Az Európai Unió
Tanácsa

Brüsszel, 2025. december 17.
(OR. en)

16960/25

CYBER 389
JAI 1924
DATAPROTECT 345
TELECOM 485
MI 1075
CSC 693
CSCI 284
DELACT 198

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2025. december 11.
Címzett:	Thérèse BLANCHET, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	C(2025) 8407 final
Tárgy:	A BIZOTTSÁG (EU) .../... FELHATALMAZÁSON ALAPULÓ RENDELETE (2025.12.11.) az (EU) 2024/2847 európai parlamenti és tanácsi rendeletnek az értesítések terjesztésének késleltetésével kapcsolatos, kiberbiztonsággal összefüggő indokok alkalmazására vonatkozó feltételek meghatározása tekintetében történő kiegészítéséről

Mellékelten továbbítjuk a delegációknak a következő dokumentumot: C(2025) 8407 final.

Melléklet: C(2025) 8407 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2025.12.11.
C(2025) 8407 final

A BIZOTTSÁG (EU) .../... FELHATALMAZÁSON ALAPULÓ RENDELETE

(2025.12.11.)

az (EU) 2024/2847 európai parlamenti és tanácsi rendeletnek az értesítések terjesztésének késleltetésével kapcsolatos, kiberbiztonsággal összefüggő indokok alkalmazására vonatkozó feltételek meghatározása tekintetében történő kiegészítéséről

(EGT-vonatkozású szöveg)

INDOKOLÁS

1. A FELHATALMAZÁSON ALAPULÓ JOGI AKTUS HÁTTERE

Az (EU) 2024/2847 európai parlamenti és tanácsi rendelet (a továbbiakban: a kiberrezilienciáról szóló rendelet) előírja a digitális elemeket tartalmazó termékek gyártói számára, hogy egyetlen jelentéstételi platformon keresztül jelentsenek minden olyan aktívan kihasznált sérülékenységet vagy súlyos eseményt, amely érinti a digitális elemeket tartalmazó termék biztonságát. Az említett rendelet 16. cikkének (2) bekezdése értelmében az értesítést elsődlegesen fogadó, a tagállam által koordinátorként kijelölt számítógép-biztonsági incidensekre reagáló csoport (CSIRT) kivételes körülmények között és a kiberbiztonsággal összefüggő jogos indokok alapján elhalaszthatja az értesítés továbbítását azon egyéb tagállamok CSIRT-jeinek, ahol a digitális elemeket tartalmazó terméket rendelkezésre bocsátották.

E felhatalmazáson alapuló jogi aktus célja tehát a kiberrezilienciáról szóló rendelet kiegészítése, hogy meghatározásra kerüljenek azok a feltételek, amelyek mellett az értesítések továbbításának késleltetése érdekében alkalmazhatóak a kiberbiztonsággal összefüggő indokok. A jogi aktus három olyan indokot azonosít, amelyek esetén az értesítést elsődlegesen fogadó CSIRT úgy dönthet, hogy el kell halasztani az értesítés többi CSIRT-nek való továbbterjesztését. Az ilyen halasztásra vonatkozó döntést három esetben lehet meghozni:

- a bejelentett információk jellegének kiértékelése alapján;
- ha az értesítést fogadó CSIRT nem tudja biztosítani a szóban forgó információk bizalmas kezelését;
- ha az egységes jelentéstételi platform veszélybe került vagy ideiglenesen nem működik.

Az (EU) 2024/2847 rendelet 14. cikkében meghatározott jelentéstételi kötelezettségek 2026. szeptember 11-től kezdve alkalmazandók.

