AZ EURÓPAI KÖZPONTI BANK VÉLEMÉNYE

(2022. április 11.)

az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló európai parlamenti és tanácsi irányelv iránti javaslatról

(CON/2022/14)

(2022/C 233/03)

Bevezetés és jogalap

2020. december 16-án az Európai Bizottság elfogadta az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló európai parlamenti és tanácsi irányelv iránti javaslatot ([1]) (a továbbiakban: a javasolt irányelv). Az Európai Unió Tanácsa 2021. december 3-án megállapodott a javasolt irányelvre vonatkozó általános megközelítéséről ([2]). Az EKB véleményalkotásra szolgáló hatásköre az Európai Unió működéséről szóló szerződés 127. cikke (4) bekezdésének második albekezdésén alapul, mivel a javasolt irányelv olyan rendelkezéseket tartalmaz, amelyek az EKB hatáskörébe tartoznak, érintett különösen a Szerződés 127. cikke (2) bekezdésének negyedik franciabekezdésében, 127. cikkének (5) bekezdésében, illetve 127. cikkének (6) bekezdésében említett, a fizetési rendszerek zavartalan működésének előmozdítása, a hatáskörrel rendelkező hatóságoknak a pénzügyi rendszer stabilitására vonatkozó politikáik zavartalan megvalósításában való támogatása, és az EKB hitelintézetek prudenciális felügyeletével kapcsolatos feladatai. Az Európai Központi Bank eljárási szabályzata 17.5. cikkének első mondatával összhangban a Kormányzótanács fogadta el ezt a véleményt.

Általános észrevételek

Az EKB határozottan támogatja a javasolt irányelv arra irányuló célkitűzéseit, hogy növelje a kiberreziliencia szintjét az összes releváns ágazatban, csökkentse a belső piacon tapasztalható következetlenségeket, valamint az Unión belüli hatékony együttműködés biztosítása révén javítsa a helyzetismeret szintjét és a felkészülés és az elhárítás kollektív képességét.

Az EKB elismeri a javasolt irányelv és a pénzügyi szektor közötti szoros kapcsolat fenntartásának fontosságát, amelynek továbbra is a hálózati és információs rendszerek (NIS) ökoszisztémájának részét kell képeznie annak érdekében, hogy Unió-szerte előmozdítsa az információs és kommunikációs technológiákkal (IKT) kapcsolatos kockázatok következetes értékelését, és előmozdítsa a hatékony ágazatközi információcserét és együttműködést a kiberfenyegetések kezelése során. E célból lehetővé kell tenni a pénzügyi ágazat digitális működési rezilienciájáról szóló európai parlamenti és tanácsi rendelet (a továbbiakban: DORA-rendelet) iránti javaslat ([3]) szerinti illetékes hatóságok számára, hogy részt vegyenek a kiberbiztonsági együttműködési csoport stratégiai szakpolitikai megbeszélésein és technikai munkájában, valamint hogy információt cseréljenek és más módon is együttműködjenek a javasolt irányelvben említett egyedüli kapcsolattartó pontokkal és számítógép-biztonsági eseményekre reagáló nemzeti csoportokkal ([4]).

1. A javasolt irányelv hatálya

1.1 Az EKB értelmezése szerint a pénzügyi ágazatbeli szervezetek tekintetében a DORA-rendeletet olyan ágazatspecifikus jogszabálynak kell tekinteni, amely a kiberbiztonsági kockázatkezelésre és az események bejelentésére vonatkozóan olyan követelményeket vezet be, amelyek legalább egyenértékűek a javasolt irányelvben meghatározottakkal ([5]). Ezért a javasolt irányelv kiberbiztonsági kockázatkezelésre, jelentéstételi kötelezettségekre, információmegosztásra, felügyeletre és végrehajtásra vonatkozó rendelkezései nem alkalmazandók a DORA-rendelet hatálya alá tartozó pénzügyi szervezetekre ([6]). Amint azt a javasolt irányelv preambulumbekezdései

