Az Európai Unió
Hivatalos Lapja

L 333

65. évfolyam

Magyar nyelvű kiadás **Jogszabályok**

2022. december 27.

Tartalom

[1] EGT-vonatkozású szöveg.

HU

Azok a jogi aktusok, amelyek címe normál szedéssel jelenik meg, a mezőgazdasági ügyek napi intézésére vonatkoznak, és rendszerint csak korlátozott ideig maradnak hatályban.

Valamennyi más jogszabály címét vastagon szedik, és előtte csillag szerepel.

I

(Jogalkotási aktusok)

RENDELETEK

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2554 RENDELETE

(2022. december 14.)

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

(EGT-vonatkozású szöveg)

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 114. cikkére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Központi Bank véleményére ([1]),

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére ([2]),

rendes jogalkotási eljárás keretében ([3]),

mivel:

(1) A digitális korban a mindennapos tevékenységek során alkalmazott összetett rendszereket információs és kommunikációs technológia (IKT) támogatja. Ez biztosítja a gazdaság folyamatos működését az ágazatokban, többek között a pénzügyi ágazatban, és javítja a belső piac működését is. A megnövekedett digitalizáció és az összekapcsoltság felerősíti az IKT-kockázatot is, kiszolgáltatottabbá téve a társadalom egészét és különösen a pénzügyi rendszert, a kiberfenyegetésekkel és az IKT-zavarokkal szemben. Míg az IKT-rendszerek általános alkalmazása, valamint a nagy fokú digitalizáció és összekapcsoltság ma az uniós pénzügyi szervezetek tevékenységeire alapvetően jellemző, a digitális rezilienciájukkal többet kell még foglalkozni, és azt jobban kell integrálni a tágabb működési kereteikbe.

(2) Az IKT használata az elmúlt évtizedekben lényeges szerepet nyert a pénzügyi szolgáltatások nyújtása terén, egészen addig a pontig, hogy mára kritikus fontosságra tett szert a valamennyi pénzügyi szervezet által ellátott tipikus mindennapos funkciók működésében. A digitalizáció mostanra kiterjed például a fizetésekre amelyek a készpénz- és papíralapú módszerektől mind inkább a digitális megoldások alkalmazása felé mozdultak el , valamint az értékpapírok elszámolására és kiegyenlítésére, az elektronikus és algoritmikus kereskedésre, a hitelnyújtási és finanszírozási műveletekre, a személyközi finanszírozásra, a hitelminősítésekre, a követeléskezelésre és a háttértevé-

([1]) HL C 343., 2021.8.26., 1. o.
([2]) HL C 155., 2021.4.30., 38. o.
([3]) Az Európai Parlament 2022. november 10-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2022. november 28-i határozata.

kenységekre. Az IKT-technológia használata a biztosítási ágazatot is átalakította, az InsturTech-hel működő, szolgáltatásaikat online kínáló biztosításközvetítők megjelenésétől kezdve a digitális biztosítási kockázatvállalásig. Amellett, hogy a pénzügyi szolgáltatások az ágazat egészében nagyrészt digitálissá váltak, a digitalizáció fokozottabb összekapcsoltságot és kölcsönös függést is eredményezett a pénzügyi ágazaton belül, valamint a harmadik felektől igénybe vett infrastruktúrák és szolgáltatások terén.

(3) Az Európai Rendszerkockázati Testület (ERKT) a rendszerszintű kiberkockázattal foglalkozó 2020. évi jelentésében megerősítette, hogy a pénzügyi szervezetek, a pénzügyi piacok és a pénzügyi piaci infrastruktúrák meglévő nagy fokú összekapcsoltsága és különösen az IKT-rendszereik kölcsönös függései miképpen jelenthetnek rendszerszintű sérülékenységet amiatt, hogy a lokalizált kiberbiztonsági események a mintegy 22 000 uniós pénzügyi szervezet bármelyikéről gyorsan, földrajzi határoktól függetlenül átterjedhetnek a teljes pénzügyi rendszerre. Súlyos IKT-biztonsági sérülések, amelyek előfordulnak a pénzügyi ágazatban, nem csak elszigetelt pénzügyi szervezeteket érintenek. Lehetővé teszik a lokalizált sérülékenységek pénzügyi transzmissziós csatornákon keresztüli zavartalan terjedését is, és potenciálisan kedvezőtlen következményekkel járhatnak az Unió pénzügyi rendszerének stabilitására nézve, így például likviditáselvonási hullámokat és a pénzügyi piacokkal szembeni általános bizalomvesztést kelthetnek.