2. AZ AKTUS ELFOGADÁSÁT MEGELŐZŐ KONZULTÁCIÓK

E jogi aktus különböző tervezeteivel kapcsolatban a CSIRT-hálózattal és az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA) folytatott konzultációra került sor. 2025. március 26-án zajlott az irányadó kérdéseken alapuló előzetes megbeszélés, amelyet követően 2025. április 11-ig lehetett írásbeli észrevételeket benyújtani. A jogi aktus első tervezetét 2025. május 16-án osztották meg a CSIRT-hálózattal és az ENISA-val, 2025. június 6-án pedig megbeszélésre került sor, amelyet követően 2025. június 27-ig lehetett írásbeli észrevételeket benyújtani. A jogi aktus második tervezetét 2025. július 23-án osztották meg a CSIRT-hálózattal ezt követően 2025. szeptember 1-jéig lehetett írásbeli észrevételeket benyújtani. A jogi aktus harmadik tervezetét 2025. szeptember 25-én osztották meg a CSIRT-hálózattal és az ENISA-val, majd 2025. október 9-én megbeszélésre került sor, amelyet követően 2025. október 27-ig lehetett írásbeli észrevételeket benyújtani.

2025. október 16. és 2025. november 13. között nyilvános konzultációra került sor a jogi aktus tervezetével kapcsolatban. Ennek keretében 34 válasz érkezett, 31 egyedi válaszadótól (mivel az egyik válaszadó 4 különböző alkalommal nyújtotta be ugyanazt a választ). A válaszok 29,41 %-a vállalkozói szövetségektől, 26,47 %-a vállalatoktól/vállalkozásoktól,

17,65 %-a uniós polgároktól, 14,71 %-a közigazgatási szervektől, 5,88 %-a nem kormányzati szervezetektől, 5,88 %-a pedig tudományos-/kutatóintézetektől érkezett[1].

Október 22-én a tervezetet megvitatták a digitális elemeket tartalmazó termékek kiberbiztonságával foglalkozó szakértői csoportban (E03967) is, amelynek tagjai többek között a tagállami hatóságok, az ENISA, a személyes minőségükben kinevezett egyéni szakértők és a szó tágabb értelmében vett szervezetek (pl. vállalatok, egyesületek, nem kormányzati szervezetek).

3. A FELHATALMAZÁSON ALAPULÓ JOGI AKTUS JOGI ELEMEI

A felhatalmazáson alapuló jogi aktusok elfogadására vonatkozó felhatalmazásról a kiberrezilienciáról szóló jogszabály 14. cikkének (9) bekezdése rendelkezik, amely szerint a Bizottságnak 2025. december 11-ig meg kell határoznia az értesítések terjesztésének késleltetésével kapcsolatos, kiberbiztonsággal összefüggő indokok alkalmazásának feltételeit.

[1] Ezek a százalékos arányok nem veszik figyelembe azt a tényt, hogy az egyik válaszadó 4 különböző alkalommal nyújtott be azonos választ.

A BIZOTTSÁG (EU) .../... FELHATALMAZÁSON ALAPULÓ RENDELETE

(2025.12.11.)

az (EU) 2024/2847 európai parlamenti és tanácsi rendeletnek az értesítések terjesztésének késleltetésével kapcsolatos, kiberbiztonsággal összefüggő indokok alkalmazására vonatkozó feltételek meghatározása tekintetében történő kiegészítéséről

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról szóló, 2024. október 23-i (EU) 2024/2847 európai parlamenti és tanácsi rendeletre (a kiberrezilienciáról szóló rendelet)[2] és különösen annak 14. cikke (9) bekezdésére,

mivel:

(1) Kivételes körülmények között és különösen a gyártó kérésére, valamint a bejelentett információk érzékenységi szintjére tekintettel és a kiberbiztonsággal összefüggő jogos indokok alapján az a koordinátorként kijelölt számítógép-biztonsági eseményekre reagáló csoport (CSIRT), amely először kap értesítést egy aktívan kihasznált sérülékenységről vagy a digitális elemeket tartalmazó termék biztonságát érintő súlyos eseményről (a továbbiakban: az értesítést elsődlegesen fogadó CSIRT) úgy dönthet, hogy a feltétlenül szükséges ideig elhalasztja az értesítésnek az egységes jelentéstételi platformon keresztül történő továbbítását azon, koordinátorként kijelölt CSIRT-ek részére, amelyek területén az értesítést benyújtó gyártó jelzése szerint a digitális elemeket tartalmazó terméket rendelkezésre bocsátották (a továbbiakban: releváns CSIRT). Ezért meg kell határozni az említett indokok alkalmazásának feltételeit. Amennyiben ilyen indokok alkalmazandók, az értesítést elsődlegesen fogadó CSIRT a feltétlenül szükséges ideig elhalaszthatja a releváns CSIRT-ek számára történő továbbítást, de nem köteles erre. Az (EU) 2024/2847 rendelet 16. cikkének (2) bekezdése szerint abban az esetben, ha az értesítést elsődlegesen fogadó CSIRT úgy dönt, hogy az említett indokokra hivatkozik, haladéktalanul tájékoztatnia kell az Európai Uniós Kiberbiztonsági Ügynökséget (a továbbiakban: ENISA) a halasztásra vonatkozó döntéséről és annak okairól, valamint arról, hogy mikor szándékozik továbbítani az értesítést.

