2024/3143

2024.12.19.

A BIZOTTSÁG (EU) 2024/3143 VÉGREHAJTÁSI RENDELETE

(2024. december 18.)

az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló (EU) 2019/881 európai parlamenti és tanácsi rendelet 61. cikkének (5) bekezdése szerinti bejelentések feltételeinek, formátumainak és eljárásainak megállapításáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel 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) szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendeletre ([1]) és különösen annak 61. cikke (5) bekezdésére,

mivel:

(1) Az (EU) 2019/881 rendelet (kiberbiztonsági jogszabály) 61. cikkének (1) bekezdése értelmében a nemzeti kiberbiztonsági tanúsító hatóságok felelősek azért, hogy bejelentsék a Bizottságnak azokat a megfelelőségértékelő szervezeteket, amelyeket akkreditáltak és – adott esetben – meghatározott megbízhatósági szintű európai kiberbiztonsági tanúsítványok kiadására feljogosítottak; a nemzeti kiberbiztonsági tanúsító hatóságoknak továbbá naprakészen kell tartaniuk a bejelentéseket. Ezenkívül az (EU) 2019/881 rendelet 61. cikkének (2) bekezdése értelmében a Bizottságnak egy évvel az adott európai kiberbiztonsági tanúsítási rendszer hatálybalépését követően közzé kell tennie az *Európai Unió Hivatalos Lapjában* az adott rendszer keretében bejelentett megfelelőségértékelő szervezetek jegyzékét. A bejelentésekre vonatkozó harmonizált megközelítés biztosítása és a nemzeti kiberbiztonsági tanúsító hatóságokra vonatkozó bejelentési eljárás megkönnyítése érdekében e rendeletnek további pontosításokkal kell szolgálnia a bejelentésekkel kapcsolatos feltételek, formátumok és eljárások tekintetében. Ezeket a szempontokat fontos tisztázni az első közös kritériumokon alapuló kiberbiztonsági tanúsítási rendszer (EUCC) alkalmazására való tekintettel, amelyet az (EU) 2024/482 bizottsági végrehajtási rendelet ([2]) határoz meg.

(2) Ez a rendelet elismeri az (EU) 2019/881 rendelet és a vonatkozó uniós harmonizációs jogszabályok, többek között az (EU) 2024/2847 európai parlamenti és tanácsi rendelet (a kiberrezilienciáról szóló jogszabály) ([3]) közötti szinergiákat. Ezért azt javasoljuk, hogy a nemzeti kiberbiztonsági tanúsító hatóságok a 768/2008/EK európai parlamenti és tanácsi határozatban ([4]) említett, a Bizottság által kifejlesztett és kezelt elektronikus bejelentési eszközön keresztül nyújtsák be a Bizottság számára a bejelentésüket. A Bizottság azon kötelezettségének sérelme nélkül, hogy a bejelentett megfelelőségértékelő szervezetek jegyzékét közzé kell tennie az *Európai Unió Hivatalos Lapjában*, a jegyzéket a Bizottság által kifejlesztett és kezelt elektronikus bejelentési eszközön keresztül is nyilvánosan hozzáférhetővé kell tenni.

([1]) HL L 151., 2019.6.7., 15. o., ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) A Bizottság (EU) 2024/482 végrehajtási rendelete (2024. január 31.) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról (HL L, 2024/482, 2024.2.7., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([3]) Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, a 168/2013/EU 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).

([4]) A termékek forgalomba hozatalának közös keretrendszeréről, valamint a 93/465/EGK tanácsi határozat hatályon kívül helyezéséről szóló, 2008. július 9-i 768/2008/EK európai parlamenti és tanácsi határozat (HL L 218., 2008.8.13., 82. o., ELI: http://data.europa.eu/eli/dec/2008/768(1)/oj).

(3) Az akkreditált és – adott esetben – engedélyezett megfelelőségértékelő szervezetek bejelentése azt jelenti, hogy ezek a szervezetek megbízhatóan elvégzik az (EU) 2019/881 rendelet szerinti értékelési és tanúsítási tevékenységeket, hozzájárulva az európai kiberbiztonsági tanúsítási rendszerek általános hírnevéhez. Ezért alapvető fontosságú annak biztosítása, hogy a bejelentett megfelelőségértékelő szervezetek mindvégig megfeleljenek a követelményeknek és teljesítsék kötelezettségeiket. A bejelentett megfelelőségértékelő szervezetek közzétett jegyzékének pontosnak és naprakésznek kell lennie, tükrözve az (EU) 2019/881 rendeletben meghatározott követelményeknek és adott esetben az európai kiberbiztonsági tanúsítási rendszer egyedi vagy kiegészítő követelményeinek való megfelelésüket. E célból a nemzeti kiberbiztonsági tanúsító hatóságoknak az (EU) 2019/881 rendelet 61. cikke (1) bekezdésével összhangban indokolatlan késedelem nélkül értesíteniük kell a Bizottságot a bejelentést érintő bármely változásról.

