és kiemelte a nem technikai jellegű kockázati tényezők – például a harmadik államok által a beszállítókra és a szolgáltatókra gyakorolt jogtalan befolyásolás –jelentőségét. Végezetül, az IKT-ellátási lánc biztonságáról szóló, 2022. október 17-i következtetéseiben[3] a Tanács hangsúlyozta, hogy meg kell erősíteni az IKT-ellátási láncok rezilienciáját és biztonságát, tekintettel a geopolitikai feszültségekből, valamint az IKT-termékektől és -szolgáltatásoktól való függőségekből fakadó hatásokra.

---

1 16527/24.
2 10133/24.
3 13664/22.

3. Az EUMSZ 114. cikkén alapuló rendeletjavaslat célja az Unió kiberbiztonsági keretének megerősítése. Megerősíti az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) arra irányuló szerepét és feladatait, hogy támogassa a tagállamokat és az uniós szervezeteket az Unión belüli magas szintű kiberbiztonság, reziliencia és bizalom elérésében. Emellett hatékonyabbá és eredményesebbé hivatott tenni az európai kiberbiztonsági tanúsítási keretrendszert (ECCF), hogy ezáltal gyorsabbá válhasson a rendszer kiépítése és bevezetése. A javaslat létrehozza továbbá a megbízható IKT-ellátási láncok uniós biztonsági keretrendszerét, amely a kritikus IKT-infrastruktúrák és -szolgáltatások biztonságát érintő nem technikai jellegű kockázati tényezőket és függőségeket hivatott kezelni. Ehhez célzott egyszerűsítési intézkedések társulnak a NIS 2 irányelv[4] végrehajtását illetően, amelyek célja a megfelelési követelmények egyszerűsítése, a szükségtelen adminisztratív terhek csökkentése és a jogi egyértelműség növelése.

4. Az állam-, illetve kormányfők 2026. április 24-én Cipruson megrendezett nem hivatalos találkozója alkalmával aláírt „Egy Európa, egy piac” ütemterv[5] ezt a javaslatot nevezi meg a prioritásként elérendő eredmények egyikeként.

5. Az Európai Parlament Gregorová Markétát (Verts/ALE) nevezte ki a javaslatért felelős ITRE bizottság előadójává.

6. Az Európai Gazdasági és Szociális Bizottság 2026. április 29-én nyilvánított véleményt[6] a javaslatról.

---

4 HL L 333., 2022.12.27., 80. o.
5 8473/26.
6 8980/26.

A MUNKA AKTUÁLIS ÁLLÁSA A TANÁCS ELŐKÉSZÍTŐ SZERVEIBEN

7. A kiberbiztonsági csomag általános ismertetésére a kiberkérdésekkel foglalkozó horizontális munkacsoport (HWPCI) 2026. január 26-i ülésén, valamint az Állandó Képviselők Bizottsága 2026. január 28-i ülésén került sor.

8. A HWPCI 2026. február 2-án a Bizottság által tartott részletes ismertetővel kezdte meg a javaslat megvitatását. Ennek az ismertetőnek a során a Bizottság beszámolt az értékelő jelentés, a pénzügyi kimutatás és a hatásvizsgálat megállapításairól is.