(4) Az elmúlt években az IKT-kockázat magára vonzotta a nemzetközi, uniós és nemzeti szakpolitikai döntéshozók, szabályozó és standardalkotó szervek figyelmét, arra törekedve, hogy fokozzák a digitális rezilienciát, rögzítsenek standardokat, és koordinálják a szabályozói és felügyeleti munkát. Nemzetközi szinten a Bázeli Bankfelügyeleti Bizottság, a Fizetési és Piaci Infrastruktúra Bizottság, a Pénzügyi Stabilitási Tanács, a Pénzügyi Stabilitási Intézet, valamint a G7 és a G20 célja az, hogy a különböző joghatóságokban az illetékes hatóságokat és a piaci szereplőket olyan eszközökhöz juttassák, amelyek támogatják pénzügyi rendszereik rezilienciáját. Az említett munkát annak szükségessége is vezérli, hogy az IKT-kockázatot – egy nagymértékben összekapcsolt globális pénzügyi rendszer összefüggésében – megfelelően figyelembe vegyék, és a releváns legjobb gyakorlatok terén nagyobb következetességre törekedjenek.

(5) Az uniós és nemzeti célzott szakpolitikai és jogalkotási kezdeményezések ellenére az IKT-kockázat továbbra is kihívást jelent az uniós pénzügyi rendszer digitális működési rezilienciája, teljesítménye és stabilitása szempontjából. A 2008. évi pénzügyi válságot követő reformok elsősorban az uniós pénzügyi ágazat pénzügyi rezilienciáját erősítették, és arra irányultak, hogy – gazdasági és prudenciális szempontból, valamint a piaci magatartás tekintetében – megóvják az Unió versenyképességét és stabilitását. Bár az IKT-biztonság és a digitális reziliencia a működési kockázat részei, a pénzügyi válság utáni szabályozási menetrendben kisebb hangsúlyt kaptak, és fejlesztésükre az Unió pénzügyi szolgáltatásokkal kapcsolatos szakpolitikájának és szabályozási környezetének csak egyes területein vagy csak néhány tagállamban került sor.

(6) A „Pénzügyi technológiai cselekvési terv: Egy versenyképesebb és innovatívabb európai pénzügyi ágazat felé” című, 2018. március 8-i közleményében a Bizottság kiemelte annak kiemelkedő fontosságát, hogy az uniós pénzügyi ágazatot – többek között működési szempontból is – reziliensebbé kell tenni annak érdekében, hogy garantált legyen technológiai biztonsága és megfelelő működése, az IKT-biztonsági sérüléseket és eseményeket követő gyors helyreállítása, ami végső soron lehetővé teszi a pénzügyi szolgáltatások hatékony és zökkenőmentes nyújtását az Unió egészében stresszkörülmények között is, egyúttal hozzájárul a fogyasztói és piaci bizalom megóvásához is.

(7) 2019 áprilisában az 1093/2010/EU európai parlamenti és tanácsi rendelettel ([4]) létrehozott európai felügyeleti hatóság (Európai Bankhatóság, EBH), az 1094/2010/EU európai parlamenti és tanácsi rendelettel ([5]) létrehozott európai felügyeleti hatóság (Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság, EIOPA) és az 1095/2010/EU

([4]) 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.).

([5]) 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.).

európai parlamenti és tanácsi rendelettel ([6]) létrehozott európai felügyeleti hatóság (Európai Értékpapírpiaci Hatóság, ESMA) (a továbbiakban együttesen: európai felügyeleti hatóságok vagy EFH-k) együttes szakvéleményt adtak ki, szorgalmazva a pénzügyi szolgáltatási ágazat IKT-kockázatához való koherens megközelítést, és javaslatot téve a pénzügyi szolgáltatási ágazat digitális működési rezilienciájának egy ágazatspecifikus uniós kezdeményezésen keresztül, arányos módon történő megerősítésére.

(8) Az uniós pénzügyi ágazatot egységes szabálykönyv szabályozza, és a Pénzügyi Felügyeletek Európai Rendszere irányítja. Mindazonáltal a digitális működési rezilienciára és az IKT-biztonságra vonatkozó rendelkezések egyelőre nem teljesen, vagy nem következetesen harmonizáltak annak ellenére, hogy a digitális korban a digitális működési reziliencia létfontosságú a pénzügyi stabilitás és a piaci integritás biztosításához, és legalább olyan fontos, mint például a prudenciális vagy a piaci magatartásra vonatkozó általános előírások. Az egységes szabálykönyvet és a felügyeleti rendszert ezért olyan módon kell továbbfejleszteni, hogy azok a digitális működési rezilienciára is kiterjedjenek; ehhez meg kell erősíteni az illetékes hatóságok megbízatását, hogy e hatóságok – a belső piac integritásának és hatékonyságának védelme, valamint a piac szabályos működésének elősegítése érdekében – felügyelni tudják az IKT-kockázat kezelését a pénzügyi ágazatban.

