III

(Előkészítő jogi aktusok)

EURÓPAI KÖZPONTI BANK

AZ EURÓPAI KÖZPONTI BANK VÉLEMÉNYE

(2021. június 4.)

a pénzügyi ágazat digitális működési rezilienciájáról szóló európai parlamenti és tanácsi rendeletre vonatkozó javaslatról

(CON/2021/20)

(2021/C 343/01)

Bevezetés és jogalap

2020. december 22-én, 23-án és 29-én az Európai Központi Bank (EKB) az Európai Unió Tanácsától és az Európai Parlamenttől azt a felkérést kapta, hogy alkosson véleményt a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK rendelet, a 648/2012/EU rendelet, a 600/2014/EU rendelet, valamint a 909/2014/EU rendelet módosításáról szóló európai parlamenti és tanácsi rendelet iránti javaslatról ([1]) (a továbbiakban: javasolt rendelet), valamint a 2006/43/EK irányelv, a 2009/65/EK irányelv, a 2009/138/EK irányelv, a 2011/61/EU irányelv, a 2013/36/EU irányelv, a 2014/65/EU irányelv, az (EU) 2015/2366 irányelv és az (EU) 2016/2341 irányelv módosításáról szóló irányelv iránti javaslatról ([2]) (a továbbiakban: javasolt módosító irányelv, a javasolt rendelettel együtt: a javasolt jogi aktusok).

Az EKB véleményalkotásra szolgáló hatásköre az Európai Unió működéséről szóló szerződés 127. cikkének (4) bekezdésén és 282. cikkének (5) bekezdésén alapul, mivel a javasolt jogi aktusok olyan rendelkezéseket tartalmaznak, amelyek az EKB hatáskörébe tartoznak, érintett különösen a Szerződés 127. cikke (2) bekezdésének első és negyedik francia bekezdésében, 127. cikkének (5) bekezdésében, illetve 127. cikkének (6) bekezdésében említett, a monetáris politika meghatározása és végrehajtása, 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.

1. Általános észrevételek

1.1 Az EKB üdvözli a javasolt rendeletet, amelynek célja a pénzügyi ágazat kiberbiztonságának és működési rezilienciájának javítása. Az EKB üdvözli különösen a javasolt rendelet célját, amely arra irányul, hogy javítsa a pénzügyi szolgáltatások belső piacának kiépítését és működését biztosító feltételeket, továbbá elhárítsa annak akadályait azzal, hogy harmonizálja az információs és kommunikációs technológiákhoz (IKT) kapcsolódó kockázatok kezelése és bejelentése, a tesztelés, valamint a harmadik féltől eredő IKT-kockázatok területén alkalmazandó szabályokat. Az EKB üdvözli továbbá a javasolt rendelet azon célját, hogy észszerűsítse és harmonizálja az egymást átfedő szabályozási követelményeket és felügyeleti elvárásokat, amelyek jelenleg az uniós jog alapján a pénzügyi szervezetekre vonatkoznak.

1.2 Az EKB értelmezése szerint a javasolt rendelet az alapvető szolgáltatást nyújtó szereplőként azonosított pénzügyi szervezetek tekintetében ([3]) az (EU) 2016/1148 európai parlamenti és tanácsi irányelv ([4]) (a továbbiakban: NIS-irányelv) 1. cikkének (7) bekezdése értelmében ágazatspecifikus jogszabálynak *(lex specialis)* minősül; ez azt jelenti, hogy a javasolt rendelet szerinti követelmények főszabály szerint elsőbbséget élveznének a NIS-irányelvvel szemben. A gyakorlatban az alapvető szolgáltatást nyújtó szereplőként azonosított pénzügyi szervezetek ([5]) a biztonsági eseményeket a javasolt rendelet, nem pedig a NIS-irányelv

([1]) COM(2020) 595 final.
([2]) COM (2020) 596 final.
([3]) Lásd a javasolt rendelet 1. cikkének (2) bekezdését.
([4]) Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).
([5]) Lásd a NIS-irányelv 5. cikkét.

alapján jelentenék be. Míg az EKB üdvözli a biztonsági események bejelentése terén a pénzügyi szervezetekre vonatkozó, potenciálisan egymást átfedő követelmények csökkentését, további figyelmet kell szentelni a javasolt rendelet és a NIS-irányelv közötti kölcsönhatásnak. Például a javasolt rendelet alapján a vezető felvigyázó ajánlásokat bocsáthat ki egy harmadik félnek minősülő IKT-szolgáltatóra ([6]) vonatkozóan ([7]). Ugyanakkor ugyanaz a harmadik félnek minősülő IKT-szolgáltató a NIS-irányelv alapján alapvető szolgáltatásokat nyújtó szereplőnek minősülhet, és az illetékes hatóság kötelező erejű utasításokat fogadhat el vele szemben ([8]). Ebben az esetben a harmadik félnek minősülő IKT-szolgáltatóra vonatkozhatnak egymással ellentétes, a javasolt rendelet alapján kibocsátott ajánlások és a NIS-irányelv alapján kibocsátott kötelező erejű utasítások. Az EKB azt javasolja, hogy az uniós jogalkotó szervek vizsgálják tovább a javasolt rendelet és a NIS-irányelv közötti potenciális következetlenségeket, amelyek akadályozhatják a pénzügyi szervezetekre vonatkozó, egymást átfedő és egymásnak ellentmondó követelmények harmonizálását és csökkentését.

1.3 Az EKB értelmezése szerint 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 javaslat ([9]) (a továbbiakban: javasolt NIS 2 irányelv) alapján a majdnem bekövetkezett (near miss) események ([10]) adatszolgáltatási kötelezettségek tárgyát fogják képezni ([11]). Noha a javasolt NIS 2 irányelv (39) preambulumbekezdése hivatkozik a „majdnem bekövetkezett (near miss) esemény" kifejezés jelentésére, nem világos, hogy azt kívánják-e megkövetelni, hogy a javasolt rendelet 2. cikkében felsorolt pénzügyi szervezetek jelentsék a majdnem bekövetkezett (near miss) eseményeket. E tekintetben, továbbá figyelemmel arra, hogy a majdnem bekövetkezett (near miss) események csak a bekövetkezésüket követően azonosíthatók ilyenként, az EKB üdvözölné, ha megfelelő időben értesítést kapna a jelentős majdnem bekövetkezett (near miss) eseményekről, ahogy az jelenleg a kiberbiztonsági események esetében történik. Az EKB a javasolt rendelet és a javasolt NIS 2 irányelv közötti nagyobb mértékű koordinációt javasol azon adatszolgáltatás pontos terjedelmének egyértelművé tétele érdekében, amely valamely pénzügyi szervezetre e két különálló, azonban egymással összefüggő uniós jogszabály alapján vonatkozhat. Ugyanakkor a majdnem bekövetkezett (near miss) eseményeket meg kell határozni és a jelentőségüket egyértelművé tevő rendelkezéseket kell kidolgozni.

1.4 Az EKB üdvözli, hogy a pénzügyi szervezeteket arra ösztönöznék, hogy önkéntes alapon osszanak meg kiberfenyegetettségi információkat egymás között a kiberreziliencia terén fennálló helyzetük javítása és támogatása érdekében. Az EKB maga segítséget nyújtott a piacvezérelt kiberfenyegetettségi információmegosztási kezdeményezéshez (CIISI-EU), és az útmutatót elérhetővé tette mindenki számára, aki ilyen kezdeményezést kíván kialakítani és támogatni ([12]).

1.5 Az EKB támogatja a javasolt rendelet céljára az illetékes hatóságok, az európai felügyeleti hatóságok és a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) közötti együttműködést ([13]). Az információcsere alapvető jelentőséggel bír az Unió működési rezilienciájának biztosítása szempontjából, mivel a hatóságok közötti információmegosztás és együttműködés hozzájárulhat a kibertámadások megelőzéséhez és elősegítheti az IKT-fenyegetések terjedésének csökkentését. Elő kell mozdítani az IKT-hoz kapcsolódó kockázatok egységes értelmezését, és az Unió egészében biztosítani kell az ilyen kockázatok következetes értékelését. Kiemelt jelentőséggel bír, hogy az illetékes hatóságok az egyedüli kapcsolattartó ponttal ([14]) és a nemzeti CSIRT-ekkel csak akkor osszanak meg információkat ([15]), ha világosan meghatározott minősítési és információmegosztási mechanizmusok állnak fenn, a bizalmas jelleg biztosítására szolgáló megfelelő biztosítékokkal együtt.

1.6 Végül, az EKB üdvözölné, ha a javasolt rendelet alapján a személyes adatokra és az adatmegőrzésre vonatkozó szabályok kerülnének bevezetésre. A megőrzési időszak hosszának figyelembe kell vennie az illetékes hatóságok által a javasolt rendelet alapján fennálló kötelezettségeik részeként adott esetben elvégzendő vizsgálatot, ellenőrzést, információkérést, közlést, közzétételt, értékelést, valamint felvigyázási és felügyeleti tervek elkészítését. E tekintetben 15 éves megőrzési időszak megfelelő lenne. Ezt az

([6]) Lásd a javasolt rendelet 3. cikkének 15. pontját.
([7]) Lásd a javasolt rendelet 31. cikke (1) bekezdésének d) pontját.
([8]) Lásd a NIS-irányelv 15. cikkének (3) bekezdését.
([9]) COM (2020) 823 final.
([10]) Olyan események, amelyek potenciálisan kárt okozhattak volna, de a teljes bekövetkezésüket sikeresen megakadályozták; lásd a NIS 2 irányelv (39) preambulumbekezdését.
([11]) Lásd a NIS 2 irányelv 11. cikkét.
([12]) Kiberfenyegetettségi információmegosztási kezdeményezés (Cyber threat Intelligence Information Sharing Initiative, CIISI-EU) elérhető az EKB honlapján: www.ecb.europa.eu.
([13]) Lásd a javasolt rendelet 42. cikkét.
([14]) Lásd a NIS-irányelv 8. cikkének (3) bekezdését.
([15]) Lásd még a NIS 2 irányelv 11., 26. és 27. cikkét.

adatmegőrzési időszakot le lehetne rövidíteni vagy meg lehetne hosszabbítani, ahogy az adott esetben szükséges. E tekintetben az EKB azt javasolja, hogy az uniós jogalkotó szervek a személyes adatokra és az adatmegőrzésre vonatkozó megfelelő rendelkezés megfogalmazása során vegyék figyelembe az adattakarékosság elvét, valamint a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott további adatkezelést ([16]).

