2025/295

2025.2.13.

A BIZOTTSÁG (EU) 2025/295 FELHATALMAZÁSON ALAPULÓ RENDELETE

(2024. október 24.)

az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek a felvigyázási tevékenységek végzését lehetővé tevő előfeltételek harmonizációjáról szóló 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, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról szóló, 2022. december 14-i (EU) 2022/2554 európai parlamenti és tanácsi rendeletre [1] és különösen annak 41. cikke (2) bekezdésének második albekezdésére,

mivel:

(1) Az (EU) 2022/2554 rendelet által a pénzügyi ágazat digitális működési rezilienciája érdekében létrehozott keret a pénzügyi szektor számára szolgáltatásokat nyújtó és az említett rendelet 31. cikkével összhangban kritikusnak minősített harmadik fél információs és kommunikációs technológiai (IKT) szolgáltatókra vonatkozó uniós felvigyázási keretrendszert vezet be.

(2) Annak a harmadik fél IKT-szolgáltatónak, amely úgy dönt, hogy kritikusként való kijelölés iránti saját kezdeményezésű kérelmet nyújt be, minden szükséges információt be kell nyújtania az átvevő európai felügyeleti hatósághoz (EFH) annak érdekében, hogy az (EU) 2022/2554 rendeletben meghatározott elvekkel és kritériumokkal összhangban bizonyítsa kritikusságát. Ennélfogva az önkéntes kérelemben feltüntetendő információknak kellően részletesnek és teljesnek kell lenniük ahhoz, hogy lehetővé tegyék az említett rendelet 31. cikkének (11) bekezdése értelmében vett kritikusság egyértelmű és teljeskörű értékelését. Az illetékes EFH-nak vissza kell utasítania minden hiányos kérelmet, és hiánypótlást kell kérnie.

(3) Az e szabályozástechnikai standardok hatálya alá tartozó harmadik fél IKT-szolgáltatók jogi azonosítását össze kell hangolni az (EU) 2022/2554 rendelet 28. cikkének (9) bekezdésével összhangban elfogadott bizottsági végrehajtási rendeletben meghatározott azonosító kóddal.

(4) A vezető felvigyázó kritikus harmadik fél IKT-szolgáltatóknak címzett ajánlásainak nyomon követéseként a vezető felvigyázónak figyelemmel kell kísérnie, hogy a kritikus harmadik fél IKT-szolgáltatók betartják-e az ajánlásokat. Annak érdekében, hogy biztosítsák a kritikus harmadik fél IKT-szolgáltatók által ezen ajánlásokkal kapcsolatban tett intézkedések vagy végrehajtott korrekciók és eredményes nyomon követését, a vezető felvigyázó számára lehetővé kell tenni, hogy megkövetelje az (EU) 2022/2554 rendelet 35. cikke (1) bekezdésének c) pontjában említett jelentéseket, amelyeket időközi eredményjelentésnek és zárójelentésnek kell tekinteni.

(5) Az (EU) 2022/2554 rendelet 42. cikkének (1) bekezdésében meghatározott értékelés céljából, amely szerint a vezető felvigyázó köteles értékelni, hogy a kritikus harmadik fél IKT-szolgáltató által nyújtott magyarázat elegendő-e, a kritikus harmadik fél IKT-szolgáltató által a vezető felvigyázónak küldött, a kapott ajánlások követésére irányuló szándékáról szóló értesítést ki kell egészíteni az ajánlásokban felvázolt kockázatok csökkentése érdekében hozott intézkedések és intézkedések és azok határidejének leírásával. Az ilyen magyarázatnak korrekciós terv formáját kell öltenie.

(6) Mivel a vezető felvigyázónak értékelnie kell a kritikus harmadik fél IKT-szolgáltatók alvállalkozási megállapodásait, ki kell dolgozni az ilyen megállapodásokra vonatkozó információk benyújtására szolgáló sablont. E sablonnak figyelembe kell vennie azt a tényt, hogy a kritikus harmadik fél IKT-szolgáltatók más felépítéssel rendelkeznek, mint a pénzügyi szervezetek.