(9) A jogszabályi eltérések, valamint az IKT-kockázattal kapcsolatos heterogén nemzeti szabályozási és felügyeleti megközelítések akadályozzák a pénzügyi szolgáltatások belső piacának működését, és megnehezítik a határokon átnyúló tevékenységet végző pénzügyi szervezetek számára a letelepedés és a szolgáltatásnyújtás szabadságának zavartalan gyakorlását. Torzulhat a verseny a különböző tagállamokban tevékenységet folytató, azonos típusú pénzügyi szervezetek között is. Különösen igaz ez olyan területeken, ahol az uniós harmonizáció eddig nagyon korlátozottan valósult meg, így például a digitális működési reziliencia tesztelése tekintetében, vagy ahol hiányzik, így például a harmadik féltől eredő IKT-kockázat nyomon követése tekintetében. A nemzeti szintű tervezett fejlesztésekből adódó eltérések további akadályokat képezhetnek a belső piac működésében a piaci szereplők és a pénzügyi stabilitás kárára.

(10) Annak köszönhetően, hogy az IKT-kockázattal kapcsolatos rendelkezéseket uniós szinten csak részben kezelték, máig hiányosságok vagy átfedések mutatkoznak olyan fontos területeken, mint az IKT-vonatkozású események bejelentése és a digitális működési reziliencia tesztelése, továbbá következetlenségek is a megjelenő, egymástól eltérő nemzeti szabályoknak vagy az egymást átfedő szabályok nem költséghatékony alkalmazásának eredményeként. Ez különösen hátrányos az IKT olyan, intenzív felhasználóira nézve, mint a pénzügyi ágazat, mivel a technológiai kockázatok nem ismernek határokat, és a pénzügyi ágazat az Unión belül és azon kívül kiterjedt, határokon átnyúló jelleggel kínálja szolgáltatásait. Egyedi pénzügyi szervezetek, amelyek határokon átnyúló tevékenységet végeznek, vagy több engedéllyel is rendelkeznek (például ugyanaz a pénzügyi szervezet bankként, befektetési vállalkozásként és pénzforgalmi intézményként is rendelkezhet működési engedéllyel, amelyek mindegyikét más-más illetékes hatóság adta ki egy vagy több tagállamban), működési kihívásokkal szembesülnek az IKT-kockázat önálló, koherens és költséghatékony kezelése, valamint az IKT-vonatkozású események káros hatásainak enyhítése során.

(11) mivel az egységes szabálykönyvet nem egészítette ki átfogó IKT- vagy működésikockázat-kezelési keret, a digitális működési rezilienciára vonatkozó követelmények további harmonizációjára van szükség valamennyi pénzügyi szervezet tekintetében. Az IKT-képességek és az általános reziliencia pénzügyi szervezetek általi, az említett alapkövetelményeken alapuló, az üzemszünetek elviselése céljából történő fejlesztése elősegítené az uniós pénzügyi piacok stabilitásának és integritásának megőrzését, és így hozzájárulna a befektetők és fogyasztók magas szintű védelmének biztosításához az Unióban. Mivel e rendelet célja, hogy hozzájáruljon a belső piac zavartalan működéséhez, annak az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikkében foglalt, az Európai Unió Bíróságának (Bíróság) állandó ítélkezési gyakorlatával összhangban értelmezett rendelkezéseken kell alapulnia.

(12) E rendelet célja az, hogy egységes szerkezetbe foglalja és korszerűsítse a működési kockázatokra vonatkozó követelmények részét képező, az IKT-kockázatra vonatkozó követelményeket, amelyekkel eddig a különböző uniós jogi aktusokban külön foglalkoztak. Míg az említett jogi aktusok lefedték a pénzügyi kockázatok fő kategóriáit (pl. a hitelkockázatot, a piaci kockázatot, a partnerkockázatot, a likviditási kockázatot és a piaci magatartási kockázatot), elfogadásuk időpontjában nem kezelték átfogóan a digitális működési reziliencia valamennyi összetevőjét. A működési kockázatra vonatkozó szabályokat az említett uniós jogi aktusok gyakran a kockázatkezelés hagyományos kvantitatív megközelítését előnyben részesítve (nevezetesen az IKT-kockázat fedezését célzó tőkekövetelmény előírásával) fejlesztették tovább az IKT-vonatkozású eseményekhez kapcsolódó védelmi, észlelési,

([6]) 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.).