2. A felvigyázással, valamint az értékpapír-elszámolással és kiegyenlítéssel kapcsolatos különös észrevételek

2.1 *A KBER és az eurorendszer felvigyázási hatáskörei*

2.1.1 Az eurorendszer alapvető monetáris politikai feladataival szoros összefüggésben a Szerződés és a Központi Bankok Európai Rendszerének alapokmánya (a továbbiakban: a KBER Alapokmánya) úgy rendelkezik, hogy az eurorendszer ellátja az elszámolási és fizetési rendszerek felvigyázását. A Szerződés 127. cikke (2) bekezdésének negyedik francia bekezdése értelmében, amelyet a KBER Alapokmányának 3.1. cikke is tükröz, a Központi Bankok Európai Rendszerén (KBER) keresztül ellátandó egyik alapvető feladat a fizetési rendszerek zavartalan működésének előmozdítása. 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 ([17]). Az EKB felvigyázási szerepének megfelelően elfogadta a 795/2014/EU európai központi banki rendeletet (EKB/2014/28) (a továbbiakban: SIPS-rendelet) ([18]). A SIPS-rendelet – előíró jellegű formában – végrehajtja a Fizetési és Elszámolási Rendszerek Bizottsága és az Értékpapír-felügyeletek Nemzetközi Szervezetének Technikai Bizottsága által kibocsátott, a pénzügyi piaci infrastruktúrákra vonatkozó 2012. áprilisi alapelveket ([19]), amelyek jogilag kötelező erejűek, és az – akár eurorendszerbeli központi bank, akár magánszervezet által üzemeltetett – nagy értékű fizetési rendszerekre és rendszerszempontból jelentős kis értékű fizetési rendszerekre egyaránt kiterjednek. Az eurorendszer felvigyázási politikai keretrendszere ([20]) a fizetési eszközöket a „fizetési rendszerek szerves részeként" azonosítja, és így bevonja azokat a felvigyázás hatálya alá. A fizetési eszközökre vonatkozó felvigyázási keretrendszer jelenleg felülvizsgálat alatt áll ([21]). E keretrendszerben a fizetési eszköz (például kártya, átutalás, beszedés, elektronikuspénz-átutalás és digitális fizetési token ([22])) úgy kerül meghatározásra, mint a pénzforgalmi szolgáltatás igénybe vevője és a pénzforgalmi szolgáltató közötti megállapodás tárgyát képező, érték átruházásának ([23]) kezdeményezésére használt, személyre szabott eszköz (vagy eszközök) és/vagy eljárások.

2.1.2 A fentiekre tekintettel az EKB üdvözli, hogy a fent említett felvigyázási keretrendszerek alkalmazására tekintettel a javasolt rendelet hatálya alól kizárásra kerültek a 98/26/EK európai parlamenti és tanácsi irányelv ([24]) 2. cikkének p) pontjában meghatározott rendszerüzemeltetők, továbbá a fizetési rendszerek (a

([16]) Lásd 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 szóló, 2018. október 23-i (EU) 2018/1725 európai parlamenti és tanácsi rendelet (HL L 295., 2018.11.21., 39. o.) 4. cikkének b) pontját és 13. cikkét.

([17]) Lásd a KBER Alapokmányának 22. cikkét.

([18]) 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.).

([19]) Elérhető a Nemzetközi Fizetések Bankjának honlapján: www.bis.org.

([20]) Eurosystem oversight policy framework (Az eurorendszer felvigyázási politikai keretrendszere), felülvizsgált változat (2016. július), elérhető az EKB honlapján: www.ecb.europa.eu.

([21]) Lásd: a 2020. októberi felülvizsgált és egységes szerkezetbe foglalt Eurosystem oversight framework for electronic payment instruments, schemes and arrangements (PISA framework) (Az eurorendszer elektronikus fizetési eszközökre, modellekre és megállapodásokra vonatkozó felvigyázási keretrendszere, a továbbiakban: PISA-keretrendszer), elérhető az EKB honlapján: www.ecb.europa.eu.

([22]) A digitális fizetési token érték digitális megjelenítője, amelyet másutt rögzített követelések vagy eszközök támasztanak alá, és amely érték végfelhasználók közötti átutalását teszi lehetővé. A digitális fizetési tokenek kialakításuktól függően előirányozhatják úgy az érték átutalását, hogy az nem feltétlenül jár központi harmadik fél részvételével és/vagy fizetési számlák használatával.

([23]) „Érték átruházása": „A fizető fél által vagy nevében, vagy a kedvezményezett által kezdeményezett azon aktus, hogy pénzt vagy digitális fizetési tokeneket utal át, vagy valamely felhasználói számlára készpénzt fizet be vagy onnan készpénzt vesz fel, függetlenül a fizető fél és a kedvezményezett közötti alapkötelezettségektől. Az átruházás járhat egyetlen vagy több pénzforgalmi szolgáltató részvételével." Az „érték átruházásának" a PISA-keretrendszer szerinti e meghatározása eltér a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és az 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről szóló, 2015. november 25-i (EU) 2015/2366 európai parlamenti és tanácsi irányelv (HL L 337., 2015.12.23., 35. o.) szerinti „pénz" átutalásától. Az említett irányelvben meghatározott „készpénz-helyettesítő fizetési eszköz" összefüggésében az „érték átruházása" csak „pénz" átutalására utalhat. Ezen irányelv alapján a „pénz" nem foglalja magában a digitális fizetési tokeneket, kivéve, ha a tokenek elektronikus pénzként (vagy hipotetikusabban: számlapénzként) sorolhatók be.

([24]) Az Európai Parlament és a Tanács 98/26/EK irányelve (1998. május 19.) a fizetési és értékpapír-elszámolási rendszerekben az elszámolások véglegességéről (HL L 166., 1998.6.11., 45. o.).

központi bankok által üzemeltetetteket is beleértve), fizetési modellek és fizetési megállapodások. Ezen okokból a javasolt rendelet preambulumbekezdéseiben világosan meg kell jelölni a KBER-nek a Szerződés alapján és az eurorendszernek a SIPS-rendelet alapján fennálló hatásköreit.

2.1.3 Az EKB hasonlóképpen üdvözli, hogy a javasolt rendeletben foglalt felvigyázási keretrendszer alkalmazása alól kizárásra kerülnek azon harmadik félnek minősülő IKT-szolgáltatók, amelyek a Szerződés 127. cikkének (2) bekezdésében említett feladatok támogatására létrehozott felvigyázási keretrendszerek hatálya alá tartoznak ([25]). E tekintetben az EKB hangsúlyozni kívánja, hogy a monetáris minőségükben eljáró KBER központi bankokra ([26]), valamint a TARGET2-n, a TARGET2-Securitesen (T2S) ([27]) és a TARGET azonnali fizetési kiegyenlítésen (TIPS) ([28]) keresztül történő szolgáltatásnyújtás során eljáró eurorendszerre nem vonatkozik a javasolt rendelet hatályról szóló cikke, és ezek nem tekinthetők harmadik félnek minősülő IKT-szolgáltatóknak sem, így a javasolt rendelet alkalmazásában nem sorolhatók be harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóként. Az eurorendszer a T2S felvigyázását az elszámolási és fizetési rendszerek hatékony és megbízható működésének biztosítására irányuló feladatával összefüggésben látja el. Ezenkívül az ESMA egyértelművé tette, hogy a T2S nem minősül kritikus szolgáltatónak ([29]) a 909/2014/EU európai parlamenti és tanácsi rendelet ([30]) (a továbbiakban: a központi értéktárakról szóló rendelet) értelmében. Ennek következtében a T2S szervezeti és működési biztonsága, hatékonysága és rezilienciája a T2S-re alkalmazandó jogi, szabályozási és működési keretrendszeren és az elfogadott irányítási szabályokon keresztül kerül biztosításra, és nem a központi értéktárakról szóló rendeleten keresztül.

2.1.4 Ezen túlmenően az eurorendszer felvigyázási politikai keretrendszere ([31]) kiterjed olyan kritikus szolgáltatókra, mint a Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT). A SWIFT egy Belgiumban létrehozott, korlátolt felelősségű kooperációs társaság, amely biztonságos üzenetküldési szolgáltatásokat nyújt nemzetközi szinten. A SWIFT vezető felvigyázójaként a Nationale Bank van België/Banque Nationale de Belgique jár el, amely a SWIFT tekintetében a felvigyázást a felvigyázásra vonatkozó együttműködési megállapodás alapján a G10-ek többi központi bankjával együttműködésben folytatja, az EKB-t is ideértve. A G10-ek felvigyázói elismerik, hogy a felvigyázás fő fókusza a SWIFT működési kockázata, mivel ezt tekintik a fő kockázati kategóriának, amelynek révén a SWIFT rendszerszintű kockázatot jelenthetne az Unió pénzügyi rendszerére nézve. E tekintetben a SWIFT együttműködő felvigyázói csoport a SWIFT-re alkalmazandó különös elveket és magas szintű elvárásokat dolgozott ki, például a kockázatok azonosítása és kezelése, az információbiztonság, megbízhatóság és reziliencia, a technológiai tervezés és a felhasználókkal való kommunikáció tekintetében. A G10-ek felvigyázói elvárják a SWIFT-től, hogy betartsa a Fizetési és Piaci Infrastruktúra Bizottság (CPMI) és az Értékpapír-felügyeletek Nemzetközi Szervezetének (IOSCO) kiberrezilienciáról szóló iránymutatását ([32]), valamint az IKT-biztonságra vonatkozó más nemzetközi standardokat, amelyek – együttesen figyelembe véve – meghaladják a javasolt rendeletben foglalt követelményeket.