([1]) COM(2020) 823 final.
([2]) Elérhető a Tanács honlapján: www.consilium.europa.eu.
([3]) COM (2020) 595 final.
([4]) Lásd a pénzügyi ágazat digitális működési rezilienciájáról szóló európai parlamenti és tanácsi rendeletre vonatkozó javaslatról szóló, 2021. június 4-i CON/2021/20 európai központi banki vélemény 1.5. bekezdését (HL C 343., 2021.8.26., 1. o.). Az EKB valamennyi véleménye közzétételre kerül az EUR-Lexen. A DORA-rendelet 17. cikkének (5) bekezdése és 42. cikke, valamint a javasolt irányelv 11. cikke.
([5]) A javasolt irányelv 2. cikkének (6) bekezdése.
([6]) A javasolt irányelv (13) preambulumbekezdése és 2. cikkének (6) bekezdése.

egyértelművé teszik, a javasolt irányelv rendelkezései helyett a DORA-rendelet azon rendelkezéseit kell alkalmazni, amelyek az IKT-kockázatkezelési intézkedésekre, az IKT-val kapcsolatos események és az események jelentésére, a digitális működési reziliencia tesztekre, az információmegosztási megállapodásokra és a harmadik féllel kapcsolatos IKT-kockázatra vonatkoznak ([7]).

1.2 Az EKB azt is megjegyzi, hogy a Tanács a javasolt irányelvre vonatkozó általános megközelítésében olyan módosítást javasol ([8]), amely a javasolt irányelv alkalmazása alól kizárja az „olyan szervezeteket, amelyek az igazságszolgáltatás, a parlamentek és a központi bankok terén folytatnak tevékenységet". Az EKB értelmezése szerint a javasolt módosítás kiterjedne a Központi Bankok Európai Rendszerének (KBER) a Szerződés 127. cikkének (2) bekezdésében és a Központi Bankok Európai Rendszere és az Európai Központi Bank Alapokmányának (a továbbiakban: a KBER Alapokmánya) 3.1. cikkében meghatározott valamennyi alapvető feladatára és hatáskörére, például a fizetési rendszerek zavartalan működésének előmozdítására. E tekintetben az eurorendszer tulajdonában lévő és általa működtetett pénzügyi piaci infrastruktúrák – például a TARGET2 és a TARGET2-Securities – a központi bankoknak a javasolt irányelv alkalmazásából való kizárására irányuló tanácsi javaslat hatálya alá tartoznak.

2. **A KBER és az eurorendszer felvigyázási hatáskörei**

2.1 A KBER-nek az árstabilitás fenntartására irányuló elsődleges célja mellett és a Szerződés 127. cikkének (2) bekezdésével összhangban a KBER-en keresztül ellátandó egyik alapvető feladat a fizetési rendszerek zavartalan működésének előmozdítása ([9]). E feladat ellátása során az EKB és a nemzeti központi bankok megfelelő eszközöket bocsáthatnak rendelkezésre, az EKB pedig rendeleteket alkothat annak érdekében, hogy biztosítsák az Unión belüli és a más államokkal fenntartott elszámolási és fizetési rendszerek hatékony és megbízható működését ([10]). Felvigyázási szerepének gyakorlása során az EKB elfogadta a 795/2014/EU európai központi banki rendeletet (EKB/2014/28) ([11]) (a továbbiakban: SIPS-rendelet), amely a pénzügyi piaci infrastruktúrákra vonatkozó CPMI-IOSCO elveket ([12]) a közvetlenül alkalmazandó jogba ülteti át. A SIPS-rendelet követelményeket határoz meg mind a nagy értékű, mind a rendszerszempontból jelentős kis értékű fizetési rendszerekre vonatkozóan, függetlenül attól, hogy azok állami vagy magántulajdonban vannak. A SIPS-rendelet szerinti követelmények már magukban foglalják többek között a működési kockázatok kezelését és kibervédelmi keretrendszer létrehozását ([13]).

