2025/301

2025.2.20.

A BIZOTTSÁG (EU) 2025/301 FELHATALMAZÁSON ALAPULÓ RENDELETE

(2024. október 23.)

az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek a jelentős IKT-vonatkozású eseményekről szóló kezdeti értesítés, időközi jelentés és zárójelentés tartalmát és határidejét, valamint a jelentős kiberfenyegetésekről szóló önkéntes értesítés tartalmát meghatározó szabályozástechnikai standardok tekintetében történő kiegészítéséről

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU, valamint az (EU) 2016/1011 rendelet módosításáról szóló, 2022. december 14-i (EU) 2022/2554 európai parlamenti és tanácsi rendeletre ([1]) és különösen annak 20. cikkének harmadik albekezdésére,

mivel:

(1) A jelentős IKT-vonatkozású eseményekkel kapcsolatos, az (EU) 2022/2554 rendelet 19. cikkének (4) bekezdésében említett értesítési és bejelentési követelmények harmonizálása és egyszerűsítése érdekében a jelentős IKT-vonatkozású események bejelentésére alkalmazandó határidőknek következetes megközelítést kell alkalmazniuk a pénzügyi szervezetek valamennyi típusa esetében. Ezen okokból kifolyólag a határidőknek a lehető legnagyobb mértékben összhangban kell lenniük az (EU) 2022/2555 európai parlamenti és tanácsi irányelvben ([2]) meghatározott követelményekkel, és legalábbis azokkal azonos hatásúnak kell lenniük.

(2) Annak elkerülése érdekében, hogy a pénzügyi szervezetekre indokolatlan jelentéstételi teher nehezedjen az IKT-vonatkozású esemény kezelése során, a kezdeti értesítés tartalmát a leglényegesebb információkra kell korlátozni. Ahhoz, hogy megfelelő felügyeleti intézkedéseket lehessen hozni, az illetékes hatóságoknak a lehető leggyorsabban tájékoztatást kell kapniuk a jelentős IKT-vonatkozású eseményekről, miután a pénzügyi szervezet egy adott IKT-vonatkozású eseményt jelentősként osztályozott. Következésképpen az (EU) 2022/2554 rendelet 19. cikke (4) bekezdésének a) pontjában említett kezdeti értesítés benyújtása határidejének a lehető legrövidebbnek kell lennie az IKT-vonatkozású esemény jelentősként való osztályozását követően, ugyanakkor rugalmasságot kell biztosítania – különösen az idő szempontjából nem kritikus szolgáltatási üzleti modellek esetében – arra az esetre, ha a pénzügyi szervezeteknek a tudomásszerzést követően több időre van szükségük az IKT-vonatkozású esemény kezelésére.

(3) A kezdeti értesítés kézhezvételét követően részletesebb tájékoztatással kell szolgálni az illetékes hatóságoknak az IKT-vonatkozású eseményről az időközi jelentésben, és minden releváns információt meg kell adni a zárójelentésben. A jelentésekben szereplő információknak lehetővé kell tenniük az illetékes hatóságok számára, hogy mélyrehatóbban értékeljék az IKT-vonatkozású eseményeket, és mérlegeljék az esetlegesen meghozandó felügyeleti intézkedéseket.

(4) Az (EU) 2022/2554 rendelet 20. cikke (1) bekezdése a) pontjának ii. alpontjában említett bejelentési határidőknek ezért egyensúlyt kell teremteniük annak szükségessége között, hogy az illetékes hatóságok gyorsan megkapják az információkat, és hogy a pénzügyi szervezeteknek elegendő idő álljon rendelkezésükre a teljeskörű és pontos információk beszerzésére.

(5) Figyelembe véve az (EU) 2022/2554 rendelet 20. cikke (1) bekezdésének a) pontjában meghatározott kritériumokat, a bejelentési határidők nem róhatnak aránytalan terhet a mikrovállalkozásokra és más, nem jelentős pénzügyi szervezetekre. A pénzügyi szervezetekre nehezedő aránytalan terhek elkerülése érdekében továbbá a bejelentési határidők meghatározása során figyelembe kell venni a hétvégéket és a munkaszüneti napokat.

([1]) HL L 333., 2022.12.27., 1. o., ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) 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. ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(6) Mivel a jelentős kiberfenyegetésekről szóló értesítéseket önkéntes alapon nyújtják be, az ilyen értesítések tartalma nem róhat terhet a pénzügyi szervezetekre, és korlátozottabbnak kell lennie, mint a jelentős IKT-vonatkozású események esetében kért információk.