elszigetelési és helyreállítási képességekre, vagy a bejelentési és digitális tesztelési képességekre vonatkozó célzott kvalitatív szabályok helyett. Az említett jogi aktusok elsődleges célja a prudenciális felügyeletre, a piaci integritásra és a piaci magatartásra vonatkozó alapvető szabályok meghatározása és naprakésszé tétele volt.Az IKT-kockázatra vonatkozó különböző szabályok egységes szerkezetbe foglalása és korszerűsítése révén első alkalommal foglalnák következetes módon egyetlen jogalkotási aktusba a pénzügyi ágazatban rejlő digitális kockázatokra vonatkozó valamennyi rendelkezést. Ezért e rendelet egyes korábbi jogi aktusokban pótolja a hiányosságokat, vagy orvosolja a következetlenségeket, többek között az azokban használt terminológia kapcsán, és az IKT-kockázatkezelési képességekre, az események bejelentésére, a működési reziliencia tesztelésére és a harmadik féltől eredő IKT-kockázat nyomon követésére vonatkozó célzott szabályok révén kifejezetten utal az IKT-kockázatra. E rendeletnek tehát az IKT-kockázatra is fel kell hívnia a figyelmet, továbbá el kell ismernie, hogy az IKT-vonatkozású események és a működési reziliencia hiánya veszélyeztethetik a pénzügyi szervezetek megbízhatóságát.

(13) A pénzügyi szervezeteknek az IKT-kockázat kezelésekor ugyanazon megközelítést és ugyanazon elvalapú szabályokat kell alkalmazniuk, figyelembe véve méretüket és általános kockázati profiljukat, valamint szolgáltatásaik, tevékenységeik és műveleteik jellegét, nagyságrendjét és összetettségét. A következetesség hozzájárul a pénzügyi rendszerrel szembeni bizalom erősítéséhez és a rendszer stabilitásának megőrzéséhez, különösen az IKT-rendszerekre, -platformokra és -infrastruktúrákra való nagy fokú támaszkodás idején, amely megnövekedett digitális kockázattal jár. Az alapvető kiberhigiénia betartásával egyidejűleg – az IKT-zavarok hatásának és költségeinek minimalizálása révén – elkerülhetők a súlyos gazdasági áldozatok is.

(14) Egy rendelet elősegíti a szabályozás összetettségének csökkentését, előmozdítja a felügyeleti konvergenciát, és növeli a jogbiztonságot, továbbá hozzájárul a megfelelési költségek csökkentéséhez – különösen a határokon átnyúló tevékenységet végző pénzügyi szervezetek esetében – és a versenytorzulások mérsékléséhez. Ezért a pénzügyi szervezetek digitális működési rezilienciájára vonatkozó közös keret létrehozása céljából a leginkább megfelelő eszköz a rendelet, amellyel garantálható, hogy az uniós pénzügyi ágazat egységesen és koherensen alkalmazza az IKT-kockázatkezelés valamennyi összetevőjét.

(15) Az (EU) 2016/1148 európai parlamenti és tanácsi irányelv ([7]) volt a kiberbiztonságra vonatkozó első olyan, uniós szinten elfogadott horizontális keret, amely a pénzügyi szervezetek három típusára, nevezetesen a hitelintézetekre, a kereskedési helyszínekre, valamint a központi szerződő felekre is vonatkozott. Mivel azonban az (EU) 2016/1148 irányelv az alapvető szolgáltatásokat nyújtó gazdasági szereplők azonosítására nemzeti szintű mechanizmust határozott meg, csak egyes olyan hitelintézetek, kereskedési helyszínek és központi szerződő felek, amelyeket a tagállamok azonosítottak, kerültek a gyakorlatban annak hatálya alá, és így azok számára írták elő az IKT-biztonságra és események bejelentésére vonatkozóan az irányelvben megállapított követelményeknek való megfelelést. Az (EU) 2022/2555 európai parlamenti és tanácsi irányelv ([8]) egységes kritériumot ír elő annak meghatározására, hogy mely szervezetek tartoznak az irányelv hatálya alá (méretkorlát-szabály), miközben a pénzügyi szervezetek három típusát továbbra is a hatálya alatt tartja.

(16) mivel azonban ez a rendelet a digitális reziliencia különböző összetevői tekintetében fokozza a harmonizáció szintjét azáltal, hogy az IKT-kockázatkezelés és az IKT-vonatkozású események bejelentése tekintetében a pénzügyi szolgáltatásokra vonatkozó jelenlegi uniós jogban foglaltakhoz képest szigorúbb kötelezettségeket vezet be, ez a magasabb szintű harmonizáció az (EU) 2022/2555 irányelvben foglalt követelményeknél is fokozottabb harmonizációt jelent. Következésképpen ez a rendelet különös szabályt képez az (EU) 2022/2555 irányelv tekintetében. Ugyanakkor alapvető fontosságú a pénzügyi ágazat és a jelenleg az (EU) 2022/2555 irányelvben meghatározott uniós horizontális kiberbiztonsági keret közötti erős kapcsolat fenntartása ahhoz, hogy biztosított legyen a tagállamok által már elfogadott kiberbiztonsági stratégiákkal való összhang, valamint ahhoz, hogy a pénzügyi felügyeletek értesülhessenek az említett irányelv hatálya alá tartozó egyéb ágazatokat érintő kiberbiztonsági eseményekről.