2.1.5 Nem lehetünk biztosak abban, hogy a SWIFT és esetleg más, az eurorendszer felvigyázási politikai keretrendszerének hatálya alá tartozó más szolgáltatók harmadik félnek minősülő IKT-szolgáltatóként a javasolt rendelet hatálya alá kerülhetnének, ha a Szerződés 127. cikke (2) bekezdésének hatálya alá nem tartozó szolgáltatásokat nyújtanának. Az EKB ezért kifejezetten üdvözli, hogy azok a szolgáltatók, amelyek már az eurorendszer felvigyázási politikai keretrendszerének hatálya alá tartoznak, így többek között, de nem kizárólag a SWIFT, kizárásra kerüljenek a javasolt rendeletben foglalt felvigyázási keret hatálya alól.

([25]) Lásd a javasolt rendelet 28. cikkének (5) bekezdését.

([26]) Lásd a kriptoeszközök piacairól és az (EU) 2019/1937 irányelv módosításáról szóló rendelet iránti javaslatról szóló, 2021. február 19-i európai központi banki vélemény (CON/2021/4) 1.3. bekezdését. Az EKB valamennyi véleménye közzétételre kerül az EUR-Lexen.

([27]) Lásd a transzeurópai automatizált valós idejű bruttó elszámolású rendszerről (TARGET2) szóló, 2012. december 5-i EKB/2012/27 európai központi banki iránymutatás (HL L 30., 2013.1.30., 1. o.) IIa. mellékletét. Az Európai Központi Bank EKB/2012/13 iránymutatása (2012. július 18.) a TARGET2-Securitiesről (HL L 215., 2012.8.11., 19. o.); az Európai Központi Bank EKB/2011/20 határozata (2011. november 16.) a központi értéktárak TARGET2-Securities szolgáltatásokhoz való csatlakozásának jogosultsági feltételei végrehajtására szolgáló részletes szabályok és eljárások megállapításáról (HL L 319., 2011.12.2., 117. o.). Lásd még a T2S keretmegállapodást és a kollektív megállapodást.

([28]) Lásd az EKB/2012/27 iránymutatás IIb. mellékletét.

([29]) Lásd az Európai Unión belüli értékpapír-kiegyenlítés javításáról és a központi értéktárakról, valamint 98/26/EK és a 2014/65/EU irányelv, valamint a 236/2012/EU rendelet módosításáról szóló, 2014. július 23-i 909/2014/EU európai parlamenti és tanácsi rendelet (HL L 257., 2014.8.28., 1. o.) 30. cikkének (5) bekezdését és a 909/2014/EU európai parlamenti és tanácsi rendeletnek a központi értéktárakra vonatkozó engedélyezési, felügyeleti és működési követelményekről szóló szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló, 2016. november 11-i (EU) 2017/392 felhatalmazáson alapuló bizottsági rendelet (HL L 65., 2017.3.10., 48. o.) 68. cikkét.

([30]) Az Európai Parlament és a Tanács 909/2014/EU rendelete (2014. július 23.) az Európai Unión belüli értékpapír-kiegyenlítés javításáról és a központi értéktárakról, valamint 98/26/EK és a 2014/65/EU irányelv, valamint a 236/2012/EU rendelet módosításáról (HL L 257., 2014.8.28., 1. o.).

([31]) Eurosystem oversight policy framework (Az eurorendszer felvigyázási politikai keretrendszere), felülvizsgált változat (2016. július), elérhető az EKB honlapján: www.ecb.europa.eu.

([32]) Elérhető a Nemzetközi Fizetések Bankjának honlapján: www.bis.org.

2.2 *A KBER hatáskörei az értékpapír-kiegyenlítés területén*

2.2.1 A központi értéktárak olyan pénzügyi piaci infrastruktúrák, amelyeket különböző hatóságok szigorúan szabályoznak és felügyelnek a központi értéktárakról szóló rendelet szerint, amely meghatározza a pénzügyi eszközök kiegyenlítésére vonatkozó követelményeket, és szabályokat ír elő a központi értéktárak szervezetére és irányítására. A központi értéktáraknak továbbá figyelembe kell venniük a CPMI-IOSCO kiberrezilienciáról szóló iránymutatását, amelyet az eurorendszer pénzügyi piaci infrastruktúráknak szóló, kiberrezilienciára vonatkozó felügyeleti elvárásai (2018. december) ([33]) operacionalizáltak. A központi értéktárakról szóló rendelet értelmében az illetékes nemzeti hatóságokra ruházott felügyeleti hatáskörök mellett a KBER tagjai „érintett hatóságként" járnak el a központi értéktárak által működtetett értékpapír-kiegyenlítési rendszerek felvigyázóiként, olyan központi bankokként, amelyek a kiegyenlítések során használt leginkább releváns pénznemeket kibocsátják, valamint olyan központi bankokként, amelyek könyveiben az ügyletek pénzoldalát kiegyenlítik ([34]). E tekintetben a központi értéktárakról szóló rendelet (8) preambulumbekezdése kimondja, hogy a rendelet nem érintheti az EKB és a nemzeti központi bankok azon feladatát, hogy biztosítsák az Unión belül és más országokban működtetett elszámolási és fizetési rendszerek hatékonyságát és megfelelő működését. A (8) preambulumbekezdés megállapítja továbbá, hogy a központi értéktárakról szóló rendelet nem akadályozhatja meg, hogy a KBER tagjai hozzáférjenek azokhoz az információkhoz, amelyek a feladataik ellátásához szükségesek ([35]), ideértve a központi értéktárak és más pénzügyi piaci infrastruktúrák általuk végzett felvigyázását ([36]) is.

2.2.2 Továbbá a KBER tagjai gyakran elszámoló ügynökként járnak el az értékpapírügyletek pénzoldalán, és az eurorendszer a T2S-en keresztül kiegyenlítési szolgáltatásokat nyújt a központi értéktárak számára. A T2S eurorendszer általi felvigyázása az elszámolási és fizetési rendszerek hatékony és megbízható működésének biztosítására irányuló feladatához kapcsolódik, míg a központi értéktárak illetékes és érintett hatóságai arra törekednek, hogy saját országukban biztosítsák azok zavartalan működését, a kiegyenlítés biztonságát és hatékonyságát, valamint a pénzügyi piacok megfelelő működését.

2.2.3 A javasolt rendelet alapján ([37]) a KBER központi bankok az IKT-kockázatok meghatározását illetően nem vesznek részt a technikai standardok kidolgozásában. A javasolt rendelet alapján ([38]) az érintett hatóságokat hasonlóképpen nem tájékoztatják az IKT-vonatkozású biztonsági eseményekről. Fenn kell tartani a KBER központi bankok ugyanolyan mértékű részvételét, mint amelyet jelenleg a központi értéktárakról szóló rendelet előír, és az érintett hatóságokat tájékoztatni kell az IKT-vonatkozású biztonsági eseményekről. Az eurorendszer az érintett hatóság valamennyi euroövezeti központi értéktár, továbbá számos más uniós központi értéktár vonatkozásában. A KBER központi bankokat tájékoztatni kell azon IKT-vonatkozású biztonsági eseményekről, amelyek relevánsak a feladataik – többek között a központi értéktárak és más pénzügyi piaci infrastruktúrák felvigyázásának – ellátása szempontjából. A kockázatok, többek között IKT-kockázatok, amelyeknek a központi értéktárak ki vannak téve, fenyegethetik a központi értéktárak megbízható működését. Ezért az IKT-kockázatok jelentőséggel bírnak az érintett hatóságok számára, és e kockázatokról teljes körű és részletes áttekintést kell biztosítani számukra, hogy értékelni tudják azokat és befolyásolhassák a központi értéktárak kockázatkezelési megközelítését. A javasolt rendelet az IKT-kockázatokat illetően a központi értéktárakról szóló rendelet és a jelenlegi kapcsolódó szabályozástechnikai standardok alapján előírtakhoz képest nem írhat elő kevésbé korlátozó követelményeket.

2.2.4 Ezenkívül az uniós jogalkotó szerveknek egyértelművé kell tenniük a javasolt rendelet ([39]) és a központi értéktárakról szóló rendeletet kiegészítő szabályozástechnikai standardok közötti kölcsönhatást. Közelebbről, nem világos, hogy mentesíteni kell-e a központi értéktárat a saját másodlagos helyszínnel rendelkezésre vonatkozó kötelezettség alól, amennyiben a harmadik félnek minősülő IKT-szolgáltatója ilyen helyszínt tart fenn ([40]). Amennyiben a központi értéktárat mentesíteni kell a másodlagos helyszín fenntartására vonatkozó e kötelezettség alól, úgy nem világos, hogy milyen jogi értékkel bírna e követelmény. Hasonlóképpen, a javasolt

([33]) Elérhető az EKB honlapján: www.ecb.europa.eu.

([34]) Lásd a 909/2014/EU rendelet 12. cikkét.

([35]) Lásd még a 909/2014/EU rendelet 13. cikkét, 17. cikkének (4) bekezdését és 22. cikkének (6) bekezdését.