(4) A nemzeti kiberbiztonsági tanúsító hatóságok felelősek annak biztosításáért, hogy a megfelelőségértékelő szervezetek megfeleljenek az (EU) 2019/881 rendeletnek és az európai kiberbiztonsági tanúsítási rendszereknek, és ezzel összefüggésben biztosítaniuk kell a bejelentések pontosságát. Ezeket a tevékenységeket kölcsönös felülvizsgálatnak vetik alá, amelynek eredménye alapján meg lehet határozni, mely változtatások szükségesek a hatékonyság növeléséhez. A nemzeti kiberbiztonsági tanúsító hatóságok a különböző körülmények között tudomásukra jutott aggályok alapján arra a megállapításra juthatnak, hogy egy megfelelőségértékelő szervezet már nem felel meg a vonatkozó követelményeknek. Adott esetben a kölcsönös felülvizsgálati mechanizmusok megállapításainak támogatniuk kell a nemzeti kiberbiztonsági tanúsító hatóságokat a bejelentett megfelelőségértékelő szervezetek folyamatos felkészültségének nyomon követésében. Emellett más nemzeti kiberbiztonsági tanúsító hatóságok, a Bizottság vagy az érdekelt felek is vethetnek fel a bejelentett megfelelőségértékelő szervezetek folyamatos felkészültségével kapcsolatos aggályokat a bejelentést tevő nemzeti kiberbiztonsági tanúsító hatóságnál.

(5) A megfelelőségértékelő szervezet bejelentésének felfüggesztéséről, korlátozásáról vagy visszavonásáról szóló döntés meghozatalakor a bejelentő nemzeti kiberbiztonsági tanúsító hatóságnak együtt kell működnie a 765/2008/EK európai parlamenti és tanácsi rendelet ([5]) alapján kijelölt nemzeti akkreditáló testülettel. Ez összhangban van az (EU) 2019/881 rendelettel, amely előírja, hogy a nemzeti kiberbiztonsági tanúsító hatóságoknak aktívan segíteniük és támogatniuk kell a nemzeti akkreditáló testületeket, és együtt kell működniük velük a nyomonkövetési és felügyeleti tevékenységük során. A bejelentés korlátozása azon esetekre vonatkozik, amikor az akkreditáció vagy adott esetben az engedély hatálya – és ezáltal a bejelentés hatálya – csökken.

(6) Az (EU) 2019/881 rendelet 54. cikke (1) bekezdésének n) pontja értelmében adott esetben valamennyi európai kiberbiztonsági tanúsítási rendszernek tartalmaznia kell a megfelelőségértékelő szervezetek nyilvántartásainak megőrzésére vonatkozó szabályokat. Ezért a bejelentés korlátozása, felfüggesztése vagy visszavonása esetén, vagy ha a bejelentett megfelelőségértékelő szervezet beszüntette tevékenységét, a bejelentő nemzeti kiberbiztonsági tanúsító hatóságnak gondoskodnia kell arról, hogy az adott megfelelőségértékelő szervezet nyilvántartásait az európai kiberbiztonsági tanúsítási rendszerben előírtaknak megfelelően biztonságos módon tárolják és a szükséges ideig megőrizzék.

(7) Az e rendeletben előírt intézkedések összhangban vannak az (EU) 2019/881 rendelet 66. cikkével létrehozott bizottság véleményével,

([5]) Az Európai Parlament és a Tanács 765/2008/EK rendelete (2008. július 9.) a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről (HL L 218., 2008.8.13., 30. o., ELI: http://data.europa.eu/eli/reg/2008/765/oj).

ELFOGADTA EZT A RENDELETET:

1. cikk

Tárgy

E rendelet megállapítja a megfelelőségértékelő szervezeteknek a nemzeti kiberbiztonsági tanúsító hatóságok által az (EU) 2019/881 rendelet 61. cikkének (1) bekezdése szerint történő bejelentésének feltételeit, formátumait és eljárásait.

2. cikk

Bejelentési eljárás

(1) Az (EU) 2019/881 rendelet 61. cikkének (1) bekezdésével összhangban a nemzeti kiberbiztonsági tanúsító hatóságok értesítik a Bizottságot azokról a megfelelőségértékelő szervezetekről, amelyek teljesítették az (EU) 2019/881 rendeletben meghatározott követelményeket és adott esetben az európai kiberbiztonsági tanúsítási rendszer egyedi vagy kiegészítő követelményeit.

(2) A nemzeti kiberbiztonsági tanúsító hatóság a 768/2008/EK határozatban említett, a Bizottság által kifejlesztett és kezelt elektronikus bejelentési eszközön keresztül értesíti a Bizottságot.

(3) Az értesítés a mellékletben szereplő információkat tartalmazza.

3. cikk

A megfelelőségértékelő szervezetek azonosító száma és jegyzéke

(1) A Bizottság a bejelentett megfelelőségértékelő szervezetet azonosító számmal látja el. Egyetlen azonosító szám kerül kiadásra, még abban az esetben is, ha a szervezetet több európai kiberbiztonsági tanúsítási rendszer vagy uniós jogi aktus alapján jelentették be.