([7]) 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.).

([8]) Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (lásd e Hivatalos Lap 80. oldalát).

(17) Az Európai Unióról szóló szerződés 4. cikkének (2) bekezdésével összhangban és a Bíróság által végzett bírósági felülvizsgálat sérelme nélkül, ez a rendelet nem érintheti a tagállamoknak a közbiztonságra, a védelemre és a nemzetbiztonság védelmére vonatkozó alapvető állami funkciók – például a nemzetbiztonság védelmével ellentétes információszolgáltatás – tekintetében fennálló felelősségét.

(18) Az ágazatközi tanulás lehetővé tétele, és annak érdekében, hogy eredményesen hasznosíthatók legyenek más ágazatok tapasztalatai a kiberfenyegetések kezelése terén, az (EU) 2022/2555 irányelvben említett pénzügyi szervezeteknek továbbra is az említett irányelv „ökoszisztémájának" részét kell képezniük (például az együttműködési csoport és a számítógép-biztonsági eseményekre reagáló csoportok [CSIRT-ek]). Az EFH-knak és az illetékes nemzeti hatóságoknak részt kell tudniuk venni az említett irányelv szerinti Együttműködési Csoport szakpolitikai jellegű stratégiai egyeztetéseiben és technikai tevékenységében, továbbá információt cserélni és továbbra is együttműködni az említett irányelvvel összhangban kijelölt vagy létrehozott egyedüli kapcsolattartó pontokkal. Az e rendelet szerinti illetékes hatóságoknak egyeztetniük is kell és együttműködniük a CSIRT-ekkel. Az illetékes hatóságok számára lehetővé kell tenni azt is, hogy szakvéleményt kérjenek az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságoktól, valamint hogy együttműködési megállapodásokat kössenek a hatékony és gyors reagálású koordinációs mechanizmusok biztosítása céljából.

(19) Tekintettel a pénzügyi szervezetek digitális rezilienciája és fizikai rezilienciája közötti szoros kapcsolatokra, e rendeletben és az (EU) 2022/2557 európai parlamenti és tanácsi irányelvben ([9]) koherens megközelítésre van szükség a kritikus fontosságú szervezetek rezilienciájával kapcsolatban. Mivel az e rendelet hatálya alá tartozó IKT-kockázatkezelési és bejelentési kötelezettségek révén átfogó módon kezelik a pénzügyi szervezetek fizikai rezilienciáját, az (EU) 2022/2557 irányelv III. és IV. fejezetében meghatározott kötelezettségek az említett irányelv hatálya alá tartozó pénzügyi szervezetekre nem alkalmazandók.

(20) A felhőszolgáltatók alkotják az (EU) 2022/2555 irányelv hatálya alá tartozó digitális infrastruktúra egyik kategóriáját. Az e rendelettel létrehozott uniós felvigyázási keretrendszer (a továbbiakban: felvigyázási keretrendszer) a kritikus harmadik fél IKT-szolgáltatók mindegyikére, köztük a pénzügyi szervezetek részére IKT-szolgáltatásokat nyújtó felhőszolgáltatókra is vonatkozik, és azt az (EU) 2022/2555 irányelv alapján végzett felügyelet kiegészítésének kell tekinteni. Emellett az e rendelettel létrehozott felvigyázási keretrendszernek – a digitális felügyeleti hatóságot létrehozó horizontális uniós keret hiányában – ki kell terjednie a felhőszolgáltatókra is.

(21) Az IKT-kockázat feletti teljes kontroll megőrzése érdekében a pénzügyi szervezeteknek az erőteljes és eredményes IKT-kockázatkezelést megalapozó átfogó képességekkel, továbbá valamennyi IKT-vonatkozású esemény kezelésére és a jelentős IKT-vonatkozású események bejelentésére vonatkozó konkrét mechanizmusokkal és politikákkal kell rendelkezniük. Hasonlóképpen, a pénzügyi szervezeteknek az IKT-rendszerek, -kontrollok és -folyamatok tesztelésére, valamint a harmadik féltől eredő IKT-kockázat kezelésére vonatkozó politikákkal kell rendelkezniük. A digitális működési reziliencia-alapértéket növelni kell a pénzügyi szervezetek tekintetében, lehetővé téve ugyanakkor meghatározott pénzügyi szervezetek számára, különösen a mikrovállalkozások, valamint az egyszerűsített IKT-kockázatkezelési keretrendszer hatálya alá tartozó pénzügyi szervezetek számára a követelmények arányos alkalmazását. A foglalkoztatói nyugellátást szolgáltató intézmények olyan, hatékony felügyeletének elősegítése érdekében, amely arányos, és reagál arra, hogy az illetékes hatóságokra háruló adminisztratív terheket csökkenteni kell, az ilyen pénzügyi szervezetek tekintetében a releváns nemzeti felügyeleti rendszereknek figyelembe kell venniük azok méretét és általános kockázati profilját, valamint szolgáltatásaik, tevékenységeik és műveleteik jellegét, nagyságrendjét és összetettségét, még akkor is, amikor az (EU) 2016/2341 európai parlamenti és tanácsi irányelv ([10]) 5. cikkében megállapított releváns küszöbértékek túllépésére kerül sor. Így különösen a felügyeleti tevékenységeknek azon súlyos kockázatok kezelésének szükségességére kell összpontosítaniuk, amelyek egy adott szervezet IKT-kockázatkezeléséhez társíthatók.