2.2 A rendszerszempontból jelentős fizetési rendszerek mellett az eurorendszer felvigyázási tevékenysége kiterjed a rendszerszempontból nem jelentős fizetési rendszerekre, elektronikus fizetési eszközökre, rendszerekre és mechanizmusokra, valamint egyéb infrastruktúrákra és kritikus szolgáltatókra, az eurorendszer felvigyázási politikai keretrendszerében ([14]) meghatározottak szerint. A javasolt irányelv hatálya nem terjed ki kifejezetten a fizetési rendszerekre és az eurorendszer felvigyázási tevékenységének hatálya alá tartozó egyéb megállapodásokra ([15]). Ugyanakkor, mivel a javasolt irányelv a minimális harmonizáció eszköze ([16]), a tagállamok által elfogadott végrehajtási jogszabályok végső soron átfedésben lehetnek az eurorendszer felvigyázási hatáskörével. Ennek elkerülése érdekében a javasolt irányelv preambulumbekezdéseiben kifejezetten el kellene ismerni a KBER-nek a Szerződés és a KBER Alapokmánya szerinti hatásköreit, valamint az eurorendszernek a SIPS-rendelet és általában az eurorendszer felvigyázási politikai keretrendszere szerinti hatásköreit.

([7]) A javasolt irányelv (13) preambulumbekezdése.
([8]) A javasolt irányelvre vonatkozó tanácsi általános megközelítésben a 2. cikk (3a) bekezdése első albekezdésének b) pontja.
([9]) Az EUMSZ 127. cikkének (2) bekezdése, amint azt a KBER Alapokmányának 3.1. cikke is tükrözi.
([10]) A KBER Alapokmányának 22. cikke.
([11]) Az Európai Központi Bank 795/2014/EU rendelete (2014. július 3.) a rendszerszempontból jelentős fizetési rendszerekre vonatkozó felvigyázási követelményekről (EKB/2014/28) (HL L 217., 2014.7.23., 16. o.).
([12]) Lásd: Fizetési és Elszámolási Rendszerek Bizottsága (CPSS) és az Értékpapír-felügyeletek Nemzetközi Szervezetének (IOSCO) Technikai Bizottsága: Principles for Financial Market Infrastructures (A pénzügyi piaci infrastruktúrákra vonatkozó alapelvek), 2012. április, elérhető a Nemzetközi Fizetések Bankjának honlapján: www.bis.org. A D. felelősségi kör kimondja, hogy „a CPSS és az IOSCO valamennyi tagjával szemben elvárás, hogy joghatóságukon belül a jogi keret által megengedett legteljesebb mértékben alkalmazzák az elveket az érintett pénzügyi piaci szereplőkre".
([13]) A 795/2014/EU rendelet (EKB/2014/28) 15. cikke.
([14]) Eurosystem oversight policy framework (Az eurorendszer felvigyázási politikai keretrendszere), felülvizsgált változat (2016. július), elérhető az EKB honlapján: www.ecb.europa.eu.
([15]) A javasolt irányelv 2. cikke és a javasolt irányelv I. és II. melléklete.
([16]) A javasolt irányelv 3. cikke.

3. **Harmadik féllel kapcsolatos IKT-kockázat, nagyszabású események és válságok kezelése, információmegosztás és nemzeti kiberbiztonsági stratégia**

3.1 *Harmadik féllel kapcsolatos IKT-kockázatok kezelése*

3.1.1 A javasolt irányelv felhatalmazza az illetékes hatóságokat arra, hogy az alapvető szervezetekkel kapcsolatos végrehajtási hatáskörük gyakorlása során kötelező erejű utasításokat vagy végzést adjanak ki, amelyek előírják e szervezetek számára, hogy orvosolják a feltárt hiányosságokat vagy a javasolt irányelvben foglalt kötelezettségek megsértését ([17]). Ugyanakkor a DORA-rendelet alapján kijelölt „vezető felvigyázó" ajánlásokat fogalmazhat meg a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók számára a kiszervezés gyakorlatával és a harmadik félnek minősülő IKT-szolgáltatók koncentrációjával járó potenciális rendszerszintű kockázatok kezelése érdekében ([18]).