([36]) Lásd a kritikus infrastruktúrák információtechnológiai biztonsági célokra történő azonosításáról szóló, 2017. április 6-i európai központi banki vélemény (CON/2017/10) 7.3. bekezdését; az alapvető szolgáltatások és az alapvető szolgáltatásokat nyújtó szereplők hálózati és információs rendszerek biztonsága érdekében történő kijelöléséről szóló, 2018. november 8-i európai központi banki vélemény (CON/2018/47) 7.2. bekezdését; a hálózati és információs rendszerek biztonságáról szóló, 2019. május 2-i európai központi banki vélemény (CON/2019/17) 3.5.2. bekezdését; és a hálózati és információs rendszerek biztonságáról szóló, 2019. november 11-i európai központi banki vélemény (CON/2019/38) 3.5.2. bekezdését.

([37]) Lásd a javasolt rendelet 54. cikkének (5) bekezdését és a 909/2014/EU rendelet 45. cikkének (7) bekezdését.

([38]) Lásd a javasolt rendelet 54. cikkének (4) bekezdését és a 909/2014/EU rendelet 45. cikkének (6) bekezdését.

([39]) Lásd a javasolt rendelet 11. cikkének (5) bekezdését.

([40]) Lásd a 909/2014/EU európai parlamenti és tanácsi rendeletnek a központi értéktárakra vonatkozó engedélyezési, felügyeleti és működési követelményekről szóló szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló, 2016. november 11-i (EU) 2017/392 felhatalmazáson alapuló bizottsági rendelet (HL L 65., 2017.3.10., 48. o.) 78. cikkének (3) bekezdését.

rendelet ([41]) az egyes funkciókhoz kapcsolódó helyreállítási időre és helyreállítási pontra vonatkozó célkitűzésre hivatkozik ([42]), míg a vonatkozó szabályozástechnikai standard a központi értéktárak kritikus műveletei vonatkozásában meghatározott helyreállítási idő tekintetében különbséget tesz a kritikus funkciók ([43]) és a kritikus műveletek ([44]) között. Az egymásnak ellentmondó követelmények kockázatának elhárítása érdekében az uniós jogalkotó szervek részéről további pontosítást és megfontolást igényel a javasolt rendelet és a központi értéktárakról szóló rendeletet kiegészítő szabályozástechnikai standardok közötti kölcsönhatás. Végül, egyértelművé kell tenni, hogy a központi értéktárakról szóló rendelet ([45]) alapján bizonyos közszervezetek által üzemeltetett központi értéktáraknak biztosított mentességek a javasolt rendelet alapján kiterjesztésre kerülnek.

2.3 *A KBER hatáskörei az értékpapír-elszámolás területén*

2.3.1 A KBER központi bankok a központi szerződő felek vonatkozásában felvigyázói hatáskörökkel rendelkeznek. E tekintetben az eurorendszerbeli nemzeti központi bankok gyakran együttműködnek az érintett illetékes nemzeti hatóságokkal a központi szerződő felek felvigyázási és felügyeleti funkciói terén, valamint részt vesznek az adott központi szerződő fél 648/2012/EU európai parlamenti és tanácsi rendelet ([46]) (a továbbiakban: EMIR) alapján létrehozott kollégiumában. Az eurorendszer érintett tagjai ([47]) felvigyázói minőségükben részt vesznek az EMIR szerinti kollégiumokban és képviselik az eurorendszert mint a központi szerződő felek kibocsátó központi bankját, amennyiben az elszámolt pénzügyi eszközök tekintetében az egyik legfontosabb pénznem az euro (továbbá azon offshore központi szerződő felek esetében, amelyek a pénzügyi eszközök jelentős részét euróban számolják el). Az EKB a kibocsátó központi bank a nem euroövezeti központi szerződő felek számára.

2.3.2 A javasolt rendelet alapján ([48]) a KBER központi bankok az IKT-kockázatok meghatározását illetően nem vesznek részt a technikai standardok kidolgozásában. Ezenkívül a javasolt rendelet ([49]) nem hivatkozik a helyreállítási időre és a helyreállítási pontra vonatkozó célkitűzéssel kapcsolatos, EMIR szerinti követelményekre ([50]). A javasolt szabályozási keret az IKT-kockázatokat illetően nem írhat elő a jelenleg fennállóaknál kevésbé korlátozó követelményeket. Ezért a megbízható üzletmenet-folytonosság kezelési keretrendszerrel rendelkezés szempontjából kritikus fontosságú a helyreállítási időre és pontra vonatkozó egyértelmű célkitűzések meghatározása. A helyreállítási időre és pontra vonatkozó konkrét célkitűzések fenntartása a pénzügyi piaci infrastruktúrákra vonatkozó CPMI-IOSCO elvek ([51]) részét is képezi. Meg kell tartani az EMIR szerinti jelenlegi rendelkezést, és a javasolt rendeletet megfelelően ki kell igazítani. Az egymásnak ellentmondó vagy egymást átfedő követelmények kockázatának elhárítása érdekében a KBER központi bankoknak részt kell venniük a másodlagos szintű jogszabályok kidolgozásában, valamint a javasolt rendelet és a kiegészítő szabályozástechnikai standardok közötti kölcsönhatással kapcsolatos, az uniós jogalkotó szervek általi további pontosításra és vizsgálatra irányuló folyamatban.

3. **A prudenciális felügyeleti aspektusokkal kapcsolatos különös észrevételek**

3.1 Az 1024/2013/EU tanácsi rendelet ([52]) (a továbbiakban: SSM-rendelet) az euroövezeti hitelintézetek prudenciális felügyeletével kapcsolatos külön feladatokkal bízza meg az EKB-t, és felelőssé teszi az – egyes felügyeleti feladatok EKB és a mechanizmusban részt vevő illetékes nemzeti hatóságok közötti megosztását magában foglaló – egységes felügyeleti mechanizmus (SSM) hatékony és konzisztens működéséért. Közelebbről, az EKB feladata valamennyi hitelintézet engedélyezése és engedélyének visszavonása. Az EKB feladata továbbá többek között, hogy biztosítsa a hitelintézetek számára prudenciális követelményeket előíró releváns uniós jognak való megfelelést, ideértve azt a követelményt is, hogy megbízható irányítási rendszerekkel, például megfelelő kockázatkezelési eljárásokkal és belső ellenőrzési mechanizmusokkal rendelkezzenek ([53]). E célból az EKB-t minden olyan felügyeleti hatáskörrel felruházták, amely a hitelintézetek tevékenységeibe a feladatai ellátása érdekében történő beavatkozáshoz

([41]) Lásd a javasolt rendelet 11. cikkének (6) bekezdését.
([42]) Lásd a javasolt rendelet 3. cikkének (17) bekezdését.
([43]) Lásd az (EU) 2017/392 felhatalmazáson alapuló bizottsági rendelet 76. cikke (2) bekezdésének d) és e) pontját.
([44]) Lásd az (EU) 2017/392 felhatalmazáson alapuló bizottsági rendelet 78. cikkének (2) és (3) bekezdését.
([45]) Lásd a 909/2014/EU rendelet 1. cikkének (4) bekezdését.
([46]) Az Európai Parlament és a Tanács 648/2012/EU rendelete (2012. július 4.) a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról (HL L 201., 2012.7.27., 1. o.).
([47]) Lásd az EMIR 18. cikke (2) bekezdésének g) és h) pontját.
([48]) Lásd a javasolt rendelet 53. cikke (2) bekezdésének b) pontját és (3) bekezdését, valamint az EMIR 34. cikkének (3) bekezdését.
([49]) Lásd a javasolt rendelet 53. cikke (2) bekezdésének a) pontját.
([50]) Lásd az EMIR 34. cikkét.
([51]) Lásd a pénzügyi piaci infrastruktúrákra vonatkozó CPMI-IOSCO elveket (Principles for financial market infrastructures), elérhető a Nemzetközi Fizetések Bankja honlapján:www.bis.org.
([52]) A Tanács 1024/2013/EU rendelete (2013. október 15.) az Európai Központi Banknak a hitelintézetek prudenciális felügyeletére vonatkozó politikákkal kapcsolatos külön feladatokkal történő megbízásáról (HL L 287., 2013.10.29., 63. o.).
([53]) Lásd az 1024/2013/EU rendelet 4. cikke (1) bekezdésének e) pontját és 6. cikkének (4) bekezdését.

szükséges. Így az EKB és az érintett illetékes nemzeti hatóságok a 2013/575/EU európai parlamenti és tanácsi rendelet ([54]) (a továbbiakban: tőkekövetelményekről szóló rendelet) és a 2013/36/EU európai parlamenti és tanácsi irányelv ([55]) (a továbbiakban: tőkekövetelményekről szóló irányelv) szerinti meghatározott prudenciális felügyeleti hatásköröket gyakorló illetékes hatóságok.

3.2 A javasolt rendelet kimondja, hogy az egységes szabálykönyvet és a felügyeleti rendszert a digitális működési rezilienciára és az IKT-biztonságra kiterjedően szükséges továbbfejleszteni, a pénzügyi stabilitás és a piaci integritás nyomon követéséért és védelméért felelős pénzügyi felügyeletek szélesebb körű felhatalmazásával ([56]). A cél egy átfogó IKT- vagy működésikockázat-kezelési keret előmozdítása a pénzügyi szervezetek teljes körére kiterjedő, digitális működési rezilienciára vonatkozó követelmények harmonizációja révén ([57]). A javasolt rendelet célja különösen, hogy egyesítse és korszerűsítse azokat az IKT-kockázatokra vonatkozó követelményeket, amelyeket eddig különböző jogszabályok elkülönítetten rögzítettek ([58]).