([9]) Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus fontosságú szervezetek rezilienciájáról és a 2008/114/EC tanácsi irányelv hatályon kívül helyezéséről (lásd e Hivatalos Lap 164. oldalát).

([10]) Az Európai Parlament és a Tanács (EU) 2016/2341 irányelve (2016. december 14.) a foglalkoztatói nyugellátást szolgáltató intézmények tevékenységéről és felügyeletéről (HL L 354., 2016.12.23., 37. o.).

Az illetékes hatóságoknak éber, de arányos megközelítést kell fenntartaniuk a foglalkoztatói nyugellátást szolgáltató olyan intézmények felügyeletével kapcsolatban is, amelyek fő tevékenységük jelentős részét – például az eszközkezelést, a biztosításmatematikai számításokat, a számvitelt és az adatgazdálkodást – az (EU) 2016/2341 irányelv 31. cikkének megfelelően – szolgáltatókhoz szervezik ki.

(22) Az IKT-vonatkozású események bejelentésének küszöbértékei és taxonómiái tagállamonként jelentősen eltérnek. Míg az (EU) 2019/881 európai parlamenti és tanácsi rendelettel ([11]) létrehozott Európai Uniós Kiberbiztonsági Ügynökség (ENISA) és az (EU) 2022/2555 irányelv szerinti Együttműködési Csoport által végzett releváns munka révén közös alap teremthető, a többi pénzügyi szervezet tekintetében a küszöbértékek meghatározása és a taxonómiák alkalmazása terén továbbra is maradhatnak vagy megjelenhetnek tagállamonként eltérő megközelítések. Az említett eltérések miatt a pénzügyi szervezeteknek többszörös követelményeknek kell megfelelniük, különösen akkor, ha több tagállamban működnek, és akkor, ha egy pénzügyi csoport részét képezik. Továbbá az ilyen eltérések potenciálisan akadályozhatják olyan további egységes vagy központosított uniós mechanizmusok létrehozását, amelyek felgyorsítják a bejelentési folyamatot, és támogatják az illetékes hatóságok közötti gyors és zavartalan információcserét, ami elengedhetetlen az IKT-kockázat kezeléséhez a kiterjedt, potenciálisan rendszerszintű következményekkel járó támadások esetén.

(23) Ahhoz, hogy csökkenteni lehessen egyes pénzügyi szervezetek adminisztratív terheit és potenciálisan duplikatív bejelentési kötelezettségeit, indokolt, hogy az (EU) 2015/2366 európai parlamenti és tanácsi irányelv ([12]) alapján fennálló esemény bejelentési követelmény többé ne legyen alkalmazandó az e rendelet hatálya alá tartozó pénzforgalmi szolgáltatókra. Következésképpen az említett irányelv 33. cikkének (1) bekezdésében hivatkozott hitelintézeteknek, elektronikuspénz-kibocsátó intézményeknek, pénzforgalmi intézményeknek és számlainformációkat összesítő szolgáltatóknak e rendelet alkalmazásának kezdőnapjától e rendelet alapján kell bejelenteniük valamennyi olyan pénzforgalmi vonatkozású működési vagy biztonsági eseményt, amelyet korábban az említett irányelv alapján jelentettek be, függetlenül attól, hogy az ilyen események IKT-vonatkozásúak-e.