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

(7) Miután a vezető felvigyázó kiadta egy adott kritikus IKT-szolgáltatónak címzett ajánlásait, és az illetékes hatóságok tájékoztatták az érintett pénzügyi szervezeteket az ajánlásokban azonosított kockázatokról, a vezető felvigyázónak figyelemmel kell kísérnie és értékelnie kell a kritikus harmadik fél IKT-szolgáltató által az ajánlások teljesítése érdekében tett intézkedéseket és végrehajtott korrekciókat. Az illetékes hatóságoknak nyomon kell követniük és értékelniük kell, hogy a pénzügyi szervezetek milyen mértékben vannak kitéve az ezen ajánlásokban azonosított kockázatoknak. Annak érdekében, hogy feladataik ellátása során fenntartsák az egyenlő versenyfeltételeket, különösen akkor, ha az ajánlásokban azonosított kockázatok súlyosak és több tagállam számos pénzügyi szervezete között oszlanak meg, mind az illetékes hatóságoknak, mind a vezető felvigyázónak meg kell osztaniuk egymással a feladataik ellátásához szükséges releváns megállapításokat. Az információmegosztás célja annak biztosítása, hogy a vezető felvigyázó által a kritikus harmadik fél IKT-szolgáltatónak az utóbbi által végrehajtott intézkedésekkel és korrekciókkal kapcsolatban adott visszajelzések figyelembe vegyék a pénzügyi szervezetek kockázataira gyakorolt hatást, és hogy az illetékes hatóságok által végzett felügyeleti tevékenységek a vezető felvigyázó által végzett értékelésen alapuljanak.

(8) A hatékony és eredményes információmegosztás érdekében az illetékes hatóságoknak felügyeleti tevékenységeik részeként fel kell mérniük, hogy az általuk felügyelt pénzügyi szervezetek milyen mértékben vannak kitéve az ajánlásokban azonosított kockázatoknak. Ezt az értékelést arányosan és kockázati alapon kell elvégezni. A vezető felvigyázónak célszerű felkérnie az illetékes hatóságokat, hogy osszák meg ennek az értékelésnek az eredményeit azokban a konkrét esetekben, amikor az ajánlásokban azonosított kockázatok súlyosak, és több tagállamban sok pénzügyi szervezetet érintenek. Az illetékes hatóságok erőforrásainak legjobb kihasználása érdekében, amikor az értékelés eredményeinek megosztását kéri, a vezető felvigyázónak mindig figyelembe kell vennie, hogy ezeknek a kéréseknek a célja az intézkedések és a korrekciók kritikus harmadik fél IKT-szolgáltatók általi végrehajtásának értékelése.

(9) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([2]) 42. cikkének (1) bekezdésével összhangban a Bizottság egyeztetett az európai adatvédelmi biztossal, aki 2024. július 22-én véleményt nyilvánított.

(10) E rendelet alapját az európai felügyeleti hatóságok által a Bizottságnak benyújtott szabályozástechnikai standardtervezetek képezik.

(11) Az európai felügyeleti hatóságok vegyes bizottsága nyilvános konzultációt folytatott az e rendelet alapját képező szabályozástechnikai standardtervezetekről, elemezték az esetleges kapcsolódó költségeket és hasznokat, továbbá kikérték az 1093/2010/EU európai parlamenti és tanácsi rendelet ([3]) 37. cikkével összhangban létrehozott banki érdekképviseleti csoport, az 1094/2010/EU európai parlamenti és tanácsi rendelet ([4]) 37. cikkével összhangban létrehozott biztosítási és viszontbiztosítási érdekképviseleti csoport, valamint az 1095/2010/EU európai parlamenti és tanácsi rendelet ([5]) 37. cikkével összhangban létrehozott értékpapírpiaci érdekképviseleti csoport véleményét,

([2]) 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. o., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([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 1095/2010/EU rendelete (2010. november 24.) 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).

ELFOGADTA EZT A RENDELETET:

1. cikk

A kritikusként való kijelölés iránti kérelemben a harmadik fél IKT-szolgáltató által benyújtandó információk

(1) Az információs és kommunikációs technológiai (a továbbiakban: IKT) harmadik fél szolgáltató az alábbi információkat köteles benyújtani az (EU) 2022/2554 rendelet 31. cikkének (11) bekezdése szerinti, arra irányuló önkéntes kérelmében, hogy az (EU) 2022/2554 rendelet 31. cikke (1) bekezdésének a) pontja értelmében kritikusnak minősítsék:

a) a jogi személy neve;

b) a jogi személy azonosító kódja;

c) a kritikus harmadik fél IKT-szolgáltató kapcsolattartójának neve és elérhetőségei;

d) az ország, ahol a jogi személy bejegyzett székhelye található;