(2) A bejelentett megfelelőségértékelő szervezetek jegyzékének a Bizottság által kifejlesztett és kezelt elektronikus bejelentési eszközön keresztül történő hozzáférhetővé tétele során a Bizottság feltünteti a bejelentett megfelelőségértékelő szervezetekhez rendelt azonosító számokat és azokat a tevékenységeket, amelyekre a bejelentetés irányul.

(3) Az ENISA az (EU) 2019/881 rendelet 50. cikkének (1) bekezdésében említett, az európai kiberbiztonsági tanúsítási rendszerekkel foglalkozó honlapján teszi közzé a bejelentett megfelelőségértékelő szervezetekre vonatkozó információkat.

4. cikk

A bejelentés változásai

(1) A nemzeti kiberbiztonsági tanúsító hatóság az (EU) 2019/881 rendelet 61. cikkének (1) bekezdésével összhangban a Bizottság által kifejlesztett és kezelt elektronikus bejelentési eszközön keresztül indokolatlan késedelem nélkül értesíti a Bizottságot a 2. cikkben említett bejelentés bármely későbbi változásáról.

(2) Amennyiben a nemzeti kiberbiztonsági tanúsító hatóság az (EU) 2019/881 rendeletben előírtak szerint a nemzeti akkreditáló testülettel együttműködve megállapítja, hogy a bejelentett megfelelőségértékelő szervezet már nem felel meg a rá vonatkozó követelményeknek vagy kötelezettségeknek, a nemzeti kiberbiztonsági tanúsító hatóság adott esetben korlátozza, felfüggeszti vagy visszavonja a bejelentést, attól függően, hogy mennyire súlyos az említett követelményeknek vagy kötelezettségeknek való meg nem felelés. A nemzeti kiberbiztonsági tanúsító hatóság ennek megfelelően a Bizottság által kifejlesztett és kezelt elektronikus bejelentési eszközön keresztül indokolatlan késedelem nélkül értesíti a Bizottságot.

(3) A bejelentés korlátozása, felfüggesztése vagy visszavonása esetén, vagy ha a bejelentett megfelelőségértékelő szervezet beszüntette tevékenységét, a bejelentő nemzeti kiberbiztonsági tanúsító hatóságnak meg kell tennie a megfelelő lépéseket annak érdekében, hogy az adott megfelelőségértékelő szervezet nyilvántartásait az európai kiberbiztonsági tanúsítási rendszerben előírtaknak megfelelően biztonságos módon tárolják és a szükséges ideig megőrizzék.

5. cikk

Hatálybalépés

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 18-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

MELLÉKLET

A megfelelőségértékelő szervezeteknek az európai kiberbiztonsági tanúsítási rendszerek vonatkozásában, az (EU) 2019/881 rendelet 61. cikkének (1) bekezdése értelmében történő bejelentésében feltüntetendő információk, az e rendelet 2. cikkének (3) bekezdésében előírtak szerint

(1) Általános információk:

1. A kiberbiztonsági tanúsítási rendszer megnevezése
2. Adott esetben megbízhatósági szint(ek) és a kapcsolódó megfelelőségértékelési eljárások (pl. alap, jelentős, magas)
3. Hatály (pl. az akkreditáció hatálya, termék-, szolgáltatás- és folyamatkategóriák vagy -típusok)

(2) A bejelentést tevő nemzeti kiberbiztonsági tanúsító hatósággal kapcsolatos információk:

1. Név
2. Ország
3. Postai cím
4. E-mail-cím(ek)
5. Telefonszám(ok)
6. Honlap

(3) A bejelentett megfelelőségértékelő szervezettel kapcsolatos információk:

1. Név
2. Ország
3. Postai cím
4. E-mail-cím(ek)
5. Telefonszám(ok)
6. Honlap

(4) Az akkreditációra vonatkozó információk:

1. Akkreditáció:
   a) Az akkreditáció dátuma
   b) Az akkreditáció hivatkozási száma
   c) Az akkreditáció hatálya
   d) Az akkreditáció érvényességének időtartama
2. Nemzeti akkreditáló testület:
   a) Név
   b) Ország
   c) Postai cím
   d) E-mail-cím(ek)
   e) Telefonszám(ok)
   f) Honlap

(5) Az engedélyre vonatkozó információk (adott esetben):

1. Engedély:
   a) Az engedély megadásának dátuma
   b) Az engedély hivatkozási száma
   c) Az engedély hatálya

d) Az engedély érvényességének időtartama

2. Engedélyező nemzeti kiberbiztonsági hatóság (ha eltér a bejelentő nemzeti kiberbiztonsági tanúsító hatóságtól):
   a) Név
   b) Ország
   c) Postai cím
   d) E-mail-cím(ek)
   e) Telefonszám(ok)
   f) Honlap

(6) További információk:

1. Az adott európai kiberbiztonsági tanúsítási rendszer keretében előírt bármely további információ
2. Egyéb igazoló dokumentumok