(24) Annak érdekében, hogy az illetékes hatóságok az IKT-vonatkozású események jellegére, gyakoriságára, jelentőségére és hatására vonatkozó teljes áttekintés megszerzése révén képesek legyenek ellátni felügyeleti szerepüket, továbbá a releváns hatóságok, ezen belül a bűnüldöző hatóságok és a szanálási hatóságok közötti információcsere fokozása érdekében e rendeletnek olyan, az IKT-vonatkozású események bejelentésére vonatkozó szilárd rendszert kell létrehoznia, ahol a releváns követelmények kezelik a pénzügyi szolgáltatásokra vonatkozó jogszabályok jelenlegi hiányosságait, és a költségek mérséklése érdekében megszüntetnék a fennálló átfedéseket és párhuzamosságokat. Elengedhetetlen az IKT-vonatkozású események bejelentési rendszerének harmonizálása olyan módon, hogy minden pénzügyi szervezetnek az e rendeletben meghatározott egységes, egyszerűsített keretben legyen bejelentési kötelezettsége az illetékes hatósága felé. Ezenkívül az EFH-knak felhatalmazást kell kapniuk arra, hogy részletesen meghatározzák az IKT-vonatkozású események bejelentési keretének releváns elemeit, köztük a taxonómiákat, az időkereteket, az adatállományokat, a mintadokumentumokat, valamint az alkalmazandó küszöbértékeket. Az (EU) 2022/2555 irányelvvel való teljes összhang biztosítása érdekében a pénzügyi szervezetek számára lehetővé kell tenni, hogy önkéntes alapon értesíthessék a releváns illetékes hatóságot a jelentős kiberfenyegetésekről, amennyiben úgy ítélik meg, hogy a kiberfenyegetés relevanciával bír a pénzügyi rendszer, a szolgáltatást használók vagy az ügyfelek számára.

(25) Egyes pénzügyi szolgáltatási alágazatokban ugyan kidolgoztak a digitális működési reziliencia tesztelésére vonatkozó követelményeket, de olyan keretek meghatározásával, amelyeket nem minden esetben hangoltak össze teljes mértékben. Ez a határokon átnyúló tevékenységet végző pénzügyi szervezetek számára a költségek esetleges halmozódásához vezet, emellett bonyolítja a digitális működési reziliencia tesztléséből származó eredmények kölcsönös elismerését is, ami viszont a belső piac széttagolódásával járhat.

([11]) Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).

([12]) 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 az 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről (HL L 337., 2015.12.23., 35. o.).

(26) Emellett, kötelező IKT-tesztelés hiányában a sérülékenységek észlelésére nem kerül sor, ami azt eredményezi, hogy a pénzügyi szervezet IKT-kockázatnak van kitéve, és végső soron nagyobb kockázatot jelent a pénzügyi ágazat stabilitására és integritására nézve. Uniós beavatkozás nélkül a digitális működési reziliencia tesztelése továbbra sem lenne egységes, és az IKT-teszteredmények különböző joghatóságok közötti kölcsönös elismerési rendszere sem valósulna meg. Emellett, mivel valószínűleg más pénzügyi szolgáltatási alágazatok nem vezetnének be ilyen tesztelési rendszereket érdemi nagyságrendben, nem használnák ki a tesztelési keret potenciális előnyeit az IKT-sérülékenységek és kockázatok feltárása, valamint a védelmi képességek és az üzletmenet-folytonosság tesztelése tekintetében sem, ami hozzájárul az ügyfelek, a beszállítók és az üzleti partnerek bizalmának növeléséhez. Az említett átfedések, eltérések és hiányosságok kiküszöbölése céljából meg kell állapítani a koordinált tesztelési rendszerre vonatkozó szabályokat, és ezáltal megkönnyíteni a fejlett tesztelés kölcsönös elismerését az e rendeletben meghatározott kritériumoknak megfelelő pénzügyi szervezetek számára.

(27) A pénzügyi szervezeteket részben az motiválja IKT-szolgáltatások igénybevételére, hogy képesek legyenek alkalmazkodni a kialakulóban lévő versengő digitális világgazdasághoz, növeljék üzleti hatékonyságukat, és megfeleljenek a fogyasztói keresletnek. Az igénybevétel jellege és mértéke az elmúlt években folyamatosan alakult, csökkentve a pénzügyi közvetítés költségeit, lehetővé téve az üzleti tevékenység bővítését és skálázhatóságát a pénzügyi tevékenységek kiépítése során, ugyanakkor az összetett belső folyamatok kezeléséhez is hozzáférhetővé téve az IKT-eszközök széles körét.

(28) Az IKT-szolgáltatások kiterjedt felhasználását bizonyítják azon összetett szerződéses megállapodások is, amelyeknél a pénzügyi szervezetek gyakran szembesülnek nehézségekkel a rájuk vonatkozó prudenciális előírásokhoz vagy egyéb szabályozási követelményekhez igazodó szerződési feltételek kitárgyalása terén, vagy egyébként, konkrét jogosultságok – így például hozzáférési vagy audit jogosultságok – érvényesítése terén, még akkor is, ha ez utóbbiakat a szerződéses megállapodásaik rögzítik. Emellett az említett szerződéses megállapodások közül sok nem nyújt elegendő biztosítékot az alvállalkozói folyamatok teljeskörű nyomon követésére, ezáltal megfosztva a pénzügyi szervezetet azon képességétől, hogy értékelje a kapcsolódó kockázatokat. Ezenkívül, mivel a harmadik fél IKT-szolgáltatók gyakran nyújtanak szabványosított szolgáltatásokat különböző típusú ügyfeleknek, az ilyen szerződéses megállapodások nem minden esetben felelnek meg a pénzügyi ágazati szereplők egyedi vagy sajátos igényeinek.