e) a vállalat felépítésének ismertetése, amely tartalmazza legalább az anyavállalatára és az uniós pénzügyi szervezeteknek IKT-szolgáltatásokat nyújtó más kapcsolt vállalkozásokra vonatkozó információkat. Ezen információknak adott esetben magukban kell foglalniuk a következőket:

   i. a jogi személyek neve;

   ii. a jogi személy azonosító kódja;

   iii. az ország, ahol a jogi személy bejegyzett székhelye található;

f) a harmadik fél IKT-szolgáltató becsült piaci részesedése az uniós pénzügyi szektorban, valamint piaci részesedése az (EU) 2022/2554 rendelet 2. cikkének (1) bekezdésében említett pénzügyiszervezet-típusonkénti bontásban a kritikusként való kijelölés iránti kérelem benyújtásának évében és az azt megelőző évben;

g) az uniós pénzügyi szervezetek számára nyújtott valamennyi IKT-szolgáltatás leírása, beleértve:

   i. az üzleti tevékenység jellegének és a pénzügyi szervezeteknek nyújtott IKT-szolgáltatások típusának leírása;

   ii. a nyújtott IKT-szolgáltatások révén támogatott pénzügyi szervezetek funkcióinak listája, amennyiben ilyen lista rendelkezésre áll;

   iii. arra vonatkozó információk, hogy a pénzügyi szervezeteknek nyújtott IKT-szolgáltatások kritikus vagy fontos funkciókat támogatnak-e, amennyiben ilyen információk rendelkezésre állnak;

h) azoknak a pénzügyi szervezeteknek a listája, amelyek igénybe veszik a harmadik fél IKT-szolgáltató által nyújtott IKT-szolgáltatásokat, beleértve a következő információkat minden egyes kiszolgált pénzügyi szervezetre vonatkozóan, amennyiben ilyen információk rendelkezésre állnak:

   i. a jogi személy neve;

   ii. a jogi személy azonosító kódja, ha a harmadik fél IKT-szolgáltatónak tudomása van róla;

   iii. az (EU) 2022/2554 rendelet 2. cikkének (1) bekezdése szerinti pénzügyiszervezet-típus;

   iv. az a földrajzi hely, ahonnan az IKT-szolgáltatásokat az adott jogi személynek nyújtják;

i) adott esetben a kritikus harmadik fél IKT-szolgáltatóknak az európai felügyeleti hatóságok által az (EU) 2022/2554 rendelet 31. cikkének (9) bekezdése értelmében közzétett, legfrissebb elérhető listáján szereplő olyan kritikus harmadik fél IKT-szolgáltatók listája, amelyek igénybe veszik a kérelmező által nyújtott szolgáltatásokat;

j) a következők tekintetében elvégzett önértékelés:

   i. a kérelmező által nyújtott egyes IKT-szolgáltatások helyettesíthetőségének mértéke, figyelembe véve a következőket:

      — a harmadik fél IKT-szolgáltató piaci részesedése az uniós pénzügyi szektorban,

— az ismert releváns versenytársak száma IKT-szolgáltatástípusonként vagy IKT-szolgáltatáscsoportonként,

— a nyújtott IKT-szolgáltatások sajátosságainak ismertetése, többek között bármely szabadalmaztatott technológia, vagy a harmadik fél IKT-szolgáltató szervezeti szerkezetének vagy tevékenységének egyedi jellemzői kapcsán;

ii. a kérelmező harmadik fél IKT-szolgáltatóval azonos IKT-szolgáltatások nyújtó alternatív IKT-szolgáltatók rendelkezésre állásának ismerete;

k) információk az uniós pénzügyi szervezeteknek nyújtott IKT-szolgáltatásokra és -infrastruktúrára vonatkozó jövőbeni üzleti stratégiáról, beleértve a vállalatcsoportban vagy irányítási struktúrában tervezett változtatásokat, új piacokra való belépést vagy új tevékenységek végzését;

l) a harmadik fél IKT-szolgáltató olyan alvállalkozóinak azonosítása, amelyeket kritikus harmadik fél IKT-szolgáltatóként kijelöltek;

m) bármely egyéb ok, amely lényeges a harmadik fél IKT-szolgáltató kritikusként való kijelölés iránti kérelme szempontjából.

(2) Amennyiben a harmadik fél IKT-szolgáltató egy vállalatcsoporthoz tartozik, az (1) bekezdésben említett információkat a csoport egésze által nyújtott IKT-szolgáltatások tekintetében be kell nyújtani.