3.3 A pénzügyi ágazatra vonatkozó, IKT-kockázattal kapcsolatos követelmények jelenleg több uniós jogi aktusban találhatók meg, köztük a tőkekövetelményekről szóló irányelvben és puha jogi eszközökben (például az EBH iránymutatásaiban), és e követelmények sokfélék és esetenként hiányosak. Egyes esetekben az IKT-kockázattal csak hallgatólagosan, a működési kockázat részeként foglalkoznak, más esetekben pedig egyáltalán nem. Ezt orvosolni kell a javasolt rendelet és ezen jogi aktusok összehangolása révén. E célból a javasolt módosító irányelv több módosítást fogalmaz meg, amelyek szükségesnek tűnnek a digitális működési rezilienciával kapcsolatos különböző követelmények alkalmazását illetően a jogi egyértelműség és következetesség megteremtése érdekében. A javasolt módosító irányelv által jelenleg javasolt, a tőkekövetelményekről szóló irányelvet érintő módosítások ([59]) azonban csak a vészhelyzeti és üzletmenet-folytonossági tervekre vonatkozó rendelkezésekre ([60]) hivatkoznak, mivel állítólag hallgatólagosan ezek szolgálnak alapul az IKT-kockázatkezeléssel való foglalkozáshoz.

3.4 Ezenkívül a javasolt rendelet ([61]) úgy rendelkezik, hogy a pénzügyi szervezeteknek, a hitelintézeteket is beleértve, belső irányítási és kontrollkerettel kell rendelkezniük, amelyek biztosítják valamennyi IKT-kockázat eredményes és prudens kezelését. A javasolt rendelet ([62]) az abban foglalt követelmények egyedi, valamint konszolidált szinten történő alkalmazásáról rendelkezik, azonban a hivatkozott ágazatspecifikus jogszabályokkal való megfelelő koordináció nélkül. Végül, a javasolt rendelet ([63]) úgy rendelkezik, hogy – a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókra vonatkozó, a javasolt rendeletben ([64]) említett felvigyázási keret rendelkezéseinek sérelme nélkül – a javasolt rendeletben meghatározott kötelezettségek teljesítését hitelintézetek esetében a tőkekövetelményekről szóló irányelv 4. cikkével összhangban kijelölt illetékes hatóság biztosítja, az SSM-rendelettel az EKB-ra ruházott egyedi feladatok sérelme nélkül.

3.5 A fentiekre tekintettel az EKB értelmezése szerint a hitelintézetek vonatkozásában – a javasolt rendeletben szereplő, a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókra vonatkozó felvigyázási kerettel kapcsolatos rendelkezésektől ([65]) eltekintve – a javasolt rendelet az IKT-kockázat kezelésére vonatkozó olyan prudenciális belső irányítási keretet kíván kialakítani, amely integrálásra kerül a tőkekövetelményekről szóló irányelv szerinti általános belső irányítási keretbe. Ezenkívül a javasolt keret prudenciális jellegére tekintettel a javasolt keret alapján meghatározott kötelezettségeknek való megfelelés felügyeletéért felelős illetékes hatóságok, az EKB-t is beleértve, az SSM-rendeletnek megfelelően a bankfelügyeletért felelős hatóságok lesznek.

([54]) Az Európai Parlament és a Tanács 575/2013/EU rendelete (2013. június 26.) a hitelintézetekre és befektetési vállalkozásokra vonatkozó prudenciális követelményekről és a 648/2012/EU rendelet módosításáról (HL L 176., 2013.6.27., 1. o.).

([55]) Az Európai Parlament és a Tanács 2013/36/EU irányelve (2013. június 26.) a hitelintézetek tevékenységéhez való hozzáférésről és a hitelintézetek és befektetési vállalkozások 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.).

([56]) Lásd a javasolt rendelet (8) preambulumbekezdését.

([57]) Lásd a javasolt rendelet (11) preambulumbekezdését.

([58]) Lásd a javasolt rendelet (12) preambulumbekezdését.

([59]) Lásd a javasolt módosító irányelv (4) és (5) preambulumbekezdését.

([60]) Lásd a tőkekövetelményekről szóló irányelv 85. cikkét.

([61]) Lásd a javasolt rendelet 4. cikkének (1) bekezdését.

([62]) Lásd a javasolt rendelet 25. cikkének (3) és (4) bekezdését.

([63]) Lásd a javasolt rendelet 41. cikkét.

([64]) Lásd a javasolt rendelet V. fejezetének II. szakaszát.

([65]) Lásd a javasolt rendelet V. fejezetének II. szakaszát.

3.6 Az uniós jogalkotó szervek ezért figyelembe kívánhatják venni az egyértelműség, valamint a javasolt rendelet és a tőkekövetelményekről szóló irányelv közötti koordináció növelésére irányuló következő javaslatokat. Először is, a javasolt rendelet szerinti követelményeket kifejezetten prudenciális jellegűnek lehet minősíteni, amint az többek között a központi értéktárakról szóló rendeletben ([66]) történt. Másodszor, tágabbá lehetne tenni a javasolt módosító irányelv preambulumbekezdéseinek ([67]) megfogalmazását, tekintettel arra, hogy a javasolt rendelet szerinti követelmények túlterjednek pusztán a vészhelyzeti és üzletmenet-folytonossági tervek szakaszán. Az IKT-kockázatirányítási intézkedések összességében a tőkekövetelményekről szóló irányelv 74. cikke szerinti megbízható vállalatirányítási rendszer általánosabb alkalmazási köre alá tartoznak ([68]). Harmadszor, a javasolt rendeletet ([69]) módosítani kell annak érdekében, hogy a preambulum-bekezdésekben emlékeztessenek az EKB-nek a Szerződésen és az SSM-rendeleten alapuló, a hitelintézetek prudenciális felügyeletével kapcsolatos hatáskörére. Negyedszer, a javasolt rendeletben előírt követelmények egyedi és konszolidált szinten történő alkalmazására való hivatkozást ([70]) felül kell vizsgálni, mivel a szubkonszolidált és a konszolidált szint a javasolt rendeletben nem kerül meghatározásra, és bizonyos típusú közvetítők a vonatkozó jogszabályok alapján nem tartoznak összevont alapú felügyelet hatálya alá (például pénzforgalmi intézmények). Ezenkívül a javasolt rendelet szerinti követelmények alkalmazási szintjének kizárólag az egyes pénzügyi szervezetekre alkalmazandó jogszabályokból kell következnie. A hitelintézetek esetében a tőkekövetelményekről szóló irányelv és a javasolt rendelet közötti egyértelmű kapcsolat biztosított, így a javasolt rendelet szerinti követelmények esettől függően automatikusan egyedi, szubkonszolidált vagy konszolidált szinten lennének alkalmazandók ([71]). Végül, az uniós jogalkotó szervek megfontolhatnák átmeneti rendszer előírását a javasolt rendelet hatálybalépése és a javasolt rendeletben előirányzott szabályozástechnikai standardok hatálybalépése közötti időszak kezelése érdekében, figyelemmel arra, hogy bizonyos közvetítőkre, a hitelintézeteket is ideértve, már vonatkoznak IKT-kockázatokkal kapcsolatos szabályok, amelyek egyes ágazatokra alkalmazandóak, és amelyek részletesebbek, mint a javasolt rendelet általános rendelkezései.

3.7 Az SSM-rendelet alapján az EKB-t megbízták azzal a feladattal, hogy biztosítsa az azon uniós jogi követelményeknek a hitelintézetek általi megfelelést, amelyek a hitelintézetek számára előírják, hogy megbízható kockázatkezelési eljárásokkal és belső ellenőrzési mechanizmusokkal rendelkezzenek ([72]). Ez azt jelenti, hogy az EKB-nak biztosítania kell, hogy a hitelintézetek a működési kockázatnak – többek között a modellkockázatnak – való kitettségek értékelésére és kezelésére, valamint a ritkán előforduló, de súlyos következményekkel járó események lefedésére szabályzatokat és eljárásokat alkalmazzanak. A hitelintézeteknek meg kell határozniuk, hogy e szabályzatok és eljárások alkalmazásában mi minősül működési kockázatnak ([73]).

3.8 2017. júliusában az EKB Kormányzótanácsa – a Felügyeleti Testület SSM-rendelet 26. cikkének (8) bekezdése és 6. cikkének (2) bekezdése, valamint a 468/2014/EU európai központi banki rendelet (EKB/2014/17) ([74]) 21. cikkének (1) bekezdése szerinti javaslattervezete alapján – elfogadta az SSM kiberbiztonsági események bejelentésére vonatkozó keretrendszerét (a továbbiakban: Keretrendszer). A Keretrendszer az SSM-rendelet 10. cikkén alapuló kötelező információkérésből (a hitelintézetekhez intézett egyedi határozatok) és/vagy adatszolgáltatás iránti kérésből áll ([75]). Egyes országok már rendelkeznek a biztonsági események bejelentésére szolgáló eljárással, amely megköveteli a hitelintézetektől, hogy minden jelentős kiberbiztonsági eseményt bejelentsenek az illetékes nemzeti hatóságuknak. Ezekben az országokban a jelentős hitelintézetek a biztonsági eseményeket továbbra is az illetékes nemzeti hatóságoknak fogják jelenteni, amelyek azokat ezt követően a felügyelt szervezetek nevében indokolatlan késedelem nélkül továbbítják majd az EKB-nak. Ezért a fentiekben említett határozatok címzettjei ezek az illetékes nemzeti hatóságok is annak érdekében, hogy ezeket az információkat a

([66]) Lásd a központi értéktárakról szóló rendelet II. fejezete 4. szakaszának „Prudenciális követelmények” címét.

([67]) Lásd a javasolt módosító irányelv (4) preambulumbekezdését.