3.1.2 Tekintettel arra, hogy a javasolt irányelv szerinti alapvető szervezet a DORA-rendelet alapján harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatónak is kijelölhető, az EKB megismétli ([19]), hogy el kell kerülni az egymásnak ellentmondó ajánlások és kötelező erejű utasítások kiadását. E tekintetben az EKB üdvözli a Tanácsnak a javasolt irányelvre vonatkozó általános megközelítését. E megközelítés szerint az illetékes hatóságoknak tájékoztatniuk kell a DORA-rendelet alapján létrehozott „felvigyázási fórumot", ha a DORA-rendelet értelmében harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóként kijelölt alapvető szervezettel kapcsolatban gyakorolják felügyeleti és végrehajtási hatásköreiket ([20]).

3.2 *Nagyszabású események és válságok kezelése*

3.2.1 A javasolt irányelvnek megfelelően ([21]) a tagállamoknak ki kell jelölniük egy vagy több, a nagyszabású események és válságok kezeléséért felelős illetékes hatóságot. Amint azt a javasolt irányelv preambulumbekezdései egyértelművé teszik, a nagyszabású esemény olyan eseményt jelent, amelynek legalább két tagállamra jelentős hatása van, vagy amelyből származó zavar meghaladja egy tagállam elhárítási képességét. A nagyszabású események eszkalálódhatnak, és olyan teljes körű válsággá válhatnak, amely akadályozza a belső piac megfelelő működését ([22]).

3.2.2 Míg a DORA-rendelet keretében kijelölt illetékes hatóságok továbbra is felelősek a pénzügyi szervezeteket érintő kiberbiztonsági események kezeléséért, a javasolt irányelv alapján létrehozott struktúrákkal és hatóságokkal való együttműködés kulcsfontosságú lesz az Unió-szerte összehangolt reagálás biztosításához. E célból az EKB üdvözölné a DORA-rendelet keretében kijelölt illetékes hatóságok – közöttük az EKB – részvételét az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatában ([23]) (EU-CyCLONe), amennyiben a nagyszabású kiberbiztonsági események és válságok a pénzügyi szektort érintik.

3.3 *Információmegosztás*

3.3.1 A fentieknek megfelelően az EKB határozottan támogatja a DORA-rendelet keretében kijelölt illetékes hatóságok és a javasolt irányelv alapján létrehozott struktúrák és hatóságok közötti együttműködést. Közelebbről, a hatóságok közötti információmegosztás lehetővé teheti az ágazatközi tanulást, hozzájárulhat a kibertámadások megelőzéséhez és hatékony kezeléséhez, valamint Unió-szerte előmozdíthatja az IKT-val kapcsolatos kockázatok következetes értékelését. Mindazonáltal az EKB hangsúlyozza, hogy az információcserének akkor kell történnie, ha világosan meghatározott minősítési és információmegosztási mechanizmusok állnak fenn, a bizalmas jelleg biztosítására szolgáló megfelelő biztosítékokkal együtt ([24]). Az EKB üdvözli a Tanácsnak a javasolt irányelvre vonatkozó általános

([17]) A javasolt irányelv 29. cikkének (4) bekezdése.
([18]) A DORA-rendelet 31. cikke.
([19]) Lásd a CON/2021/20 vélemény 1.2. bekezdését.
([20]) A javasolt irányelvre vonatkozó tanácsi általános megközelítés 29. cikkének (10) bekezdése.
([21]) A javasolt irányelv 7. cikkének (1) bekezdése.
([22]) A javasolt irányelv (27) preambulumbekezdése.
([23]) A javasolt irányelv 14. cikke.
([24]) Lásd a CON/2021/20 vélemény 1.5. bekezdését.