2. cikk

A kritikus harmadik fél IKT-szolgáltató által benyújtandó, közzéteendő vagy jelentendő információk tartalma, struktúrája és formátuma

(1) A kritikus harmadik fél IKT-szolgáltatók a vezető felvigyázó kérésére minden olyan információt átadnak utóbbinak, amely ahhoz szükséges, hogy az az (EU) 2022/2554 rendelet követelményeivel összhangban felügyeleti feladatait el tudja látni.

(2) Az (1) bekezdésben említett információk a következőket tartalmazzák:

a) az alábbi felek között létrejött megállapodásokra vonatkozó információk, valamint a szerződéses dokumentumok másolatai:

i. a kritikus harmadik fél IKT-szolgáltató és az (EU) 2022/2554 rendelet 2. cikkének (1) bekezdésében említett pénzügyi szervezetek;

ii. a kritikus harmadik fél IKT-szolgáltató és annak alvállalkozói az Unióban működő pénzügyi szervezeteknek nyújtott IKT-szolgáltatások technológiai értékláncának megállapítása céljából;

b) a kritikus harmadik fél IKT-szolgáltató szervezeti és csoportfelépítésére vonatkozó információk, beleértve az azonos vállalatcsoporthoz tartozó valamennyi olyan jogalany azonosítását, amelyek közvetlenül vagy közvetve IKT-szolgáltatásokat nyújtanak pénzügyi szervezeteknek az Unióban;

c) a következők bármelyikének főrészvényeseire vonatkozó információk, beleértve a részvényesi szerkezetet és a földrajzi kiterjedésüket:

i. olyan jogi személyek, amelyek önállóan vagy kapcsolt vállalkozásaikkal együttesen a kritikus harmadik fél IKT-szolgáltató tőkéjének vagy szavazati jogainak legalább 25 %-át birtokolják;

ii. olyan jogi személyek, amelyek jogosultak a kritikus harmadik fél IKT-szolgáltató igazgatási, ügyvezető vagy felügyelő testülete tagjai többségének kinevezésére vagy felmentésére;

iii. olyan jogi személyek, amelyek egy megállapodás értelmében a részvényesek vagy tagok szavazati jogainak többségét ellenőrzik a kritikus harmadik fél IKT-szolgáltatónál;

d) a kritikus harmadik fél IKT-szolgáltató piaci részesedésére vonatkozó információk szolgáltatástípus szerinti bontásban azokon a releváns piacokon, ahol működik;

e) a kritikus harmadik fél IKT-szolgáltató belső vállalatirányítási rendszerére vonatkozó információk, beleértve annak felépítését, ismertetve az irányítással kapcsolatos felelősségi köröket és elszámoltathatósági szabályokat;

f) a kritikus harmadik fél IKT-szolgáltató vezető testülete és bármely más érintett belső bizottság üléséről készült jegyzőkönyv, amely bármilyen módon kapcsolódik az Unión belüli pénzügyi szervezetek funkcióit támogató, harmadik fél által nyújtott IKT-szolgáltatásokat érintő tevékenységekhez és kockázatokhoz;

g) a kritikus harmadik fél IKT-szolgáltató IKT-biztonságára vonatkozó információk, beleértve a vonatkozó stratégiákat, célkitűzéseket, szabályzatokat, eljárásokat, protokollokat, folyamatokat, az érzékeny adatok védelmét szolgáló ellenőrzési intézkedéseket, a hozzáférés ellenőrzését, a titkosítási gyakorlatokat, az eseményekre/incidensekre adandó válaszlépéseket ismertető terveket, valamint adott esetben az összes vonatkozó előírásnak, nemzeti és nemzetközi szabványnak való megfelelésre vonatkozó információk;

h) az adatvédelmet és az adatok – ideértve a személyes és nem személyes adatokat is – bizalmas kezelését biztosító technikai és szervezési intézkedésekre, az érzékeny adatok védelme érdekében végrehajtott ellenőrzési intézkedésekre, a hozzáférési jogosultságok ellenőrzésére, a titkosítási gyakorlatokra és az adatvédelmi incidensekre adandó válaszlépéseket ismertető tervre vonatkozó információk; amikor a személyes adatok kezelése tekintetében a harmadik fél IKT-szolgáltatóra harmadik országok jogszabályai vonatkoznak, amely magában foglalja harmadik országok kormányának az adatokhoz való hozzáférés iránti kérelmét, az országok listája és az alkalmazandó jogszabályok;