([68]) A 2013/36/EU irányelv 85. cikke puszta pontosítás. E tekintetben lásd még az Európai Bankhatóságnak az IKT- és biztonsági kockázatok kezelésére vonatkozó, 2019. november 29-i iránymutatásainak (a továbbiakban: EBH iránymutatások), 4., 11. és 37. oldalát, amelyek tekintetében az általános jogalap kifejezetten a 2013/36/EU irányelv 74. cikkében található.

([69]) Lásd a javasolt rendelet 41. cikkének (1) bekezdését.

([70]) Lásd a javasolt rendelet 25. cikkének (3) és (4) bekezdését.

([71]) Lásd még a tőkekövetelményekről szóló irányelv 109. cikkét.

([72]) Lásd az SSM-rendelet 4. cikke (1) bekezdésének e) pontját.

([73]) Lásd a tőkekövetelményekről szóló irányelv 85. cikkét.

([74]) Az Európai Központi Bank 468/2014/EU rendelete (2014. április 16.) az Egységes Felügyeleti Mechanizmuson belül az Európai Központi Bank és az illetékes nemzeti hatóságok, valamint a kijelölt nemzeti hatóságok közötti együttműködési keretrendszer létrehozásáról (SSM-keretrendelet) (EKB/2014/17) (HL L 141., 2014.5.14., 1. o.).

([75]) Pontosabban, valamely kiberbiztonsági eseményt (az információbiztonság azonosított lehetséges megsértését, legyen az akár rosszindulatú vagy véletlenszerű) be kell jelenteni az EKB-nak, ha a következő feltételek legalább egyike fennáll: 1. 5 millió eurót vagy az elsődleges alapvető tőke 0,1 %-át elérő potenciális pénzügyi hatásról van szó; 2. az eseményről nyilvánosan beszámolnak vagy az hírnévromlásból eredő kárt okoz; 3. az eseményt a rendes adatszolgáltatás keretén kívül felterjesztették az informatikáért felelős vezető tisztségviselőhöz; 4. a bank az eseményt bejelentette a CERT-nek/CSIRT-nek, valamely biztonsági ügynökségnek vagy a rendőrségnek; 5. katasztrófa utáni helyreállítási vagy üzletmenet-folytonossági eljárások indultak vagy kiberbiztosítási követelést nyújtottak be; 6. a jogi vagy szabályozási követelmények megsértésére került sor; vagy 7. a bank belső kritériumok és szakértői megítélés alapján (az esetleges rendszerszintű hatást is beleértve) úgy dönt, hogy tájékoztatja az EKB-t.

Keretrendszer alapján továbbítsák az EKB-nak. Az EKB támogatja az uniós jogalkotó szervek azon törekvését, hogy előmozdítsák az észszerűsítést és a harmonizációt többek között a hitelintézetekre a biztonsági események bejelentése terén alkalmazandó szabályok és kötelezettségek tekintetében. Erre tekintettel az EKB kész arra, hogy a javasolt rendelet elfogadására figyelemmel szükség esetén módosítsa (és esetlegesen hatályon kívül helyezze) a Keretrendszert.

4. **Az IKT-kockázatkezeléssel, a biztonsági események bejelentésével, a működési reziliencia tesztelésével és a harmadik féltől eredő IKT-kockázattal kapcsolatos különös észrevételek**

4.1 *IKT-kockázatkezelés*

4.1.1 Az EKB üdvözli, hogy a javasolt rendelet szilárd és átfogó IKT-kockázatkezelési keretrendszert vezet be, amely kiterjed a CPMI-IOSCO kiberrezilienciáról szóló iránymutatására és szorosan igazodik a bevált gyakorlatokhoz, az eurorendszer pénzügyi piaci infrastruktúráknak szóló, kiberrezilienciára vonatkozó felvigyázói elvárásait is ideértve.

4.1.2 Az EKB támogatja azt az elgondolást, hogy a pénzügyi szervezeteknek kockázatértékelést kelljen végezniük a hálózati és információs rendszerinfrastruktúra minden „jelentős változásakor” ([76]). Mindemellett a javasolt rendelet nem tartalmazza a „jelentős változás” meghatározását, ami nemkívánatos teret nyújt a pénzügyi szervezetek általi eltérő értelmezéseknek, amelyek végső soron akadályozhatják a javasolt rendelet harmonizációs céljait. A jogbiztonság érdekében az uniós jogalkotó szervek meg kívánhatják fontolni a „jelentős változás” meghatározásának a javasolt rendeletbe történő beiktatását.

4.1.3 Az EKB általában véve támogatja azt az elgondolást, hogy a mikrovállalkozásnak nem minősülő pénzügyi szervezetek beszámoljanak az illetékes hatóságoknak az IKT-zavarokból és az IKT-vonatkozású biztonsági eseményekből eredő releváns költségeikről és veszteségeikről ([77]). Ugyanakkor a rendszer átfogó eredményességének biztosítása érdekében, valamint, hogy ne terheljük túl az illetékes hatóságokat és a pénzügyi szervezeteket túlságosan sok jelentéssel, az uniós jogalkotó szervek hasznosan megfontolhatnák releváns, esetleg mennyiségi jellegű küszöbértékek bevezetését.

4.1.4 Az EKB elismeri annak lehetőségét, hogy a pénzügyi szervezetek az illetékes hatóságok jóváhagyásával a vállalatcsoportjukon belüli vagy külső vállalkozásokhoz delegálhassák az IKT-kockázatkezelési követelményeknek való megfelelés ellenőrzésével kapcsolatos feladatokat ([78]). Ugyanakkor fontos, hogy az uniós jogalkotó szervek egyértelművé tegyék, hogy az illetékes hatóság jóváhagyása hogyan kerül megadásra azokban az esetekben, amikor a pénzügyi szervezet vonatkozásában több illetékes hatóság létezik. Erre akkor kerülhet sor, ha a pénzügyi szervezet hitelintézet, kriptoeszközszolgáltató és/vagy pénzforgalmi szolgáltató. Végül a pénzügyi szervezetek által a javasolt rendelet alapján elvégzendő azonosítást és osztályozást ([79]) illetően az EKB véleménye szerint az eszközök osztályozása szempontjából prudens lenne, ha a javasolt rendelet azt is megkövetelné a pénzügyi szervezetektől, hogy vegyék figyelembe az ilyen eszközök kulcsfontosságú jellegét (vagyis, hogy kulcsfontosságú funkciókat támogatnak-e).

4.2 *Biztonsági események bejelentése*

4.2.1 Az EKB üdvözli a javasolt rendeletben vázolt, az IKT-vonatkozású biztonsági események bejelentése terén fennálló uniós helyzet harmonizálására és a jelentős IKT-vonatkozású biztonsági események központosított bejelentésének kialakítására irányuló törekvést ([80]). A jelentős IKT-vonatkozású biztonsági eseményeknek az illetékes hatóságokhoz történő bejelentésére vonatkozó harmonizált keretrendszer bevezetése ([81]) elvben észszerűsítené és harmonizálná a pénzügyi szervezetek, köztük a hitelintézetek adatszolgáltatási terhét. Az illetékes hatóságok számára előnyös lenne az ennek hatálya alá tartozó biztonsági események szélesebb köre, amely túlterjedne a jelenlegi keretrendszerek ([82]) hatálya alá tartozó kiberbiztonsági vonatkozású biztonsági eseményeken. A javasolt rendelet jövőbeli elfogadása szükségessé tenné a jelenlegi keretrendszerek – többek között az SSM kiberbiztonsági események bejelentésére vonatkozó keretrendszere – felülvizsgálatát és esetlegesen hatályon kívül helyezését. Mindemellett, a valamennyi keretrendszer közötti valódi észszerűsítés és teljes összehangolás eléréséhez rendkívüli jelentőséggel bír annak biztosítása, hogy a javasolt rendelet szerinti, a biztonsági események bejelentéséről szóló rendelkezések hatálya – valamennyi releváns fogalommeghatározást, küszöbértéket és adatszolgáltatási paramétert is ideértve – teljes mértékben összehangolásra kerüljön a releváns keretrendszerekkel. Kiemelt jelentőséggel bír különösen az

([76]) Lásd a javasolt rendelet 7. cikkének (3) bekezdését.
([77]) Lásd a javasolt rendelet 10. cikkének (9) bekezdését.
([78]) Lásd a javasolt rendelet 5. cikkének (10) bekezdését.
([79]) Lásd a javasolt rendelet 7. cikkét.
([80]) Lásd a javasolt rendelet 19. cikkét.
([81]) Lásd a javasolt rendelet 3. cikkének (7) és (18) bekezdését.
([82]) Lásd például a Keretrendszert.

egyrészről a javasolt rendelet, és másrészről az (EU) 2015/2366 európai parlamenti és tanácsi irányelv ([83]) (a továbbiakban: a pénzforgalmi szolgáltatásokról szóló második irányelv), valamint a súlyos események bejelentéséről szóló EBH iránymutatások (a továbbiakban: EBH iránymutatások) közötti összehangolás biztosítása. A javasolt módosító irányelv ([84]) a pénzforgalmi szolgáltatásokról szóló második irányelvet érintő módosításokat tartalmaz a biztonsági eseményeknek a javasolt rendelet, illetve a pénzforgalmi szolgáltatásokról szóló második irányelv szerinti bejelentésének elhatárolásához kapcsolódóan, amely módosítások főként a pénzforgalmi szolgáltatókat érintenék, amelyek hitelintézetként is engedélyezettek lehetnek, továbbá az illetékes hatóságokat. A biztonsági események bejelentési eljárását illetően nem egyértelmű a helyzet, és potenciális átfedés áll fenn egyes olyan biztonsági eseményeket illetően, amelyeket a javasolt rendelet és az EBH iránymutatások alapján egyaránt be kell jelenteni.