(7) Ez a rendelet az európai felügyeleti hatóságok által a Bizottsághoz benyújtott szabályozástechnikai standardtervezeteken alapul.

(8) Az európai felügyeleti hatóságok nyilvános konzultációt folytattak az e rendelet alapját képező szabályozástechnikai standardtervezetekről, elemezték az esetleges kapcsolódó költségeket és hasznot, továbbá kikérték az 1093/2010/EU ([3]), az 1094/2010/EU ([4]) és az 1095/2010/EU európai parlamenti és tanácsi rendelet ([5]) 37. cikkével összhangban létrehozott érdekképviseleti csoportok tanácsát.

(9) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([6]) 42. cikkének (1) bekezdésével összhangban a Bizottság egyeztetett az európai adatvédelmi biztossal, aki 2024. július 22-én kedvező véleményt nyilvánított. A személyes adatok e rendelet hatálya alá tartozó kezelését az (EU) 2018/1725 rendelet alkalmazandó adatvédelmi elveivel és rendelkezéseivel összhangban kell végezni,

ELFOGADTA EZT A RENDELETET:

1. cikk

A jelentős IKT-vonatkozású eseményekről szóló kezdeti értesítésben, valamint az időközi jelentésben és a zárójelentésben benyújtandó általános információk

A pénzügyi szervezetek az (EU) 2022/2554 rendelet 19. cikkének (4) bekezdésében említett kezdeti értesítésbe, időközi jelentésbe és zárójelentésbe belefoglalják a következő általános információkat:

a) a beadvány típusa (kezdeti értesítés, időközi jelentés vagy zárójelentés);

b) a pénzügyi szervezet neve, jogalany-azonosító kódja (LEI), valamint a pénzügyi szervezetnek az (EU) 2022/2554 rendelet 2. cikkének (1) bekezdésében említettek szerinti típusa;

c) annak a szervezetnek a neve és azonosító kódja, amely a pénzügyi szervezetre vonatkozóan a kezdeti értesítést, illetve az időközi vagy zárójelentést benyújtja;

d) adott esetben az összesített kezdeti értesítésben, időközi jelentésben, illetve zárójelentésben foglalt valamennyi pénzügyi szervezet neve és LEI-kódja;

e) az illetékes hatósággal a jelentős IKT-vonatkozású eseménnyel kapcsolatos kommunikációért felelős személyek elérhetősége;

f) adott esetben a csoport anyavállalatának azonosítása, amelyhez a pénzügyi szervezet tartozik;

g) amennyiben az eseménynek van pénzügyi hatása, az a pénznem, amelyben az összegek szerepelnek.

([3]) Az Európai Parlament és a Tanács 1093/2010/EU rendelete (2010. november 24.) az európai felügyeleti hatóság (Európai Bankhatóság) létrehozásáról, a 716/2009/EK határozat módosításáról és a 2009/78/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 12. o., ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Az Európai Parlament és a Tanács 1094/2010/EU rendelete (2010. november 24.) az európai felügyeleti hatóság (az Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság) létrehozásáról, valamint a 716/2009/EK határozat módosításáról és a 2009/79/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 48. o., ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Az Európai Parlament és a Tanács 2010. november 24-i 1095/2010/EU rendelete az európai felügyeleti hatóság (Európai Értékpapír-piaci Hatóság) létrehozásáról, a 716/2009/EK határozat módosításáról és a 2009/77/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 84. o., ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) 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., 39–98. o., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. cikk

A kezdeti értesítésekben szolgáltatandó konkrét információk

Az (EU) 2022/2554 rendelet 19. cikke (4) bekezdésének a) pontjában említett kezdeti értesítéseknek tartalmazniuk kell legalább a következő konkrét információk mindegyikét:

a) a pénzügyi szervezet által az eseményhez rendelt hivatkozási kód;

b) az esemény észlelésének dátuma, észlelésének időpontja és osztályozása a (EU) 2024/1772 felhatalmazáson alapuló bizottsági rendelet ([7]) 8. cikkével összhangban;

c) az IKT-vonatkozású esemény ismertetése;

d) az (EU) 2024/1772 felhatalmazáson alapuló rendelet 1–8. cikkében meghatározott kritériumok, amelyek alapján a pénzügyi szervezet az IKT-vonatkozású eseményt jelentősnek minősítette;

e) az IKT-vonatkozású esemény által érintett tagállamok;

f) arra vonatkozó információ, hogy miként fedezték fel az IKT-vonatkozású eseményt;

g) az IKT-vonatkozású esemény eredetére vonatkozó információ (amennyiben rendelkezésre áll);

h) arra vonatkozó információ, hogy a pénzügyi szervezet aktivált-e üzletmenet-folytonossági tervet;

i) adott esetben az IKT-vonatkozású esemény osztályozásának jelentősről nem jelentősre történő módosítására vonatkozó információ;

j) minden egyéb lényeges információ (amennyiben rendelkezésre áll).