(2) Az (EU) 2024/2847 rendelet 16. cikke (2) bekezdésének második albekezdésével összhangban az e rendeletben meghatározott, kiberbiztonsággal összefüggő indokok alkalmazására vonatkozó feltételek nem alkalmazandók az ENISA-nak a bejelentett információkhoz való hozzáférésére. Az ENISA-nak a bejelentett információkhoz való hozzáférése csak a következő, különösen kivételes körülmények között korlátozható: ha a gyártó az értesítésben jelzi, hogy az (EU) 2024/2847 rendelet 16. cikke (2)

[2] HL L, 2024/2847, 2024.11.20., ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

bekezdése harmadik albekezdésének a), b) vagy c) pontjában említett három feltétel egyike teljesül, és ebben az esetben is kizárólag az (EU) 2024/2847 rendelet 14. cikke (2) bekezdésének b) pontjában említett, a sérülékenységre vonatkozóan 72 órán belül benyújtandó értesítéssel kapcsolatban. Ilyen esetekben egyidejűleg csak azt az információt kell az ENISA-val közölni, hogy a gyártó értesítést tett, valamint a digitális elemeket tartalmazó termékre vonatkozó általános információkat, a sebezhetőségek kihasználásának általános jellegére vonatkozó információkat, továbbá az arra vonatkozó információkat, hogy biztonsággal összefüggő indokra történik hivatkozás.

(3) A bejelentett információkhoz való hozzáférés lehetővé teszi a CSIRT-ek számára, hogy áttekintést kapjanak a területük biztonságának állapotáról, és kockázatcsökkentő intézkedéseket vezessenek be, növelve az uniós kiberbiztonság általános szintjét. Ezért az értesítések továbbítására vonatkozóan a bejelentett információk jellegétől függően csak azokban az esetekben lehet további korlátozásokat bevezetni, ha a bejelentett információk érzékenységére való tekintettel a továbbterjesztésből eredő kiberbiztonsági kockázatok meghaladják az Unió számára jelentett biztonsági előnyöket, és ezek a kockázatok nem csökkenthetők megfelelően azáltal, hogy a CSIRT-hálózaton belül használt megfelelő protokollok – például a jelzőlámpa-protokoll (TLP) vagy a műveletek engedélyezésére vonatkozó protokoll (PAP) – segítségével korlátozzák az értesítések kezelését és további megosztását. Ilyen helyzet fordulhat elő például akkor, ha a gyártó arról tájékoztatja az értesítést elsődlegesen fogadó CSIRT-et, hogy rövidesen kockázatcsökkentő intézkedést tervez hozni (például javítócsomagot telepít). Előfordulhat az is, hogy az értesítést elsődlegesen fogadó CSIRT úgy dönt, hogy az értesítésnek csak bizonyos részeit továbbítja, ám ezek a részek mindazonáltal elegendőek ahhoz, hogy a releváns CSIRT-ek biztosítani tudják a megfelelő kockázatcsökkentő intézkedések bevezetését. Ezenkívül – a gyártók, a CSIRT-ek és a biztonsági kutatók közötti, a sérülékenységek azonosításával és feltárásával kapcsolatos együttműködés ösztönzése érdekében – ez a helyzet állhat fenn akkor is, ha a CSIRT egy folyamatban lévő, az (EU) 2022/2555 európai parlamenti és tanácsi irányelv[3] 12. cikkének (1) bekezdésében említett összehangolt, sérülékenységek feltárására irányuló eljárásban megbízható közvetítőként jár el. Az ilyen esetekben, ha a CSIRT úgy dönt, hogy elhalasztja az értesítés továbbítását, azt a szóban forgó CSIRT az (EU) 2024/2847 rendelet 16. cikkének (6) bekezdésével összhangban csak a feltétlenül szükségesnél nem hosszabb ideig halaszthatja el, és addig az időpontig, amíg az összehangolt sérülékenység-közzétételi eljárásban érintett felek beleegyezésüket nem adják a közzétételhez.

(4) Az értesítésben szereplő információk a CSIRT-ek segítségére lesznek a kockázatcsökkentéssel és az incidenskezeléssel kapcsolatos feladataik ellátásában. Egyes ritka esetekben azonban ezen információk akár a korlátozott készségekkel és erőforrásokkal rendelkező szereplők számára is elegendőek ahhoz, hogy további kutatás nélkül létrehozzanak az információk kihasználására irányuló technikákat. Ha ezekhez az információkhoz rosszindulatú szereplők is hozzáférhetnének, az súlyosan érintené az Unió kiberbiztonságát, tekintettel a kihasználás egyszerűségére. Például ilyen helyzetről lehet szó, ha egy szoftver sérülékeny változata csak kis mértékben tér

[3] 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.).

el a korábbi, nem sérülékeny változataitól. Ilyen esetekben, ha az értesítést elsődlegesen fogadó CSIRT szerint a továbbterjesztésből eredő kiberbiztonsági kockázat nem csökkenthető megfelelően a kezelésre és további megosztásra vonatkozó korlátozások bevezetésével, úgy dönthet, hogy elhalasztja a továbbítást mindaddig, amíg nem áll rendelkezésre hatékony kockázatcsökkentő intézkedés, mint például egy biztonsági frissítés vagy a felhasználóknak szóló iránymutatások.

(5) Ha a releváns CSIRT nem képes megfelelően megvédeni a bejelentett információkat, a rosszindulatú szereplők érzékeny információkhoz férhetnek hozzá, és az egységes piac egészére kiterjedően kihasználhatják azokat. Ezért, amennyiben komoly aggályok merülnek fel azzal kapcsolatban, hogy a releváns CSIRT képes-e biztosítani a bejelentett információk bizalmas kezelését, az értesítést elsődlegesen fogadó CSIRT dönthet úgy, hogy csak az említett releváns CSIRT-nek szóló értesítés továbbítását halasztja el mindaddig, amíg a szóban forgó aggályokat nem kezelték. Ez például olyan helyzetekben fordulhat elő, amikor a releváns CSIRT-et egy olyan kiberbiztonsági incidens éri, amely befolyásolja a biztonságos működésre való képességét, vagy amikor bizonyíték vagy információ áll rendelkezésre azzal kapcsolatban, hogy a CSIRT képességeinek tekintetében jelentős hiányosságokat tártak fel – például ha a CSIRT erőforrásai olyan súlyosan korlátozottak, hogy ez veszélyezteti a feladatai ellátására való képességét, illetve ha a CSIRT elavult vagy sérülékeny szoftverek használatára van utalva.

(6) Annak érdekében, hogy a rosszindulatú szereplők ne férhessenek hozzá érzékeny információkhoz, ha egy kiberbiztonsági incidens veszélyt jelent az (EU) 2024/2847 rendelet 16. cikke alapján létrehozott egységes jelentéstételi platformra nézve, az értesítést elsődlegesen fogadó CSIRT-nek el kell halasztania az egységes jelentéstételi platformon keresztül történő továbbítást mindaddig, amíg a platform nem képes biztosítani a bejelentett információk bizalmas kezelését.

(7) Az (EU) 2024/2847 rendelet 16. cikke (2) bekezdésének első albekezdésével összhangban az értesítést elsődlegesen fogadó CSIRT-nek nem kell továbbítania az értesítést más releváns CSIRT-eknek, ha a gyártó azt jelzi, hogy a digitális elemeket tartalmazó terméket csak az értesítést elsődlegesen fogadó CSIRT tagállamának piacán hozták forgalomba.

(8) A Bizottság a felhatalmazáson alapuló jogi aktus tervezetének elkészítése során konzultált az érdekelt felekkel, és kikérte a véleményüket, valamint konzultált a digitális elemeket tartalmazó termékek kiberbiztonságával foglalkozó szakértői csoporttal is.

(9) Az (EU) 2024/2847 rendelet 14. cikkének (9) bekezdése értelmében a felhatalmazáson alapuló jogi aktus tervezetének elkészítése során a Bizottság szorosan együttműködött az (EU) 2022/2555 irányelv 15. cikke alapján létrehozott CSIRT-hálózattal és az ENISA-val.

ELFOGADTA EZT A RENDELETET:

1. cikk

Tárgy

E rendelet meghatározza az (EU) 2024/2847 rendelet 16. cikkének (2) bekezdésében említett, kiberbiztonsággal összefüggő indokok alkalmazására vonatkozó feltételeket, amelyek az említett rendelet 14. cikkének (1) és (3) bekezdésével, valamint 15. cikkének (1) és (2) bekezdésével összhangban lehetővé teszik az értesítést elsődlegesen fogadó, koordinátorként

kijelölt CSIRT számára, hogy elhalassza az értesítés továbbítását azon koordinátorként kijelölt CSIRT-eknek, amelyek területén a gyártó jelzése szerint a digitális elemeket tartalmazó terméket rendelkezésre bocsátották.

2. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „az értesítést elsődlegesen fogadó CSIRT”: az (EU) 2024/2847 rendelet 14. cikkének (1) és (3) bekezdésével, valamint 15. cikkének (1) és (2) bekezdésével összhangban az értesítést elsődlegesen fogadó, koordinátorként kijelölt CSIRT;
2. „releváns CSIRT”: olyan, koordinátorként kijelölt CSIRT, amelynek területén a gyártó jelzése szerint a digitális elemeket tartalmazó terméket rendelkezésre bocsátották.

3. cikk

A bejelentett információk jellegéből eredő, kiberbiztonsággal összefüggő indokok alkalmazásának feltételei

Az értesítést elsődlegesen fogadó CSIRT úgy dönthet, hogy a feltétlenül szükségesnél nem hosszabb ideig elhalasztja az értesítéseknek vagy azok részeinek a releváns CSIRT-ek részére történő továbbítását azokban az esetekben, amikor a bejelentett információk érzékenységére való tekintettel a továbbításból eredő kiberbiztonsági kockázatok meghaladják annak biztonsági előnyeit, és ezek a kockázatok nem csökkenthetők azáltal, hogy a megfelelő protokollok – például a jelzőlámpa-protokoll (TLP) vagy a műveletek engedélyezésére vonatkozó protokoll (PAP) – segítségével korlátozzák a bejelentések kezelését és további megosztását, valamint ha emellett az alábbi feltételek közül legalább egy teljesül:

a) a gyártó arról tájékoztatta az értesítést elsődlegesen fogadó CSIRT-et, hogy várhatóan 72 órán belül hatékony kockázatcsökkentő intézkedés – például biztonsági frissítés vagy a felhasználóknak szóló iránymutatás – áll majd rendelkezésre; ha az említett időtartam végéig nem áll rendelkezésre hatékony kockázatcsökkentő intézkedés, az értesítést elsődlegesen fogadó CSIRT továbbítja az értesítést a releváns CSIRT-eknek;

b) a bejelentésben szereplő információk a bejelentett, aktívan kihasznált sérülékenység jellegére tekintettel elegendőnek tekinthetők a kihasználására irányuló technika létrehozásához, különösen akkor, ha a sérülékenységet a korlátozott készségekkel és erőforrásokkal rendelkező szereplők is könnyen azonosíthatják és kihasználhatják; amint elérhetővé válik egy hatékony kockázatcsökkentő intézkedés – például biztonsági frissítés vagy a felhasználóknak szóló iránymutatás –, az értesítést elsődlegesen fogadó CSIRT továbbítja az értesítést a releváns CSIRT-eknek;

c) az értesítést elsődlegesen fogadó CSIRT elegendő információt tud megosztani a releváns CSIRT-ekkel annak biztosítása érdekében, hogy a releváns CSIRT-ek megfelelő kockázatcsökkentő intézkedéseket vezethessenek be; amint elérhetővé válik egy hatékony kockázatcsökkentő intézkedés – például biztonsági frissítés vagy a felhasználóknak szóló iránymutatás –, az értesítést elsődlegesen fogadó CSIRT továbbítja a teljes értesítést a releváns CSIRT-eknek;

d) az aktívan kihasznált sérülékenységre vonatkozó értesítést elsődlegesen fogadó CSIRT-et az említett sérülékenységről olyan összehangolt, a sérülékenységek

feltárására irányuló eljárás keretében tájékoztatták, amelynek tekintetében a szóban forgó CSIRT az (EU) 2022/2555 irányelv 12. cikkének (1) bekezdése szerint megbízható közvetítőként jár el; ebben az esetben az (EU) 2024/2847 rendelet 16. cikkének (6) bekezdésével összhangban az értesítést elsődlegesen fogadó CSIRT továbbítja az értesítést a releváns CSIRT-eknek, amint a halasztásra már nincs feltétlenül szükség, és az összehangolt, sérülékenységek feltárására irányuló eljárásban részt vevő felek beleegyezésüket adják a közzétételhez.

4. cikk

A kiberbiztonsággal összefüggő indokok alkalmazásának feltételei egy adott CSIRT tekintetében

Az értesítést elsődlegesen fogadó CSIRT dönthet úgy, hogy a feltétlenül szükséges időtartamra elhalasztja az értesítéseknek vagy azok részeinek egy adott, releváns CSIRT részére történő továbbítását, amennyiben:

a) a releváns CSIRT-et kiberbiztonsági incidens érintette, ami kétségessé teszi, hogy képes-e biztosítani a bejelentett információk bizalmas kezelését;

b) elegendő oka van azt feltételezni, hogy a releváns CSIRT képességei nem megfelelőek a bejelentett információk bizalmas kezelésének biztosításához.

Az első albekezdés a) pontjában említett esetekben az értesítést elsődlegesen fogadó CSIRT mindaddig elhalaszthatja a továbbítást, amíg a releváns CSIRT nem tájékoztatja az (EU) 2022/2555 irányelv 15. cikkében említett CSIRT-hálózatot arról, hogy ismét képes biztosítani az értesítések bizalmas kezelését.

Az első albekezdés b) pontjában említett esetekben az értesítést elsődlegesen fogadó CSIRT mindaddig elhalaszthatja a releváns CSIRT-nek való továbbítást, amíg az adott CSIRT nem igazolja, hogy orvosolta a feltárt hiányosságokat.

5. cikk

A kiberbiztonsággal összefüggő indokok alkalmazásának feltételei az egységes jelentéstételi platform tekintetében

Az értesítést elsődlegesen fogadó CSIRT dönthet úgy, hogy elhalasztja a bejelentéseknek az (EU) 2024/2847 rendelet 16. cikkével létrehozott egységes jelentéstételi platformon keresztül történő továbbítását, amennyiben az ENISA az említett rendelet 16. cikkének (4) bekezdésével összhangban arról tájékoztatta a CSIRT-hálózatot, hogy az egységes jelentéstételi platformot kiberbiztonsági incidens érintette, ami kétségessé teszi, hogy képes-e biztosítani a bejelentett információk bizalmas kezelését. Ilyen esetekben az értesítést elsődlegesen fogadó CSIRT mindaddig elhalaszthatja az egységes jelentéstételi platformon keresztül történő továbbítást, amíg az ENISA nem tájékoztatja a CSIRT-hálózatot arról, hogy a platform ismét képes biztosítani a bejelentések bizalmas kezelését.

6. 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, -án/-én. 2025.12.11.

a Bizottság részéről
elnök
Ursula VON DER LEYEN