i) azokra a mechanizmusokra vonatkozó információk, amelyeket a kritikus harmadik fél IKT-szolgáltató az uniós pénzügyi szervezeteknek kínál az adathordozhatóság, az alkalmazások hordozhatósága és az interoperabilitás érdekében;

j) a pénzügyi szervezetek számára történő szolgáltatásnyújtás céljára igénybe vett adatközpontok és IKT-központok elhelyezkedésére vonatkozó információk, beleértve a kritikus harmadik fél IKT-szolgáltató összes releváns telephelyének és létesítményének listáját is – az Unión kívülieket is;

k) a harmadik országokból származó kritikus harmadik fél IKT-szolgáltatók által nyújtott szolgáltatásokra vonatkozó információk, beleértve a harmadik fél IKT-szolgáltató által kezelt személyes és nem személyes adatokra alkalmazandó jogi rendelkezésekre vonatkozó információkat is;

l) azokra az intézkedésekre vonatkozó információk, amelyeket a harmadik országokból származó kritikus harmadik fél IKT-szolgáltató és alvállalkozói az IKT-szolgáltatások nyújtásából eredő kockázatok kezelésére hoztak;

m) a kockázatkezelési keretre és az incidenskezelési keretre vonatkozó információk, ideértve a kritikus harmadik fél IKT-szolgáltató és alvállalkozói szabályzatait, eljárásait, eszközeit, mechanizmusait és irányítási megállapodásait, többek között az Unión belüli pénzügyi szervezetekre közvetlen vagy közvetett hatást gyakorló jelentős események listáját és ismertetését, beleértve az esemény pénzügyi szervezetekre gyakorolt jelentőségének meghatározásához és a lehetséges határokon átnyúló hatások felméréséhez szükséges, releváns adatokat;

n) a változáskezelési keretre vonatkozó információk, beleértve a kritikus harmadik fél IKT-szolgáltató és alvállalkozói szabályzatait, eljárásait és kontrolljait;

o) a kritikus harmadik fél IKT-szolgáltató átfogó reagálási és helyreállítási keretére vonatkozó információk, ideértve az üzletmenet-folytonossági terveket és a kapcsolódó intézkedéseket és eljárásokat, a szoftverfejlesztési életciklusra vonatkozó irányelveket, a reagálási és helyreállítási terveket és a kapcsolódó intézkedéseket és eljárásokat, valamint a biztonsági mentésre vonatkozó intézkedéseket és eljárásokat;

p) a teljesítmény és a biztonsági figyelemmel kísérésére és az események nyomon követésére vonatkozó információk, valamint a szolgáltatások teljesítésére, az eseményekre, továbbá a szolgáltatási szintre vonatkozó megállapodásoknak (SLA-k) és szolgáltatási szintre vonatkozó céloknak (SLO-k) vagy a kritikus harmadik fél IKT-szolgáltatók és az uniós pénzügyi szervezetek között létrejött hasonló megállapodásoknak való megfelelésre irányuló jelentési mechanizmusokra vonatkozó információk;

q) a kritikus harmadik fél IKT-szolgáltató más IKT-vel foglalkozó harmadik felek kezelésére szolgáló keretrendszerével kapcsolatos információk, beleértve a stratégiákat, szabályzatokat, eljárásokat, folyamatokat és kontrollokat, többek között a kritikus harmadik fél IKT-szolgáltató által az alvállalkozói körében azelőtt végzett átvilágításra és kockázatértékelésre vonatkozó részletes adatokat, hogy megállapodást kötne velük, és figyelemmel kísérje a kapcsolatot az összes releváns IKT- és partnerkockázatra kiterjedően;

r) a kritikus harmadik fél IKT-szolgáltató és alvállalkozói felügyeleti és átvizsgálási rendszereiből származó kivonatok, beleértve, de nem kizárólagosan a hálózatfelügyeletet, a szerverfelügyeletet, az alkalmazásfelügyeletet, a biztonsági felügyeletet, a sebezhetőségi vizsgálatokat, a naplókezelést, a teljesítményfelügyeletet, az incidenskezelést és a megbízhatósági célokkal, például SLO-kkal kapcsolatos méréseket;

s) bármely olyan éles üzemben lévő, éles üzemet megelőző szakaszban lévő és tesztelésre szolgáló rendszerből vagy alkalmazásból származó kivonatok, amelyet a kritikus harmadik fél IKT-szolgáltató és annak alvállalkozói arra használnak, hogy közvetlenül vagy közvetve szolgáltatást nyújtsanak az Unióban működő pénzügyi szervezeteknek;

t) megfelelőségi és rendelkezésre álló ellenőrzési jelentések, valamint minden releváns ellenőrzés megállapításai, beleértve az Unión belüli és az Unión kívüli nemzeti hatóságok által végzett ellenőrzéseket, amennyiben az érintett hatóságokkal kötött együttműködési megállapodások rendelkeznek ilyen információcseréről, illetve a kritikus harmadik fél IKT-szolgáltató vagy alvállalkozói által megszerzett tanúsítványok, beleértve a belső és külső ellenőrök jelentéseit, tanúsítványait, vagy az iparág-specifikus szabványoknak való megfelelőségi értékelések. Ez magában foglalja a kritikus harmadik fél IKT-szolgáltató IKT-rendszerei rezilienciájának bármely típusú elérhető független tesztelésére – beleértve a harmadik fél IKT-szolgáltató által valamely fenyegetés kapcsán végzett penetrációs (behatolási) tesztelést is – vonatkozó információkat;

u) a kritikus harmadik fél IKT-szolgáltató kérésére vagy nevében a kritikus harmadik fél IKT-szolgáltatónál kulcsfontosságú pozíciót betöltő személyek alkalmasságát és feddhetetlenségét vizsgáló értékelésekre vonatkozó információk;

v) a 3. cikk szerinti ajánlások teljesítését célzó bármely helyreállítási tervvel kapcsolatos információk, valamint a korrekciók végrehajtásának megerősítésére vonatkozó lényeges információk;

w) a rendelkezésre álló munkavállalói képzési rendszerekre és a biztonsággal kapcsolatos tudatosságot növelő programokra vonatkozó információk, beleértve adott esetben a kritikus harmadik fél IKT-szolgáltató azon beruházásaira, erőforrásaira és módszereire vonatkozó információkat, amelyek célja személyzetének az érzékeny pénzügyi adatok kezelésével és a magas szintű biztonság fenntartásával kapcsolatos képzése;

x) a kritikus harmadik fél IKT-szolgáltató tevékenységeire és a pénzügyi kimutatásaira vonatkozó információk, ideértve az IKT-val és a biztonsággal kapcsolatos költségvetésre és forrásokra vonatkozó információkat.

3. cikk

A kritikus harmadik fél IKT-szolgáltatók által az ajánlások kiadása után szolgáltatandó információk

(1) A kritikus harmadik fél IKT-szolgáltató jelentést nyújt be a vezető felvigyázóhoz, amely tartalmaz egy helyreállítási tervet, amely az ajánlásokhoz és azon korrekciókhoz kapcsolódik, amelyeket a kritikus harmadik fél IKT-szolgáltató végre kíván hajtani az (EU) 2022/2254 rendelet 35. cikke (1) bekezdésének d) pontjában említett ajánlásokban azonosított kockázatok csökkentése érdekében. A jelentésnek összhangban kell lennie a vezető felvigyázó által az egyes ajánlások esetében meghatározott ütemezéssel.

(2) A kritikus harmadik fél IKT-szolgáltató által a kapott ajánlásokkal kapcsolatban tett intézkedések vagy végrehajtott korrekciók nyomon követése érdekében a kritikus harmadik fél IKT-szolgáltató annak kérésére megosztja a vezető felvigyázóval a következőket:

a) időközi eredményjelentések és a kapcsolódó alátámasztó dokumentumok, amelyek meghatározzák a kritikus harmadik fél IKT-szolgáltató által a vezető felvigyázóhoz – az utóbbi által megállapított határidőn belül – benyújtott jelentésben szereplő tevékenységek és intézkedések végrehajtásának előrehaladását;

b) zárójelentések és a kapcsolódó alátámasztó dokumentumok, amelyek meghatározzák a kritikus harmadik fél IKT-szolgáltató által az ajánlásban azonosított kockázatok mérséklése érdekében tett intézkedéseket vagy végrehajtott korrekciókat.

4. cikk

A kritikus harmadik fél IKT-szolgáltatók által benyújtott információk struktúrája és formátuma

(1) A kritikus harmadik fél IKT-szolgáltató a kért információkat a vezető felvigyázó által annak kérelmében megjelölt, külön erre a célra szolgáló, biztonságos elektronikus csatornákon és a vezető felvigyázó által meghatározott formában nyújtja be a vezető felvigyázónak.

(2) A vezető felvigyázónak történő információszolgáltatás során a kritikus harmadik fél IKT-szolgáltatók:

a) betartják a vezető felvigyázó által az adatszolgáltatás iránti kérelemben jelzett struktúrát;

b) egyértelműen megjelölik a lényeges információkat a benyújtott dokumentációban.

(3) A kritikus harmadik fél IKT-szolgáltatók által a vezető felvigyázónak benyújtott, közzétett vagy jelentett információkat a nemzetközi pénzügyek területén szokásos nyelven kell feltüntetni.

5. cikk

Sablon az alvállalkozói megállapodásokkal kapcsolatos adatszolgáltatáshoz

Az a kritikus harmadik fél IKT-szolgáltató, amelynek meg kell osztania az alvállalkozási megállapodásokkal kapcsolatos információkat, a mellékletben található sablonnak megfelelően nyújtja be az információkat a vezető felvigyázónak.

6. cikk

A vezető felvigyázó ajánlásaiban tárgyalt kockázatok illetékes hatóságok általi értékelése

(1) A pénzügyi szervezetek felügyeletének részeként az illetékes hatóság az arányosság elvével összhangban értékeli a kritikus harmadik fél IKT-szolgáltató által a vezető felvigyázó ajánlásai alapján hozott intézkedések pénzügyi szervezetekre gyakorolt hatását.

(2) Az (1) bekezdésben említett értékelés lefolytatása során az illetékes hatóság a következők mindegyikét figyelembe veszi:

a) a pénzügyi szervezetek által az ajánlásokban azonosított kockázatok mérséklése érdekében végrehajtott korrekciós és helyreállító intézkedések megfelelősége és koherenciája;

b) a vezető felvigyázó arra vonatkozó értékelése, hogy a kritikus harmadik fél IKT-szolgáltató végrehajtja-e a jelentésben szereplő intézkedéseket és tevékenységeket, amennyiben az hatással van a hatáskörébe tartozó pénzügyi szervezeteknek az ajánlásokban azonosított kockázatoknak való kitettségére;

c) bármely más olyan illetékes hatóság álláspontja, amellyel az (EU) 2022/2554 rendelet 42. cikkének (5) bekezdésével összhangban konzultáltak;

d) a vezető felvigyázó megfelelőnek ítélte-e meg a kritikus harmadik fél IKT-szolgáltató által végrehajtott intézkedéseket és korrekciókat annak érdekében, hogy mérsékelje a vezető felvigyázó hatáskörébe tartozó pénzügyi szervezeteknek az ajánlásokban azonosított kockázatoknak való kitettségét.

(3) A vezető felvigyázó kérésére az illetékes hatóság észszerű időn belül átadja az (1) bekezdésben meghatározott értékelés eredményeit. Az értékelési eredmények átadásának kérésekor a vezető felvigyázó figyelembe veszi az arányosság elvét és az ajánlásokkal érintett kockázatok mértékét, beleértve e kockázatok határokon átnyúló hatásait is, ha egynél több tagállamban működő pénzügyi szervezeteket érintenek.

(4) Adott esetben az illetékes hatóság felkéri a pénzügyi szervezeteket, hogy adjanak meg minden olyan információt, amely az (1) bekezdésben említett értékelés elvégzéséhez szükséges.

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 24-én.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

MELLÉKLET

SABLON AZ ALVÁLLALKOZÓI MEGÁLLAPODÁSOKKAL KAPCSOLATOS INFORMÁCIÓK MEGOSZTÁSÁHOZ

Információs kategória	Legfontosabb információs elemek
Általános információk	— A kritikus harmadik fél IKT-szolgáltató neve. — A kritikus harmadik fél IKT-szolgáltató azonosító kódja. — A kritikus harmadik fél IKT-szolgáltató kapcsolattartójának neve és elérhetőségei. — A sablon benyújtásának időpontja.
Az alvállalkozói megállapodások áttekintése	— Az alvállalkozói megállapodások feltérképezése, amely magában foglalja az alvállalkozói kapcsolatok céljának és terjedelmének rövid leírását (többek között szerepelnie kell annak, hogy az alvállalkozói megállapodások mennyire kritikusak vagy fontosak a kritikus harmadik fél IKT-szolgáltató számára). — Az alvállalkozásba adott IKT-szolgáltatások típusainak meghatározása és ismertetése, valamint ezek jelentősége a pénzügyi szervezeteknek nyújtott IKT-szolgáltatások szempontjából, összhangban az (EU) 2022/2554 rendelet 28. cikkének (9) bekezdése alapján elfogadott végrehajtás-technikai standardokkal. — Az IKT-szolgáltatások típusainak meghatározásakor kérjük, olvassa el az (EU) 2022/2554 rendelet 28. cikkének (9) bekezdése alapján elfogadott végrehajtás-technikai standardoknak a IV. mellékletben található listáját.
Alvállalkozókra vonatkozó információk	— Az egyes alvállalkozók neve és a jogi személy adatai (az azonosító kóddal együtt). — A kritikus harmadik fél IKT-szolgáltató irányítási struktúrájában az egyes alvállalkozói kapcsolatokért felelős munkatársak elérhetőségei. — Minden egyes alvállalkozó esetében a szerződött IKT-szolgáltatásokhoz kapcsolódó szakértelem, tapasztalatok és képesítések áttekintése.
Az alvállalkozók által nyújtott szolgáltatások leírása	— Az egyes alvállalkozók által nyújtott konkrét IKT-szolgáltatások részletes leírása. — Az alvállalkozókra átruházott felelősségek és feladatok megoszlása az IKT-folyamatok különböző szakaszaiban betöltött szerepek részletes bemutatásával. — Arra vonatkozó információk, hogy a pénzügyi szervezeteknek nyújtott IKT-szolgáltatások kapcsán az alvállalkozók milyen szintű hozzáféréssel rendelkeznek a személyes vagy egyéb módon érzékeny adatokhoz vagy rendszerekhez. — Azokra a helyszínekre vonatkozó információk, ahonnan az alvállalkozók a szolgáltatásaikat nyújtják, valamint az Unión kívül nyújtott szolgáltatásokból eredő kockázatok kezelésére hozott intézkedésekre vonatkozó információk.
Az alvállalkozásba adás irányítása és felügyelete	— Az alvállalkozói kapcsolatok kezelésére szolgáló szerződéses és irányítási keret leírása, beleértve az érzékeny adatok felhasználását korlátozó záradékok ismertetését. — Az alvállalkozók kiválasztására, bevonására és felügyeletére szolgáló folyamatok ismertetése. — A teljesítménymutatók, a szolgáltatási szintre vonatkozó célkitűzések és megállapodások, valamint az alvállalkozói teljesítmény és megbízhatóság felügyeletére használt fő teljesítménymutatók áttekintése.
Kockázatkezelés és megfelelés	— Az alvállalkozó kockázati profiljának és a pénzügyi szervezeteknek nyújtott IKT-szolgáltatásokra gyakorolt lehetséges hatásnak az értékelése. — Az alvállalkozásban végzett tevékenységekkel kapcsolatos kockázatok kezelése érdekében végrehajtott kockázatcsökkentő intézkedések magyarázata. — Annak részletes ismertetése, hogy az alvállalkozó milyen módon felel meg a vonatkozó előírásoknak, többek között az adatvédelmi és iparági szabványoknak.

Információs kategória	Legfontosabb információs elemek
Üzletmenet-folytonosság és vészhelyzeti tervezés	— Az alvállalkozó üzletmenet-folytonossági, valamint reagálási és helyreállítási terveinek áttekintése. — A szolgáltatások folytonosságát biztosító intézkedések leírása az alvállalkozó által okozott fennakadások vagy a szolgáltatások alvállalkozó általi megszüntetése esetén. — Az üzletmenet-folytonossági tervek, valamint a reagálási és helyreállítási tervek alvállalkozók általi tesztelésének gyakorisága, a legutóbbi tesztek időpontjai az elmúlt 3 évben, valamint annak pontosítása, hogy a kritikus harmadik fél IKT-szolgáltató részt vett-e ezekben a tesztekben.
Jelentéstétel	— A kritikus harmadik fél IKT-szolgáltató és alvállalkozói közötti jelentéstételi mechanizmusok és a jelentéstétel gyakoriságának ismertetése.
Korrekció és incidenskezelés	— Az alvállalkozókhoz köthető incidensek, szabálysértések vagy meg nem felelés kezelésére vonatkozó eljárások vázlatos bemutatása.
Tanúsítványok és auditok	— Az alvállalkozókkal kapcsolatosan végrehajtott olyan tanúsításokra, független auditokra vagy értékelésekre vonatkozó információk, amelyek célja az alvállalkozók biztonsági kontrolljainak, minőségi szabványainak vagy előírásoknak való megfelelőségének ellenőrzése. — A kritikus harmadik fél IKT-szolgáltató által az alvállalkozók körében lefolytatott auditok időpontja és gyakorisága.