3. cikk

Az időközi jelentésekben szolgáltatandó konkrét információk

Az (EU) 2022/2554 rendelet 19. cikke (4) bekezdésének b) pontjában említett időközi jelentéseknek tartalmazniuk kell legalább a következő konkrét információk mindegyikét:

a) adott esetben az illetékes hatóság által az eseményhez rendelt hivatkozási kód;

b) az IKT-vonatkozású esemény előfordulásának dátuma és időpontja;

c) adott esetben az a dátum és időpont, amikor a pénzügyi szervezet helyreállította rendes tevékenységét;

d) arra vonatkozó információ, hogy milyen módon teljesültek az (EU) 2024/1772 felhatalmazáson alapuló rendelet 1–8. cikkében meghatározott kritériumok, amelyek alapján a pénzügyi szervezet az IKT-vonatkozású eseményt jelentősnek minősítette;

e) az IKT-vonatkozású esemény típusa;

f) adott esetben a fenyegetések és a fenyegető szereplő által alkalmazott technikák;

g) az érintett funkcionális területek és üzleti folyamatok;

h) az üzleti folyamatokat támogató, érintett infrastrukturális elemek;

i) az ügyfelek pénzügyi érdekeire gyakorolt hatás;

j) az IKT-vonatkozású eseményről más hatóságoknak történt bejelentésre vonatkozó információk;

k) a pénzügyi szervezet által az IKT-vonatkozású esemény utáni helyreállás érdekében tett vagy tervezett ideiglenes lépések vagy intézkedések;

l) adott esetben a fertőzöttségi mutatókra vonatkozó információk.

([7]) A Bizottság (EU) 2024/1772 felhatalmazáson alapuló rendelete (2024. március 13.) az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek az IKT-vonatkozású események és kiberfenyegetések osztályozására vonatkozó kritériumokat, a lényegességi küszöbértékeket és a jelentős eseményekkel kapcsolatos bejelentések részleteit meghatározó szabályozástechnikai standardok tekintetében történő kiegészítéséről (HL L, 2024/1772, 2024.6.25., ELI: http://data.europa.eu/eli/dir/2024/1772/oj).

4. cikk

A zárójelentésekben szolgáltatandó konkrét információk

Az (EU) 2022/2554 rendelet 19. cikke (4) bekezdésének c) pontjában említett zárójelentéseknek tartalmazniuk kell a következő konkrét információk mindegyikét:

a) az IKT-vonatkozású esemény kiváltó okaira vonatkozó információ;

b) az IKT-vonatkozású esemény megoldásának és a kiváltó oka(i) kezelésének dátuma és időpontja;

c) az IKT-vonatkozású esemény megoldására vonatkozó információk;

d) adott esetben a szanálási hatóságok számára releváns információk;

e) az IKT-vonatkozású eseményből eredő közvetlen és közvetett költségekre és veszteségekre vonatkozó információk, valamint a megtérülésekre vonatkozó információk;

f) adott esetben az ismétlődő IKT-vonatkozású eseményekre vonatkozó információk.

5. cikk

A kezdeti értesítés, az időközi jelentés és a zárójelentés benyújtási határideje

(1) A pénzügyi szervezetek az (EU) 2022/2554 rendelet 19. cikke (4) bekezdésének a), b) és c) pontjában említett kezdeti értesítést, időközi jelentést és zárójelentést az alábbi határidőkön belül nyújtják be:

a) a kezdeti értesítés esetében: a lehető leghamarabb, de mindenképpen azt követő négy órán belül, hogy egy IKT-vonatkozású esemény „jelentős IKT-vonatkozású esemény” osztályozást kapott, és legkésőbb attól a pillanattól számított 24 órán belül, hogy a pénzügyi szervezet tudomást szerzett az IKT-vonatkozású eseményről;

b) az időközi jelentés esetében: legkésőbb a kezdeti értesítés benyújtásától számított 72 órán belül, még akkor is, ha az esemény állapota vagy kezelése nem változott az (EU) 2022/2554 rendelet 19. cikke (4) bekezdésének b) pontjában említettek szerint. A pénzügyi szervezetek indokolatlan késedelem nélkül, minden esetben benyújtanak frissített időközi jelentést, amikor a szokásos tevékenységek helyreálltak;

c) a zárójelentés esetében: legkésőbb egy hónappal az időközi jelentés benyújtását követően vagy – adott esetben – a legutóbbi frissített időközi jelentést követően.