megközelítését, amely a releváns információk hatóságok közötti rendszeres cseréjét ([25]), az információcsere mechanizmusát meghatározó együttműködési megállapodások létrehozását ([26]), valamint az eseményekre vonatkozó bejelentések automatikus és közvetlen továbbítását javasolja ([27]). E tekintetben biztosítani kell, hogy a DORA-rendelet szakmai titoktartásra vonatkozó rendelkezései ([28]) vagy a vonatkozó ágazatspecifikus jogszabályok ([29]) értelmében bizalmasnak minősülő információkat csak akkor lehet megosztani a javasolt irányelvben említett illetékes hatóságokkal, ha ez az információcsere szükséges ahhoz, hogy az illetékes hatóságok alkalmazni tudják a javasolt irányelv rendelkezéseit ([30]).

3.4 *Nemzeti kiberbiztonsági stratégia*

3.4.1 A javasolt irányelv értelmében a tagállamoknak nemzeti kiberbiztonsági stratégiát kell elfogadniuk, amely meghatározza a stratégiai célokat, valamint a megfelelő politikai és szabályozási intézkedéseket a magas szintű kiberbiztonság elérése és fenntartása céljából ([31]). Amint azt a javasolt irányelv preambulumbekezdései egyértelművé teszik, a tagállamoknak továbbra is be kell vonniuk a pénzügyi ágazatot kiberbiztonsági stratégiájukba ([32]). Indikatív jelleggel, nemzeti kiberbiztonsági stratégiáik részeként a tagállamoknak olyan szakpolitikákat kell elfogadniuk, amelyek a szervezetek által szolgáltatásaik nyújtásához használt IKT-termékek és -szolgáltatások ellátási láncában a kiberbiztonsággal foglalkoznak. A pénzügyi ágazat tekintetében a nemzeti kiberbiztonsági stratégiáknak összhangban kell lenniük a DORA-rendeletből eredő szabályozási kerettel. E tekintetben az EKB úgy véli, hogy további pontosításokra van szükség annak biztosítása érdekében, hogy a nemzeti kiberbiztonsági stratégiák összhangban legyenek az ágazatspecifikus jogszabályokkal.

Abban az esetben, ahol az EKB a javasolt irányelv módosítására tesz javaslatot, külön technikai munkadokumentum tartalmazza a szövegezési javaslatokat és az azokhoz fűzött magyarázatot. A technikai munkadokumentum angol nyelven elérhető az EUR-Lexen.

Kelt Frankfurt am Mainban, 2022. április 11-én.

az EKB elnöke
Christine LAGARDE

([25]) A javasolt irányelvre vonatkozó tanácsi általános megközelítés 11. cikkének (5) bekezdése.
([26]) A javasolt irányelvre vonatkozó tanácsi általános megközelítés (23a) preambulumbekezdése.
([27]) A javasolt irányelvre vonatkozó tanácsi általános megközelítés (23a) preambulumbekezdése.
([28]) A DORA-rendelet 49. cikke.
([29]) Az Európai Parlament és a Tanács 2013/36/EU irányelve (2013. június 26.) a hitelintézetek tevékenységéhez való hozzáférésről és a hitelintézetek prudenciális felügyeletéről, a 2002/87/EK irányelv módosításáról, a 2006/48/EK és a 2006/49/EK irányelv hatályon kívül helyezéséről (HL L 176., 2013.6.27., 338. o.), 53-62. cikk.
([30]) A javasolt irányelv 2. cikkének (5) bekezdése és 11. cikkének (4) bekezdése.
([31]) A javasolt irányelv 5. cikke.
([32]) A javasolt irányelv (13) preambulumbekezdése.