9. A rendelet átolvasását a HWPCI 2026. február 23-án kezdte meg.

10. A tagállamok üdvözölték a javaslatot, és általánosságban támogatásuknak adtak hangot annak általános célkitűzéseit – különösen az ENISA által a tagállamok közötti operatív együttműködéshez nyújtott támogatás megerősítését és a tanúsítási keretrendszer észszerűsítését– illetően. A megbeszélések azonban azt is megmutatták, hogy a javaslatnak több aspektusa kapcsán is további vizsgálatra lenne szükség. A delegációk további pontosítást kértek az ENISA számára előirányzott kibővített operatív szereppel és feladatokkal – például a korai riasztások kiadásával, a zsarolóvírus-ügyfélszolgálat létrehozásával és az ENISA CSIRT-hálózatban betöltött szerepével – kapcsolatban. Több delegáció részéről kérdések hangzottak el azt illetően, hogy milyen erőforrás-vonzatokkal járna a tagállamokra nézve az ENISA feladatainak támogatására kirendelendő tagállamonként két nemzeti szakértővel kapcsolatos, javasolt hozzájárulás. Az igazgatótanács szavazási szabályairól szintén további egyeztetésre van szükség. A delegációk hangsúlyozták, hogy egyértelműbbé kell tenni és pontosítani kell a javaslatban használt fogalommeghatározásokat és fogalmakat. Az ENISA költségvetésének összetétele és különösen a díjak felszámítása szintén további pontosításra szorul.

11. A tanúsítási folyamat hatékonyabbá és eredményesebbé tételét célzó új rendelkezések általánosságban pozitív fogadtatásban részesültek, bár általános igényként fogalmazódott meg az, hogy a tagállamok a tanúsítási folyamatban mindvégig fokozottabban részt vegyenek. Általánosságban üdvözölték a tanúsítás önkéntes jellegét. A tanúsítási keretrendszerben alkalmazandó határidők közül néhányat azonban megkérdőjeleztek a delegációk.

12. A megbízható IKT-ellátási láncok keretéről folytatott megbeszélések a tagállamok számos aggályára rávilágítottak. A delegációk további pontosítást kértek a kulcsfontosságú IKT-eszközök és a magas kockázatú beszállítók azonosítására szolgáló módszertan és eljárások, valamint a javasolt intézkedések hatálya és lehetséges hatása tekintetében. A delegációk hangsúlyozták annak fontosságát, hogy biztosított legyen a tagállamok megfelelő szintű bevonása.

13. Több delegáció vizsgálati fenntartással élt a javaslat különböző részeivel kapcsolatban, különös tekintettel az irányítási szempontokra, a végrehajtási jogi aktusok alkalmazására, valamint a magas kockázatú beszállítók azonosítása, illetve az IKT-ellátási lánc biztonsága tekintetében javasolt mechanizmusra.

14. A HWPCI keretében folytatott megbeszéléseket követően a tagállamok felkérést kaptak, hogy nyújtsanak be írásbeli észrevételeket az általános rendelkezésekről szóló I. címhez és az ENISA-ról szóló II. címhez kapcsolódó rendelkezésekről. 23 tagállam nyújtott be észrevételeket. Később a tagállamok arra is felkérést kaptak, hogy nyújtsák be írásbeli észrevételeiket az európai kiberbiztonsági tanúsítási keretrendszerről szóló III. címmel kapcsolatban. 20 tagállam élt az írásbeli észrevételek benyújtásának lehetőségével.

15. A tagállamok ezen írásbeli észrevételei és a HWPCI keretében végzett munka alapján az elnökség kompromisszumos szöveget fog kidolgozni a II. címről (ENISA) és a III. címről (európai kiberbiztonsági tanúsítási keretrendszer), amelynek ismertetésére a HWPCI 2026. június elején tartandó ülésén fog sor kerülni.

16. Több tagállam is kérte, hogy a Tanács Jogi Szolgálata vizsgálja meg a jogalap megfelelőségét.

17. Az elnökség 2026. május végén megkezdi a NIS 2 irányelv egyszerűsítési intézkedéseinek áttekintését.

18. A ciprusi elnökség lezárultával elmondható lesz, hogy a munkacsoport az elnökség alatt összesen 15 ülést szentelt a 2. kiberbiztonsági jogszabálynak.

19. A soron következő ír elnökség a ciprusi elnökség alatt elért eredményekre építve folytatni kívánja a munkát e fontos javaslattal kapcsolatban.

20. A fentiek fényében felkérjük az Állandó Képviselők Bizottságát és a Tanácsot, hogy nyugtázza a rendeletjavaslat vizsgálata során elért eredményeket.