4.2.2 A jelentős biztonsági események bejelentésére szolgáló, a javasolt rendelet ([85]), illetve a pénzforgalmi szolgáltatásokról szóló második irányelv és a megfelelő EBH iránymutatások szerinti eljárások megkövetelnék a pénzforgalmi szolgáltatóktól, hogy amint a biztonsági eseményt osztályozták, arról jelentést nyújtsanak be az illetékes hatóságukhoz. Az előzetes jelentések valójában nem ragadják meg a biztonsági esemény lényegét, okát vagy az esemény által érintett funkcionális területet, és a pénzforgalmi szolgáltatók adott esetben csak egy későbbi szakaszban képesek ilyen megkülönböztetések tételére, amikor az eseménnyel kapcsolatban részletesebb információk válnak elérhetővé. Ennek következtében a biztonsági eseményről szóló előzetes jelentéseket vagy be lehet nyújtani mind a javasolt rendelet, mind az EBH iránymutatások alapján, vagy a pénzforgalmi szolgáltatók kiválaszthatnak egyetlen adatszolgáltatási keretrendszert, és a későbbiekben kijavíthatják a benyújtott anyagokat. Ugyanezt a (például valamely biztonsági esemény kiváltó okával kapcsolatos) bizonytalanságot tükrözhetik az időközi és a végleges jelentések is. Ez ismét növelné a jelentések javasolt rendelet és a pénzforgalmi szolgáltatásokról szóló második irányelv alapján történő párhuzamos benyújtásának lehetőségét.

4.2.3 Egyes biztonsági események, amelyek besorolhatók IKT-vonatkozású biztonsági eseményként, más területekre is hatást gyakorolhatnak, és azokat ennek következtében az EBH iránymutatások alapján is be kellene jelenteni. Ez lehet a helyzet akkor, ha egy biztonsági esemény hatással jár IKT-szempontból, azonban ugyanakkor közvetlenül érinti a pénzforgalmi szolgáltatások nyújtását és/vagy más nem-IKT funkcionális területeket vagy csatornákat is. Ezenkívül lehetnek olyan esetek is, amikor nem lehet különbséget tenni a működési és az IKT-vonatkozású biztonsági események között. Abban az esetben továbbá, amikor ugyanaz a pénzügyi szervezet jelentős hitelintézet és pénzforgalmi szolgáltató is, a javasolt rendelet alapján e szervezetnek az IKT-vonatkozású biztonsági eseményt kétszer kellene bejelentenie, mivel két illetékes hatósággal rendelkezik. A fentiekre tekintettel a javasolt rendeletnek világosabban meg kellene fogalmaznia, hogy a pénzforgalmi szolgáltatásokról szóló második irányelvvel és az EBH iránymutatásokkal fennálló kölcsönhatásoknak a gyakorlatban hogyan kell működniük. Ami még fontosabb, az adatszolgáltatási kötelezettségek harmonizálása és észszerűsítése céljából fontos lenne, hogy az uniós jogalkotó szervek vizsgálják meg a kettős adatszolgáltatással kapcsolatos fennmaradó kérdéseket, és tegyék egyértelművé, hogy a javasolt rendelet és a pénzforgalmi szolgáltatásokról szóló második irányelv hogyan létezne egymás mellett, illetve, hogy a biztonsági események bejelentésére vonatkozó egységes követelményekre van-e szükség.

4.2.4. A javasolt rendelet az illetékes hatóságok számára arra vonatkozó követelményt ([86]) vezet be, hogy valamely jelentés átvételekor visszaigazolják a bejelentés fogadását, és a lehető leghamarabb ellássák a pénzügyi szervezetet a szükséges visszajelzéssel és iránymutatásokkal, különösen a szervezeti szintű korrekciós intézkedésekre, valamint a több ágazatot érintő káros hatások enyhítésének módjaira vonatkozóan. Ez azt jelentené, hogy az illetékes hatóságoknak tevékenyen hozzá kell járulniuk a biztonsági események kezeléséhez és elhárításához, és ugyanakkor értékelniük kell a felügyelt szervezet kritikus eseményekre való reagálását. Az EKB hangsúlyozza, hogy a biztonsági események korrekciójáért és következményeiért való felelősség továbbra is kizárólag és egyértelműen az érintett pénzügyi szervezetet kell, hogy terhelje. Az EKB ezért azt javasolná, hogy a visszajelzést és iránymutatást korlátozzák kizárólag magas szintű prudenciális visszajelzésre és iránymutatásra. Ha a visszajelzés szélesebb körű lenne, ahhoz igen jelentős technikai ismeretekkel rendelkező, erre specializálódott szakemberekre lenne szükség, amelyek tipikusan nem találhatóak meg a prudenciális hatóságok rendelkezésére álló tehetségbázisban.

4.3 *A digitális működési reziliencia tesztelése*

4.3.1 Az EKB üdvözli a javasolt rendeletben ([87]) szereplő, a digitális működési reziliencia pénzügyi szervezeteknél történő tesztelésével kapcsolatos követelményeket, valamint azt, hogy minden intézménynek saját tesztelési programmal kell rendelkeznie. A javasolt rendelet ([88]) a pénzügyi szervezetek számára indikatív jelleggel különböző típusú

([83]) Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről (HL L 337., 2015.12.23., 35. o.).

([84]) Lásd a javasolt módosító irányelv 7. cikkének (9) bekezdését.

([85]) Lásd a javasolt rendelet 17. cikkének (3) bekezdését.

([86]) Lásd a javasolt rendelet 20. cikkét.

([87]) Lásd a javasolt rendelet 21. és 22. cikkét.

([88]) Lásd a javasolt rendelet 22. cikkének (1) bekezdését.

teszteket ír le. A tesztek típusai nem igazán egyértelműek, és egyes tesztek, így például a kompatibilitásvizsgálatok, a kérdőívek vagy a forgatókönyv-alapú tesztek az európai felügyeleti hatóságok, az illetékes hatóságok vagy a pénzügyi szervezetek által különféleképpen értelmezhetők. Ezenkívül nincs útmutatás az egyes tesztek gyakoriságát illetően. Egy lehetséges megközelítés az lehetne, hogy a javasolt rendelet általános tesztelési követelményeket határozna meg, és a tesztek típusainak pontosabb leírását szabályozás- és végrehajtástechnikai standardok tartalmaznák.

4.3.2 A fenyegetettségi szempontú behatolási tesztelés (TLPT) a biztonsági védelem és felkészültség tesztelésének hatékony eszköze. Az EKB ezért ösztönzi a TLPT pénzügyi szervezetek általi alkalmazását. Ez az eszköz nem csak a technikai intézkedéseket teszteli, hanem a személyzetet és a folyamatokat is. E tesztek eredményei jelentősen növelhetik a tesztelt szervezeten belül a vezető tisztviselők biztonsággal kapcsolatos tudatosságát. A fenyegetettségi információkon alapuló etikai érdekütköztetéses elemzés európai kerete (TIBER-EU) ([89]) és az Unión kívül elérhető más TLPT eszközök az elsődleges eszközei annak, hogy a szervezetek maguk értékeljék, teszteljék, gyakorolják és javítsák a kiberreziliencia terén fennálló helyzetüket és védelmüket.

4.3.3 A legtöbb tagállamban, ahol a TIBER-EU-t végrehajtották, a felvigyázást, illetve a felügyeletet ellátó hatóságok nem játszanak tevékeny szerepet a helyi TIBER-XX program végrehajtásában, és a TIBER kibercsoport (TCT) szinte minden esetben elkülönül e funkcióktól. Ezért a javasolt rendelet ([90]) alapján fejlett módszerekkel, TLPT útján végzett tesztelést a pénzügyi ökoszisztéma erősítésére és a pénzügyi stabilitás növelésére szolgáló eszközként kell végrehajtani, nem pedig tisztán felügyeleti eszközként. Ezen túlmenően nincs szükség a kiberreziliencia fejlett módszerekkel történő tesztelésére vonatkozó új keretrendszer kialakítására, mivel a tagállamok már széles körben alkalmazzák az EU jelenleg egyetlen ilyen keretét, a TIBER-EU-t.

4.3.4 A tesztelőkre vonatkozó követelményeknek nem a javasolt rendelet fő szövegében kell szerepelniük, mivel a TLPT-hez kapcsolódó ágazat még kialakulóban van, és a konkrét követelmények előírása akadályozhatja az innovációt. Mindemellett az EKB azt az álláspontot képviseli, hogy a tesztek lefolytatása során a magas fokú függetlenség biztosítása érdekében a pénzügyi szervezetek ne foglalkoztassanak olyan tesztelőket, illetve ne kössenek szerződést olyan tesztelőkkel, akiket a saját csoportjukhoz tartozó pénzügyi szervezetek foglalkoztatnak vagy akikkel, illetve amelyekkel ilyen szervezetek szerződést kötöttek, vagy amelyek más módon a tesztelendő pénzügyi szervezetek tulajdonában és/vagy ellenőrzése alatt állnak.

4.3.5 A széttagoltság kockázatának csökkentése és a harmonizáció biztosítása érdekében a javasolt rendeletnek kötelezővé kell tennie egy TLPT keretrendszert, amely az Unióban mindenütt alkalmazandó a pénzügyi ágazatra. A széttagoltság költségnövekedéshez, valamint a technikai, működési és pénzügyi erőforrásigények növekedéséhez vezethet mind az illetékes hatóságok, mind a pénzügyi intézmények számára. E megnövekedett költségek és igények végső soron negatív hatást gyakorolhatnak a tesztek kölcsönös elismerésére. A harmonizáció e hiánya és a kölcsönös elismeréssel kapcsolatos, ebből eredő problémák különösen kritikusok azon pénzügyi szervezetek számára, amelyek több engedéllyel rendelkeznek és/vagy az Unióban több országban működnek. A javasolt rendelet alapján a TLPT-re vonatkozóan kidolgozandó szabályozás- és végrehajtástechnikai standardoknak összhangban kell állniuk a TIBER-EU-val. Az EKB üdvözli továbbá a lehetőséget, hogy az európai felügyeleti hatóságokkal együttműködésben részt vehet e szabályozás- és végrehajtástechnikai standardok kidolgozásában.