(2) Ha a pénzügyi szervezet az IKT-vonatkozású eseményt nem minősítette jelentősnek attól a pillanattól számított 24 órán belül, hogy a pénzügyi szervezet tudomást szerzett az IKT-vonatkozású eseményről, ugyanakkor azt később jelentősnek minősíti, akkor a pénzügyi szervezetnek az IKT-vonatkozású esemény jelentősnek minősítésétől számított négy órán belül be kell nyújtania a kezdeti értesítést.

(3) Azok a pénzügyi szervezetek, amelyek nem tudják az (1) bekezdésben meghatározott határidőn belül benyújtani a kezdeti értesítést, az időközi jelentést vagy a zárójelentést, erről indokolatlan késedelem nélkül, de legkésőbb az értesítés vagy a jelentés benyújtására vonatkozó határidőn belül tájékoztatják az illetékes hatóságot, és megindokolják a késedelmet.

(4) Amennyiben a kezdeti értesítés, az időközi jelentés vagy a zárójelentés benyújtásának határideje a jelentést benyújtó pénzügyi szervezet tagállamában hétvégi napra vagy munkaszüneti napra esik, a pénzügyi szervezet a kezdeti értesítést, az időközi jelentést vagy a zárójelentést a következő munkanapon déli 12 óráig is benyújthatja.

(5) A (4) bekezdés nem alkalmazandó a kezdeti értesítések vagy időközi jelentések hitelintézetek, központi szerződő felek, kereskedési helyszínek üzemeltetői és más, az (EU) 2022/2555 irányelv 3. cikke szerint alapvető vagy fontos szervezetként azonosított pénzügyi szervezetek általi benyújtására.

(6) Az illetékes hatóságok határozhatnak úgy, hogy a (4) bekezdés nem alkalmazandó az (5) bekezdésben említettektől eltérő azon pénzügyi szervezetek által benyújtandó kezdeti értesítésekre vagy időközi jelentésekre, amelyek nemzeti vagy uniós szinten a pénzügyi ágazat szempontjából jelentősek vagy rendszerszintű jellegűek. Az illetékes hatóságok erről a határozatukról értesítik az ekként azonosított pénzügyi szervezeteket. Az illetékes hatóság határozata csak azon események tekintetében alkalmazandó, amelyeket azt követően jelentettek be, hogy az illetékes hatóság értesítette az azonosított pénzügyi szervezeteket határozatáról.

6. cikk

A jelentős kiberfenyegetésekről szóló önkéntes értesítés tartalma

Az (EU) 2022/2554 rendelet 19. cikkének (2) bekezdésében említett jelentős kiberfenyegetésekkel kapcsolatos önkéntes értesítésnek a következők mindegyikét tartalmaznia kell:

a) a bejelentő pénzügyi szervezetre vonatkozó, az 1. cikkben meghatározottak szerinti általános információk;

b) a jelentős kiberfenyegetés észlelésének dátuma és időpontja, valamint a jelentős kiberfenyegetéssel kapcsolatos egyéb releváns időbélyegzők;

c) a jelentős kiberfenyegetés ismertetése;

d) a jelentős kiberfenyegetésnek a pénzügyi szervezetre, annak ügyfeleire vagy pénzügyi partnereire gyakorolt lehetséges hatására vonatkozó információk;

e) az (EU) 2024/1772 felhatalmazáson alapuló rendelet 1–8. cikkében meghatározott azon osztályozási kritériumok, amelyek alapján a kiberfenyegetés megvalósulása esetén jelentős eseményről szóló bejelentést kellett volna tenni;

f) a jelentős kiberfenyegetés állapotára és a fenyegetést jelentő tevékenységben bekövetkezett változásokra vonatkozó információk;

g) adott esetben a pénzügyi szervezet által a jelentős kiberfenyegetések megvalósulásának megelőzése érdekében tett intézkedések leírása;

h) más pénzügyi szervezeteknek vagy hatóságoknak a jelentős kiberfenyegetéssel kapcsolatos értesítésére vonatkozó információk;

i) adott esetben a fertőzöttségi mutatókra vonatkozó információk;

j) minden egyéb lényeges információ (amennyiben rendelkezésre áll).

7. 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. október 23-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN