2024/1773

2024.6.25.

# A BIZOTTSÁG (EU) 2024/1773 FELHATALMAZÁSON ALAPULÓ RENDELETE

**(2024. március 13.)**

**az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek a harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokra vonatkozó szabályzat tartalmi elemeit meghatározó szabályozástechnikai standardok tekintetében történő kiegészítéséről**

**(EGT-vonatkozású szöveg)**

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a pénzügyi ágazat digitális működési rezilienciájáról, 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 28. cikke (10) bekezdésének harmadik albekezdésére,

mivel:

(1) A pénzügyi ágazat digitális működési rezilienciájára vonatkozóan az (EU) 2022/2554 rendelettel létrehozott keret előírja, hogy a pénzügyi szervezeteknek meg kell határozniuk a harmadik féltől eredő IKT-kockázat kezelésére vonatkozó bizonyos alapvető elveket, amelyek kiemelt jelentőséggel bírnak, ha a pénzügyi szervezetek – kritikus vagy fontos funkcióik támogatása érdekében – harmadik fél IKT-szolgáltatókkal működnek együtt.

(2) A pénzügyi szervezeteknek IKT-kockázatkezelési keretrendszerük részeként a harmadik féltől eredő IKT-kockázatra vonatkozó stratégiát kell elfogadniuk és azt rendszeresen felül kell vizsgálniuk. Az (EU) 2022/2554 rendelet 28. cikkének (2) bekezdésével összhangban az említett stratégiának tartalmaznia kell a harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételére vonatkozó szabályzatot. A stratégiát egyedi és adott esetben szubkonszolidált, valamint konszolidált alapon kell alkalmazni.

(3) A pénzügyi szervezetek méretüket, felépítésüket és belső szervezetüket, valamint tevékenységük és műveleteik jellegét és összetettségét tekintve igen eltérőek. Figyelembe kell venni ezt a sokféleséget, ugyanakkor elő kell írni bizonyos alapvető szabályozási követelményeket, amelyek valamennyi pénzügyi szervezet számára megfelelőek a harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételének céljából kötött szerződéses megállapodásokra vonatkozó szabályzat (a továbbiakban: szabályzat) kidolgozásához, és biztosítani kell, hogy ezeket a követelményeket arányos módon alkalmazzák.

(4) Amennyiben csoporthoz tartozó pénzügyi szervezetről van szó, a csoport összevont (konszolidált) vagy szubkonszolidált pénzügyi kimutatásainak elkészítéséért felelős anyavállalatnak ezért biztosítania kell, hogy a szabályzatot a csoporton belül következetes és koherens módon alkalmazzák.

(5) A szabályzat alkalmazása során a csoporton belüli IKT-szolgáltatókat – beleértve azokat is, amelyek teljes egészében vagy együttesen ugyanazon intézményvédelmi rendszeren belüli pénzügyi szervezetek tulajdonában állnak – harmadik fél IKT-szolgáltatónak kell tekinteni. A csoporton belüli IKT-szolgáltatók tevékenységéből eredő kockázatok eltérőek lehetnek, de a rájuk vonatkozó követelmények az (EU) 2022/2554 rendelet értelmében azonosak. Ugyanígy a szabályzatot kell alkalmazni – harmadik fél IKT-szolgáltatók láncolata esetén – azokra az alvállalkozókra, amelyek kritikus vagy fontos funkciókat vagy azok érdemi részeit támogató IKT-szolgáltatásokat nyújtanak harmadik fél IKT-szolgáltatók számára.

(6) Az, hogy a pénzügyi szervezet IKT-kockázatának kezeléséért a vezető testületet terheli a végső felelősség, olyan általános elv, amelynek a harmadik fél IKT-szolgáltatók igénybevétele tekintetében is érvényesülnie kell. Ennek a felelősségnek abban is meg kell nyilvánulnia, hogy a vezető testület folyamatosan részt vesz az IKT-kockázatkezelés kontrolljában és nyomon követésében, ami kiterjed a szabályzat legalább évente egyszer történő felülvizsgálatára.

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

(7) A vezető testület megfelelő tájékoztatása érdekében a szabályzatban egyértelműen meg kell határozni és azonosítani kell a harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételére vonatkozó szerződéses megállapodások (a továbbiakban: szerződéses megállapodások) jóváhagyására, irányítására, kontrolljára és dokumentálására vonatkozó belső hatásköröket, beleértve az (EU) 2022/2554 rendelet 28. cikke (1) bekezdésének a) pontja szerinti szerződéses megállapodások alapján nyújtott IKT-szolgáltatásokat is.

(8) A kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokra vonatkozó szerződéskötésből eredő esetleges kockázatok figyelembevétele érdekében a szabályzat szerkezetének követnie kell a harmadik fél szolgáltatókkal kötött szerződéses megállapodások életciklusának egyes fő szakaszaiban végrehajtandó valamennyi lépést.

(9) Az azonosított kockázatok mérséklése céljából a szabályzatnak ki kell terjednie a szerződéses megállapodások megtervezésére, többek között a kockázatértékelésre, az átvilágításra és az említett szerződéses megállapodások új vagy lényeges módosításaira vonatkozó jóváhagyási eljárásra. A harmadik fél IKT-szolgáltatóval létrejövő szerződéses megállapodás megkötése előtt esetleg felmerülő kockázatok kezeléséhez a szabályzatban megfelelő és arányos eljárást kell meghatározni a potenciális harmadik fél IKT-szolgáltatók kiválasztására és alkalmasságának értékelésére, és elő kell írni, hogy a pénzügyi szervezet tekintse át azon – nem kimerítő jelleggel felsorolt – elemeket, amelyeknek a harmadik fél IKT-szolgáltatóknak eleget kell tenniük. A listának tartalmaznia kell a szolgáltatók üzleti hírnevével, pénzügyi, humán és technikai erőforrásaival, információbiztonságával, szervezeti felépítésével – beleértve a kockázatkezelést is – és belső kontrolljaival kapcsolatos elemeket.

(10) A kritikus vagy fontos funkciókat támogató IKT-szolgáltatások harmadik fél IKT-szolgáltatók általi nyújtásához kapcsolódó megbízható kockázatkezelés biztosítása érdekében a szabályzatnak információkat kell tartalmaznia a szerződéses megállapodások végrehajtásáról, nyomon követéséről és irányításáról, adott esetben a konszolidált és szubkonszolidált szint vonatkozásában is. Ez magában foglalja a pénzügyi szervezetek és a harmadik fél IKT-szolgáltatók kölcsönös kötelezettségeivel kapcsolatos szerződéses rendelkezésekre vonatkozó követelményeket, amelyeket írásban kell rögzíteni. Annak érdekében, hogy az üzleti modellben vagy az üzleti környezetben bekövetkező változások esetén biztosítható legyen a hatékony felügyelet és a reziliencia megerősítése, a szabályzatban rendelkezni kell a pénzügyi szervezetek vagy kijelölt harmadik felek és illetékes hatóságok vizsgálatok elvégzésére és információkhoz való hozzáférésre vonatkozó jogáról, valamint tovább kell pontosítani a kilépési stratégiákat és a megszüntetési eljárásokat.

(11) Amennyiben a harmadik fél IKT-szolgáltatók személyes adatokat kezelnek, a szabályzat és a szerződéses megállapodások nem érintik az (EU) 2016/679 európai parlamenti és tanácsi rendelet ([2]) szerinti kötelezettségeket, és ki kell egészíteniük azokat például a személyes adatok kezelését ismertető írásbeli szerződés létrehozásával, a személyes adatok biztonságos kezelésére vonatkozó követelménnyel, valamint az említett rendeletben előírt egyéb elemek meghatározásával.

([2]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Az 1093/2010/EU európai parlamenti és tanácsi rendelet ([3]) 54. cikkében, az 1094/2010/EU európai parlamenti és tanácsi rendelet ([4]) 54. cikkében, valamint az 1095/2010/EU európai parlamenti és tanácsi rendelet ([5]) 54. cikkében említett, európai felügyeleti hatóságok vegyes bizottsága nyilvános konzultációt folytatott az e rendelet alapját képező szabályozástechnikai standardtervezetekről, elemezte a javasolt standardok esetleges költségeit és hasznát, továbbá kikérte az 1093/2010/EU rendelet 37. cikkével összhangban létrehozott Banki Érdekképviseleti Csoport, az 1094/2010/EU rendelet 37. cikkével összhangban létrehozott Biztosítási és Viszontbiztosítási Érdekképviseleti Csoport és a Foglalkoztatói-nyugdíj Érdekképviseleti Csoport, valamint az 1095/2010/EU rendelet 37. cikkével összhangban létrehozott Értékpapírpiaci Érdekképviseleti Csoport tanácsát.

(13) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([6]) 42. cikkének (1) bekezdésével összhangban a Bizottság egyeztetett az európai adatvédelmi biztossal, aki 2024. január 24-én véleményt nyilvánított,

ELFOGADTA EZT A RENDELETET:

*1. cikk*

**Általános kockázati profil és összetettség**

A harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételére vonatkozó szabályzatban (a továbbiakban: szabályzat) figyelembe kell venni a pénzügyi szervezet méretét és általános kockázati profilját, valamint szolgáltatásainak, tevékenységeinek és működésének jellegét, léptékét, továbbá szolgáltatásai nagyobb vagy kisebb mértékű összetettségének elemeit, többek között a következőkhöz kapcsolódóan:

a) a harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételére vonatkozóan a pénzügyi szervezet és a harmadik fél IKT-szolgáltató között létrejött szerződéses megállapodásban (a továbbiakban: szerződéses megállapodás) foglalt IKT-szolgáltatások típusa;

b) a harmadik fél IKT-szolgáltató szerinti hely vagy az anyavállalat szerinti hely;

c) a kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokat nyújtó, harmadik fél IKT-szolgáltató valamely tagállamban vagy harmadik országban található-e, tekintettel az IKT-szolgáltatások nyújtásának, valamint az adatok kezelésének és tárolásának helyére is;

d) a harmadik fél IKT-szolgáltatóval megosztott adatok jellege;

e) a harmadik fél IKT-szolgáltató ugyanahhoz a csoporthoz tartozik-e, mint az a pénzügyi szervezet, amelynek a szolgáltatást nyújtják;

([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 Értékpapírpiaci Hatóság) létrehozásáról, a 716/2009/EK határozat módosításáról és a 2009/77/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 84. o., ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

f) a valamely tagállam illetékes hatósága által engedélyezett, nyilvántartásba vett, illetve felügyelete vagy felvigyázása alá tartozó, vagy az (EU) 2022/2554 rendelet V. fejezetének II. szakasza szerinti felvigyázási keretrendszer hatálya alá tartozó harmadik fél IKT-szolgáltatók igénybevétele, valamint az említetteknek meg nem felelő harmadik fél IKT-szolgáltatók igénybevétele;

g) harmadik ország felügyeleti hatósága által engedélyezett, nyilvántartásba vett, illetve felügyelete vagy felvigyázása alá tartozó harmadik fél IKT-szolgáltatók igénybevétele, valamint az említetteknek meg nem felelő harmadik fél IKT-szolgáltatók igénybevétele;

h) a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások nyújtása egyetlen vagy kis számú harmadik fél IKT-szolgáltatónál összpontosul-e;

i) a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások más harmadik fél IKT-szolgáltatóra való, többek között technológiai sajátosságok miatti átruházhatósága;

j) a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások nyújtásában bekövetkező zavarok által a pénzügyi szervezet tevékenységének folytonosságára és szolgáltatásainak rendelkezésre állására gyakorolt lehetséges hatás.

*2. cikk*

**Csoportra való alkalmazás**

E rendelet szubkonszolidált vagy konszolidált alapon történő alkalmazása esetén a csoport konszolidált vagy szubkonszolidált pénzügyi kimutatásainak elkészítéséért felelős anyavállalat biztosítja, hogy a csoporthoz tartozó valamennyi pénzügyi szervezet következetesen alkalmazza a szabályzatot, és az a csoport valamennyi releváns szintjén megfelelő legyen e rendelet hatékony alkalmazásához.

*3. cikk*

**Irányítási rendszerek**

(1) A vezető testület évente legalább egyszer felülvizsgálja és szükség esetén aktualizálja a szabályzatot. A szabályzat módosításait kellő időben és a releváns szerződéses megállapodásoktól függően a lehető leghamarabb végre kell hajtani. A pénzügyi szervezet dokumentálja a végrehajtás tervezett ütemtervét.

(2) A szabályzatba bele kell foglalni azt a módszertant, amellyel meghatározható, hogy mely IKT-szolgáltatások támogatnak kritikus vagy fontos funkciókat vagy a szabályzatban hivatkozni kell erre a módszertanra. A szabályzatban továbbá meg kell határozni, hogy mikor kell elvégezni és felülvizsgálni ezt az értékelést.

(3) A szabályzatban egyértelműen meg kell határozni a releváns szerződéses megállapodások jóváhagyására, irányítására, ellenőrzésére és dokumentálására vonatkozó belső felelősségi köröket, és biztosítani kell, hogy a pénzügyi szervezeten belül megfelelő készségek, tapasztalatok és ismeretek álljanak rendelkezésre a releváns szerződéses megállapodások – és az e megállapodások alapján nyújtott IKT-szolgáltatások – hatékony felvigyázásához.

(4) A pénzügyi szervezet arra vonatkozó végső felelősségének sérelme nélkül, hogy hatékonyan felügyeli a releváns szerződéses megállapodásokat, a szabályzat előírja, hogy a harmadik fél IKT-szolgáltatónak elegendő erőforrással kell rendelkeznie annak biztosításához, hogy a pénzügyi szervezet megfeleljen a nyújtott kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokra vonatkozó valamennyi jogi és szabályozási követelménynek.

(5) A szabályzatban egyértelműen meg kell határozni egy feladatkört vagy a felső vezetés egy tagját, amely/aki felelős a releváns szerződéses megállapodások ellenőrzéséért. A szabályzatban meg kell határozni, hogy az említett feladatkörben eljáró személynek vagy a felső vezetés tagjának hogyan kell együttműködnie a kontrollfunkciókkal, kivéve, ha a feladatkör vagy a tag a kontrollfunkció részét képezi, és meg kell határozni a vezető testületnek történő jelentéstétel útvonalait, beleértve a jelentendő információk jellegét és a benyújtandó dokumentumokat. A szabályzatban meg kell határozni az említett jelentéstétel gyakoriságát is.

(6) A szabályzatnak biztosítania kell, hogy a szerződéses megállapodások összhangban legyenek a következőkkel:

a) az (EU) 2022/2554 rendelet 6. cikke szerinti IKT-kockázatkezelési keretrendszer;

b) az (EU) 2022/2554 rendelet 9. cikkének (4) bekezdése szerinti információs biztonsági szabályzat;

c) az (EU) 2022/2554 rendelet 11. cikke szerinti IKT-üzletmenetfolytonossági politika;

d) az (EU) 2022/2554 rendelet 19. cikkében meghatározott biztonsági események bejelentésére vonatkozó követelmények.

(7) A szabályzatban elő kell írni, hogy a harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokat független felülvizsgálatnak kell alávetni, és e felülvizsgálatokat bele kell foglalni az ellenőrzési tervbe.

(8) A szabályzatban kifejezetten rendelkezni kell arról, hogy a szerződéses megállapodás:

a) nem mentesíti a pénzügyi szervezetet és annak vezető testületét szabályozási kötelezettségei és ügyfeleivel szembeni felelőssége alól;

b) nem akadályozhatja a pénzügyi szervezet hatékony felügyeletét, és nem sértheti a szolgáltatásokra és tevékenységekre vonatkozó felügyeleti korlátozásokat;

c) tartalmaz arra vonatkozó előírást, hogy a harmadik fél IKT-szolgáltatók együttműködnek az illetékes hatóságokkal;

d) tartalmaz arra vonatkozó előírást, hogy a pénzügyi szervezet, annak ellenőrei és az illetékes hatóságok számára tényleges hozzáférést kell biztosítani a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételével kapcsolatos adatokhoz és helyiségekhez.

*4. cikk*

**Az életciklus fő szakaszai a szerződéses megállapodások elfogadásával és alkalmazásával összefüggésben**

A szabályzatban meg kell határozni a szerződéses megállapodás életciklusának egyes fő szakaszaira vonatkozó követelményeket, beleértve a szabályokat, a felelősségi köröket és a folyamatokat, legalább a következőkre kiterjedően:

a) a vezető testület felelősségi körei, beleértve adott esetben a harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételével kapcsolatos döntéshozatali folyamatban való részvételét;

b) a szerződéses megállapodások megtervezése, beleértve a kockázatértékelést, az 5. és a 6. cikkben meghatározott átvilágítást, valamint a 8. cikk (4) bekezdése szerinti, a szerződéses megállapodások új vagy lényeges módosításaira vonatkozó jóváhagyási eljárást;

c) az üzleti egységek, a belsőkontroll-egységek és más releváns egységek részvétele a szerződéses megállapodásokkal összefüggésben;

d) a szerződéses megállapodások végrehajtása, nyomon követése és irányítása a 7., 8. és 9. cikkben említettek szerint, adott esetben a konszolidált és szubkonszolidált szint vonatkozásában is;

e) dokumentáció és nyilvántartás, figyelembe véve az (EU) 2022/2554 rendelet 28. cikkének (3) bekezdésében az információ-nyilvántartásra vonatkozóan meghatározott követelményeket;

f) a 10. cikkben meghatározott kilépési stratégiák és megszüntetési eljárások.

*5. cikk*

**Előzetes kockázatértékelés**

(1) A szabályzatban elő kell írni, hogy a pénzügyi szervezet üzleti igényeit a szerződéses megállapodás megkötése előtt meg kell határozni.

(2) A szabályzatban rendelkezni kell arról, hogy a szerződéses megállapodás megkötése előtt kockázatértékelést kell végezni a pénzügyi szervezet szintjén, valamint adott esetben konszolidált és szubkonszolidált szinten.

A kockázatértékelésnek figyelembe kell vennie az (EU) 2022/2554 rendeletben meghatározott valamennyi vonatkozó követelményt és az alkalmazandó ágazati uniós jogszabályokat. Figyelembe kell vennie mindenekelőtt a harmadik fél IKT-szolgáltatók által a kritikus vagy fontos funkciók támogatásához nyújtott IKT-szolgáltatások pénzügyi szervezetre gyakorolt hatását, valamint a harmadik fél IKT-szolgáltatók által kritikus vagy fontos funkciók támogatásához nyújtott, említett IKT-szolgáltatásokból eredő kockázatokat, többek között a következőket:

a) működési kockázatok;

b) jogi kockázatok;

c) IKT-kockázatok;

d) reputációs kockázatok;

e) a bizalmas vagy személyes adatok védelméhez kapcsolódó kockázatok;

f) az adatok rendelkezésre állásával kapcsolatos kockázatok;

g) az adatkezelés és az adattárolás helyéhez kapcsolódó kockázatok;

h) a harmadik fél IKT-szolgáltató helyéből eredő kockázatok;

i) IKT-koncentrációs kockázatok a szervezet szintjén.

*6. cikk*

**Átvilágítás**

(1) A szabályzatban megfelelő és arányos eljárást kell meghatározni a leendő harmadik fél IKT-szolgáltatók kiválasztására és értékelésére, figyelembe véve, hogy a harmadik fél IKT-szolgáltató csoporton belüli IKT-szolgáltató-e, és elő kell írni, hogy a pénzügyi szervezetnek a szerződéses megállapodás megkötése előtt értékelnie kell, hogy a harmadik fél IKT-szolgáltató:

a) rendelkezik-e üzleti hírnévvel, megfelelő képességekkel, szakértelemmel és kellő pénzügyi, humán és technikai erőforrásokkal, információbiztonsági előírásokkal, megfelelő szervezeti felépítéssel, kockázatkezeléssel és belső kontrollokkal, valamint adott esetben a kritikus vagy fontos funkciót támogató IKT-szolgáltatások megbízható és professzionális nyújtásához szükséges engedélyekkel vagy regisztrációval;

b) képes-e arra, hogy nyomon kövesse a releváns technológiai fejleményeket, azonosítsa az IKT-biztonsággal kapcsolatos legfontosabb gyakorlatokat, és adott esetben alkalmazza azokat annak érdekében, hogy a digitális működési rezilienciára vonatkozóan hatékony és megbízható keretet biztosítson;

c) igénybe vesz-e vagy tervez-e igénybe venni kritikus vagy fontos funkciókat vagy azok érdemi részeit támogató IKT-szolgáltatásokat nyújtó IKT-alvállalkozókat;

d) harmadik országban található-e vagy az adatkezelést és -tárolást harmadik országban végzi-e, és amennyiben igen, ez a gyakorlat befolyásolja-e a működési vagy reputációs kockázatok szintjét, vagy annak kockázatát, hogy olyan korlátozó intézkedések – többek között embargók és szankciók – hatálya alá tartozik, amelyek befolyásolhatják a harmadik fél IKT-szolgáltató azon képességét, hogy IKT-szolgáltatásokat nyújtson, vagy hogy a pénzügyi szervezet igénybe vegye ezeket az IKT-szolgáltatásokat;

e) elfogadja-e azokat a szerződéses megállapodásokat, amelyek biztosítják, hogy a pénzügyi szervezet, a kijelölt harmadik felek és az illetékes hatóságok ténylegesen ellenőrzést végezhessenek a harmadik fél IKT-szolgáltatónál, beleértve a helyszíni ellenőrzéseket is;

f) etikus és társadalmilag felelős módon jár-e el, tiszteletben tartja-e az emberi jogokat és a gyermekek jogait, beleértve a gyermekmunka tilalmát, továbbá az alkalmazandó környezetvédelmi elveket, és megfelelő munkakörülményeket biztosít-e.

(2) A szabályzatban meg kell határozni a harmadik fél IKT-szolgáltatók kockázatkezelési keretrendszerének hatékonyságával kapcsolatban elvárt megbízhatósági szintet a harmadik fél IKT-szolgáltató által nyújtandó, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások tekintetében. A szabályzatban elő kell írni, hogy az átvilágítási folyamatnak magában kell foglalnia a kockázatcsökkentő és az üzletmenet-folytonossági intézkedések meglétének, valamint annak az értékelését, hogy a harmadik fél IKT-szolgáltató miként biztosítja azok alkalmazását.

(3) A szabályzatban meg kell határozni a leendő harmadik fél IKT-szolgáltatók kiválasztására és értékelésére vonatkozó átvilágítási eljárást, és ismertetni kell, hogy a harmadik fél IKT-szolgáltató teljesítményére vonatkozó elvárt megbízhatósági szint eléréséhez az alábbiak közül melyiket kell alkalmazni:

a) a pénzügyi szervezet által vagy nevében végzett ellenőrzések vagy független értékelések;

b) a harmadik fél IKT-szolgáltató kérésére készített független ellenőrzési jelentések felhasználása;

c) a harmadik fél IKT-szolgáltató belső ellenőrzési egysége által készített ellenőrzési jelentések felhasználása;

d) harmadik fél általi megfelelő tanúsítás használata;

e) a pénzügyi szervezet rendelkezésére álló egyéb releváns információk, vagy a harmadik fél IKT-szolgáltató által nyújtott egyéb információk felhasználása.

(4) A pénzügyi szervezeteknek – figyelembe véve a (3) bekezdés a)–e) pontjában felsorolt elemeket – biztosítaniuk kell, hogy a harmadik fél IKT-szolgáltató teljesítményének megbízhatósága megfelelő szintű legyen. Adott esetben az említett pontokban felsoroltak közül egynél többet kell felhasználni.

*7. cikk*

**Összeférhetetlenség**

(1) A szabályzatban meg kell határozni a harmadik fél IKT-szolgáltatók igénybevételéből eredő tényleges vagy esetleges összeférhetetlenségek azonosítása, megelőzése és kezelése céljából a releváns szerződéses megállapodások megkötése előtt meghozandó megfelelő intézkedéseket, és biztosítani kell az említett összeférhetetlenségek folyamatos nyomon követését.

(2) Amennyiben a kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokat csoporton belüli IKT-szolgáltatók nyújtják, a szabályzatban meg kell határozni, hogy az IKT-szolgáltatások feltételeire – többek között a pénzügyi feltételekre – vonatkozó döntéseket objektív módon kell meghozni.

*8. cikk*

**Szerződéses rendelkezések**

(1) A szabályzatban rendelkezni kell arról, hogy a releváns szerződéses megállapodást írásba kell foglalni, és annak tartalmaznia kell az (EU) 2022/2554 rendelet 30. cikkének (2) és (3) bekezdésében említett valamennyi elemet. A szabályzatnak tartalmaznia kell továbbá az (EU) 2022/2554 rendelet 1. cikke (1) bekezdésének a) pontjában említett követelményekkel, valamint adott esetben az egyéb vonatkozó uniós és nemzeti jogszabályokkal kapcsolatos elemeket is.

(2) A szabályzatban meg kell határozni, hogy a releváns szerződéses megállapodásoknak tartalmazniuk kell a pénzügyi szervezet információkhoz való hozzáféréssel, vizsgálatok és ellenőrzések végrehajtásával, valamint IKT-tesztek elvégzésével kapcsolatos jogát. E célból – és a pénzügyi szervezet végső felelősségének sérelme nélkül – a szabályzatban elő kell írni, hogy a pénzügyi szervezetnek alkalmaznia kell a következő módszereket:

a) saját belső ellenőrzése vagy kijelölt harmadik fél által végzett ellenőrzés;

b) adott esetben olyan csoportos ellenőrzések és csoportos IKT-tesztelés, beleértve a fenyegetés alapú behatolási tesztelést is, amelyeket az ugyanazon harmadik fél IKT-szolgáltató által nyújtott IKT-szolgáltatásokat igénybe vevő különböző szerződő pénzügyi szervezetek vagy vállalkozások közösen szerveznek, és ezek a szerződő pénzügyi szervezetek vagy vállalkozások, vagy az általuk kijelölt harmadik fél végeznek el;

c) adott esetben harmadik fél általi tanúsítás;

d) adott esetben a harmadik fél IKT-szolgáltató által rendelkezésre bocsátott belső ellenőrzési jelentések vagy harmadik fél által készített ellenőrzési jelentések.

(3) A pénzügyi szervezet nem támaszkodhat hosszabb ideig kizárólag a (2) bekezdés c) pontjában említett tanúsításra vagy az említett bekezdés d) pontjában említett ellenőrzési jelentésekre. A szabályzat csak akkor teheti lehetővé a (2) bekezdés c) és d) pontjában említett módszerek alkalmazását, ha a pénzügyi szervezet:

a) a releváns szerződéses megállapodással összefüggésben megfelelőnek tartja a harmadik fél IKT-szolgáltató ellenőrzési tervét;

b) biztosítja, hogy a tanúsítványok vagy az ellenőrzési jelentések hatálya kiterjedjen az általa azonosított rendszerekre és kulcsfontosságú kontrollokra, és biztosítja a releváns szabályozási követelményeknek való megfelelést;

c) folyamatosan elvégzi a tanúsítványok vagy ellenőrzési jelentések tartalmának részletes értékelését, és ellenőrzi, hogy a jelentések vagy tanúsítványok nem avultak-e el;

d) biztosítja, hogy a tanúsítványok vagy az ellenőrzési jelentések későbbi változatai kiterjedjenek a kulcsfontosságú rendszerekre és kontrollokra;

e) meggyőződik arról, hogy a tanúsítást vagy az ellenőrzést végző fél alkalmas a feladat elvégzésére;

f) meggyőződik arról, hogy a tanúsítványok kibocsátása és az ellenőrzések elvégzése széles körben elismert releváns szakmai normák alapján történik, és részét képezi a meglévő kulcsfontosságú kontrollok működési hatékonyságának vizsgálata;

g) szerződésben foglalt joga, hogy kockázatkezelési szempontból észszerű és jogszerű gyakorisággal kérje a tanúsítványok vagy ellenőrzési jelentések hatályának más releváns rendszerekre és kontrollokra való kiterjesztését;

h) szerződésben foglalt joga, hogy saját belátása szerint egyedi és csoportos ellenőrzéseket végezzen a szerződéses megállapodások tekintetében, és ezeket a jogokat a megállapodásban rögzített gyakorisággal hajtsa végre.

(4) A szabályzatban rendelkezni kell arról, hogy a szerződéses megállapodás lényeges módosításait valamennyi fél által aláírt és keltezett írásos dokumentumban formalizálják, és meg kell határozni a szerződéses megállapodások meghosszabbításának eljárását.

*9. cikk*

**A szerződéses megállapodások nyomon követése**

(1) A szabályzatban elő kell írni, hogy a szerződéses megállapodásokban meg kell határozni a harmadik fél IKT-szolgáltatók teljesítményének folyamatos nyomon követésére szolgáló intézkedéseket és fő mutatókat, többek között azokat az intézkedéseket, amelyek az adatok és információk bizalmas kezelésére, rendelkezésre állására, integritására és hitelességére vonatkozó követelményeknek való megfelelés, valamint a harmadik fél IKT-szolgáltatók általi, a pénzügyi szervezet vonatkozó szabályzatainak és eljárásainak való megfelelés nyomon követésére irányulnak. A szabályzatban meg kell határozni azokat az intézkedéseket is – beleértve adott esetben a szerződéses szankciókat –, amelyek akkor alkalmazandók, ha a szolgáltatási szintre vonatkozó megállapodásokat nem tartják be.

(2) A szabályzatban rendelkezni kell arról, hogy a pénzügyi szervezetnek milyen módon kell értékelnie azt, hogy a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások biztosításához igénybe vett harmadik fél IKT-szolgáltatók betartják-e a szerződéses megállapodással és a pénzügyi szervezet saját szabályzatával összhangban levő megfelelő teljesítmény- és minőségi előírásokat. A szabályzatban rendelkezni kell mindenekelőtt arról, hogy:

a) a harmadik fél IKT-szolgáltatók tevékenységükkel és szolgáltatásaikkal összefüggésben megfelelő jelentéseket – többek között időszakos jelentéseket, eseményjelentéseket, szolgáltatásnyújtási jelentéseket, az IKT-biztonságról szóló jelentéseket, valamint az üzletmenet-folytonossági intézkedésekről és tesztelésről szóló jelentéseket – nyújtsanak be a pénzügyi szervezetnek;

b) a harmadik fél IKT-szolgáltatók teljesítményét fő teljesítménymutatók, fő kontrollmutatók, ellenőrzések, öntanúsítások és független felülvizsgálatok révén értékeljék a pénzügyi szervezet IKT-kockázatkezelési keretrendszerével összhangban;

c) a harmadik fél IKT-szolgáltatók továbbítsák a pénzügyi szervezetnek az egyéb releváns információkat;

d) a pénzügyi szervezet adott esetben értesítést kapjon az IKT-vonatkozású eseményekről, valamint a pénzforgalmi vonatkozású működési zavarokról vagy biztonsági eseményekről;

e) sor kerüljön a jogi és szabályozási követelményeknek és előírásoknak való megfelelést ellenőrző független felülvizsgálatra és ellenőrzésekre.

(3) A szabályzatban meg kell határozni, hogy a (2) bekezdésben említett értékelést dokumentálni kell, és annak eredményeit fel kell használni a pénzügyi szervezet 6. cikk szerinti kockázatértékelésének aktualizálásához.

(4) A szabályzatba bele kell foglalni azokat a megfelelő intézkedéseket, amelyeket a pénzügyi szervezetnek abban az esetben kell hoznia, ha a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások nyújtásával, illetve a szerződéses megállapodásoknak vagy jogi követelményeknek való megfeleléssel kapcsolatban a harmadik fél IKT-szolgáltatóknál hiányosságokat tár fel, ideértve az IKT-vonatkozású eseményeket és a pénzforgalmi vonatkozású működési zavarokat vagy biztonsági eseményeket is. Meg kell határozni továbbá az említett intézkedések nyomon követésének módját, biztosítva, hogy azokat – figyelembe véve a hiányosságok lényegességét – meghatározott határidőn belül eredményesen végrehajtsák.

*10. cikk*

**A szerződéses megállapodásból való kilépés és a megállapodás megszüntetése**

A szabályzatba bele kell foglalni az egyes szerződéses megállapodásokra vonatkozó dokumentált kilépési tervre, valamint a dokumentált kilépési terv rendszeres felülvizsgálatára és tesztelésére vonatkozó követelményeket. A kilépési terv kidolgozásakor a következőket kell figyelembe venni:

a) a szolgáltatásnyújtás előre nem látható és tartós zavara;

b) nem megfelelő vagy sikertelen szolgáltatásnyújtás;

c) a szerződéses megállapodás váratlan megszüntetése.

A kilépési tervnek reálisnak, megvalósíthatónak kell lennie, megalapozott forgatókönyveken és észszerű feltételezéseken kell alapulnia, és olyan tervezett végrehajtási ütemtervvel kell rendelkeznie, amely összeegyeztethető a szerződéses megállapodásokban meghatározott kilépési és megszüntetési feltételekkel.

*11. 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. március 13-án.

*a Bizottság részéről*
*az elnök*
Ursula VON DER LEYEN