4.3.6 Az illetékes hatóságoknak a tesztekben való tevékeny részvétele az általuk ellátott egyéb feladatokkal, például a pénzügyi szervezet tesztelési keretrendszerének értékelésével való potenciális összeférhetetlenséghez vezethet. Erre tekintettel az EKB azt javasolja, hogy a javasolt rendeletből kerüljön eltávolításra az illetékes hatóságokat terhelő minden olyan kötelezettség, amely a TLPT-teszthez kapcsolódó dokumentumok validálására és igazolás kiadására vonatkozik.

4.4 Harmadik féltől eredő IKT-kockázat

4.4.1 Az EKB üdvözli a harmadik félnek minősülő IKT-szolgáltatóktól eredő IKT-kockázatok azonosítására és kezelésére szolgáló alapelvek és szilárd felvigyázási keret bevezetését, függetlenül attól, hogy a pénzügyi szervezetek ugyanazon csoportjához tartoznak-e e szolgáltatók vagy nem. Ezzel együtt az IKT-kockázatok eredményes azonosításának és kezelésének elérése érdekében fontos többek között a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók helyes azonosítása és osztályozása. E tekintetben, noha az EKB üdvözli az osztályozáshoz használandó kritériumokat ([91]) a jövőben kiegészítő felhatalmazáson alapuló jogi aktusok ([92]) bevezetését, az EKB-val e felhatalmazáson alapuló jogi aktusok elfogadása előtt konzultálni kell.

([89]) Elérhető az EKB honlapján: www.ecb.europa.eu.
([90]) A javasolt rendelet 23. és 24. cikke.
([91]) Lásd a javasolt rendelet 28. cikkének (2) bekezdését.
([92]) Lásd a javasolt rendelet 28. cikkének (3) bekezdését.

4.4.2 A felvigyázási keret felépítését ([93]) illetően további pontosításra van szükség a vegyes bizottság által betöltendő szereppel kapcsolatban. Ugyanakkor az EKB üdvözli, hogy a felvigyázási fórumban megfigyelőként részt fog venni, mivel ez a szerep a dokumentációhoz és információkhoz való ugyanolyan hozzáférést fog biztosítani számára, mint amely a szavazati joggal rendelkező tagokat megilleti ([94]). Az EKB fel kívánja hívni az uniós jogalkotó szervek figyelmét arra, hogy az EKB megfigyelői szerepében a felvigyázási fórum munkájához mind a piaci infrastruktúrák felvigyázásáért való felelősséget viselő kibocsátó központi banki minőségében, mind a hitelintézetek prudenciális felügyeleti hatóságakénti minőségében hozzá fog járulni. Ezen túlmenően az EKB megjegyzi, hogy azon kívül, hogy a felvigyázási fórumban megfigyelőként részt vesz, az EKB illetékes hatóságként a közös vizsgálócsoportnak is tagja lesz. E tekintetben az uniós jogalkotó szervek további megfontolás tárgyává tehetnék a közös vizsgálócsoportok ([95]) összetételét annak érdekében, hogy az érintett illetékes hatóságok megfelelően súlyozott részvételét biztosítsák. Hasonlóképpen, az EKB úgy véli, hogy a közös vizsgálócsoportokban részt vevő személyek maximális számát növelni kell, figyelembe véve a harmadik fél által nyújtott IKT-szolgáltatások kritikus jellegét, összetettségét és terjedelmét.

4.4.3 Az EKB megjegyzi, hogy a javasolt rendelet alapján a vezető felvigyázó megakadályozhatja, hogy a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók alvállalkozási megállapodást kössenek, amennyiben i. a bevonni tervezett alvállalkozó harmadik félnek minősülő IKT-szolgáltató vagy harmadik országban letelepedett IKT-alvállalkozó, és ii. az alvállalkozó bevonása a pénzügyi szervezet kulcsfontosságú vagy lényeges funkciójának ellátására irányul. Az EKB hangsúlyozni kívánja, hogy e hatáskört a vezető felvigyázó az alvállalkozási megállapodásokkal összefüggésben csak akkor gyakorolhatja, ha valamely harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató harmadik országban letelepedett külön jogalannyal valamely kulcsfontosságú vagy lényeges funkcióra vonatkozóan köt alvállalkozási szerződést. Az EKB értelmezése szerint a vezető felvigyázó nem gyakorolhat hasonló hatáskört annak megakadályozása érdekében, hogy valamely harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató a pénzügyi szervezet kulcsfontosságú vagy lényeges funkcióit az adott szolgáltató harmadik országban található létesítményeihez szervezze ki. Előfordulhat például, hogy működési szempontból kulcsfontosságú adatokat és/vagy információkat az Európai Gazdasági Térségen (EGT) kívül található létesítmények tárolnak vagy kezelnek. Ilyen esetben a vezető felvigyázó nem tudja megfelelően felhatalmazni az illetékes hatóságokat a pénzügyi szervezet valamennyi kulcsfontosságú vagy lényeges funkciójának ellátása szempontjából releváns valamennyi információhoz, helyiséghez, infrastruktúrához és személyzethez való hozzáférésre. Annak biztosítása érdekében, hogy az illetékes hatóságok akadálytalanul el tudják látni feladataikat, az EKB javasolja, hogy a vezető felvigyázó számára biztosítsanak hatáskört arra, hogy korlátozza az EGT-n kívül található létesítményeknek a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók általi igénybevételét. Ezt a hatáskört azokban a konkrét esetekben lehetne gyakorolni, amikor az érintett harmadik országbeli hatóságokkal nem állnak fenn a javasolt rendeletben foglaltak szerinti igazgatási megállapodások ([96]), vagy a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató képviselői az érintett harmadik ország keretrendszere alapján nem nyújtottak elegendő biztosítékot az információkhoz, helyiségekhez, infrastruktúrához és személyzethez való, a felvigyázási vagy felügyeleti feladatok ellátásához szükséges hozzáférést illetően.

4.4.4 Végül, fennáll a kockázata, hogy nem bizonyul eredményesnek annak előírása, hogy az illetékes hatóságok biztosítsák a vezető felvigyázó ajánlásainak utókövetését ([97]), mivel az illetékes hatóságok adott esetben nem rendelkeznek az egyes harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók okozta kockázatokról alkotott holisztikus képpel. Ezenkívül az illetékes hatóságoknak adott esetben fel kell lépniük a felügyelt pénzügyi szervezeteikkel szemben, amennyiben a harmadik félnek minősülő kulcsfontosságú szolgáltatók nem tesznek eleget az ajánlásoknak. A javasolt rendelet ([98]) alapján az illetékes hatóságok előírhatják a felügyelt pénzügyi szervezeteik számára a harmadik fél által nyújtott kulcsfontosságú szolgáltatás átmeneti felfüggesztését vagy a harmadik félnek minősülő kulcsfontosságú szolgáltatóval kötött fennálló szerződések megszüntetését. Az előirányzott utókövetési folyamatot nehéz konkrét intézkedésekre lefordítani. Közelebbről, nem világos, hogy a felügyelt pénzügyi szervezet olyan helyzetben lesz-e, hogy a harmadik félnek minősülő kulcsfontosságú szolgáltatóval kötött szerződést fel tudja függeszteni vagy meg tudja szüntetni. Ennek az az oka, hogy a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató lehet az adott pénzügyi szervezet számára jelentős szolgáltató, vagy ez lehet azon költségek és – szerződésen alapuló vagy egyéb – kártérítés miatt, amelyek a pénzügyi szervezetet a felfüggesztés vagy megszüntetés következtében terhelhetik. Ezen túlmenően ez a megközelítés nem segíti elő a felvigyázási konvergenciát, mivel az illetékes hatóságok ugyanazt az ajánlást különféleképpen értelmezhetik. Ez végső soron akadályozhatja a kulcsfontosságú harmadik féltől eredő IKT-kockázat uniós szintű nyomon követése terén előirányzott harmonizációt és egységes megközelítést. A fentiekre tekintettel az uniós jogalkotó szervek meg kívánhatják fontolni, hogy a jog szerinti felvigyázókat a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókkal szemben különös végrehajtási hatáskörökkel ruházzák fel, figyelembe véve a – Bíróság által az ESMA ügyben hozott ítéletében ([99]) részlegesen mérsékelt – Meroni-elv által előírt korlátokat.

([93]) Lásd a javasolt rendelet 29. cikkét.
([94]) Lásd a javasolt rendelet 29. cikkének (3) bekezdését.
([95]) Lásd a javasolt rendelet 35. cikkét.
([96]) Lásd a javasolt rendelet 39. cikkének (1) bekezdését.
([97]) Lásd a javasolt rendelet 29. cikkének (4) bekezdését és 37. cikkét.
([98]) Lásd a javasolt rendelet 37. cikkének (3) bekezdését.
([99]) Lásd a Bíróság (nagytanács) 2014. január 22-i Nagy-Britannia és Észak-Írország Egyesült Királysága kontra Európai Parlament és az Európai Unió Tanácsa ítéletét, (a 236/2012/EU rendeletre vonatkozó) C-270/12. sz. ügy.

Abban az esetben, ahol az EKB a javasolt rendelet 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, 2021. június 4-én.

az EKB elnöke
Christine LAGARDE