(29) Bár a pénzügyi szolgáltatásokra vonatkozó uniós jogszabályok tartalmaznak bizonyos általános kiszervezési szabályokat, a szerződéses dimenzió nyomon követése nem épült be teljes mértékben az uniós jogba. A harmadik fél IKT-szolgáltatókkal kötött szerződéses megállapodásokra vonatkozó egyértelmű és célzott uniós előírások hiányában az IKT-kockázat külső forrásainak átfogó kezelése nem valósul meg. Következésképpen szükséges bizonyos, a pénzügyi szervezetek harmadik féltől eredő IKT-kockázatának kezelésére irányadó alapelveket rögzíteni, amelyek különös fontosságúak, amikor a pénzügyi szervezetek harmadik fél IKT-szolgáltatókat vesznek igénybe kritikus vagy lényeges funkcióik támogatása érdekében. Az említett elveket a szerződéses megállapodások teljesítésének és megszüntetésének számos elemével kapcsolatban egy sor alapvető szerződéses joggal kell kiegészíteni bizonyos minimális biztosítékok biztosítása céljából, annak érdekében, hogy erősítsék a pénzügyi szervezetek azon képességét, hogy eredményesen nyomon kövessék a harmadik fél IKT-szolgáltatók szintjén felmerülő valamennyi IKT-kockázatot. Az említett elvek kiegészítik a kiszervezésre alkalmazandó ágazati jogot.

(30) Mára nyilvánvalóvá vált a harmadik féltől eredő IKT-kockázat és a harmadik féltől való IKT-függőség nyomon követése tekintetében a homogenitás és a konvergencia bizonyos fokú hiánya. A kiszervezés kezelésére irányuló erőfeszítések így például a felhőszolgáltatókhoz történő kiszervezésről szóló 2019-es EBH-iránymutatások és a felhőszolgáltatókhoz történő kiszervezésről szóló 2021-es ESMA-iránymutatások ellenére az uniós jog nem foglalkozik elégséges módon az olyan rendszerszintű kockázat elleni fellépés tágabb kérdésével, amelyet a pénzügyi ágazatnak egy korlátozott számú kritikus harmadik fél IKT-szolgáltatóval szembeni kitettsége idézhet elő. Az uniós szintű szabályok hiányát súlyosbítja az, hogy hiányoznak az olyan felhatalmazásra és eszközökre vonatkozó nemzeti szabályok, amelyek lehetővé tennék a pénzügyi felügyeletek számára, hogy behatóan megismerhessék a harmadik féltől való IKT-függőségeket, és megfelelően nyomon követhessék a harmadik féltől való IKT-függőségek koncentrációjából eredő kockázatokat.

(31) Figyelembe véve a kiszervezés egyre elterjedtebb gyakorlatával és a harmadik fél IKT-szolgáltatók koncentrációjával járó potenciális rendszerszintű kockázatokat, továbbá szem előtt tartva az olyan nemzeti mechanizmusok elégtelenségét, amelyek megfelelő eszközöket bocsátanának a pénzügyi felügyeletek rendelkezésére a kritikus harmadik fél IKT-szolgáltatóknál felmerülő IKT-kockázat mennyiségi és minőségi értékeléséhez, valamint hatásaik elhárításához, megfelelő felvigyázási keretrendszert szükséges létrehozni, amely lehetővé teszi azon harmadik fél IKT-szolgáltatók tevékenységének folyamatos nyomon követését, amelyek pénzügyi szervezetek kritikus harmadik fél IKT-szolgáltatói, miközben biztosítja a pénzügyi szervezetektől eltérő ügyfelek bizalmas kezelésének és biztonságának megőrzését. Miközben az IKT-szolgáltatások csoporton belüli nyújtása sajátos kockázatokkal és előnyökkel jár, nem tekinthető automatikusan kevésbé kockázatosnak, mint az IKT-szolgáltatások pénzügyi csoporton kívüli szolgáltatók általi nyújtása, és ezért ugyanazon szabályozási keret hatálya alá kell tartoznia. Azonban amennyiben az IKT-szolgáltatásokat ugyanazon pénzügyi csoporton belül nyújtják, a pénzügyi szervezetek magasabb szintű kontrollt gyakorolhatnak a csoporton belüli szolgáltatók felett, amit az általános kockázatértékelés során figyelembe kell venni.

(32) Amint az IKT-kockázat egyre összetettebbé és fejlettebbé válik, az IKT-kockázat észlelésére és megelőzésére irányuló megfelelő intézkedések nagymértékben függenek a fenyegetéssel és sérülékenységgel kapcsolatos hírszerzés pénzügyi szervezetek közötti rendszeres megosztásától. Az információk megosztása hozzájárul a kiberfenyegetésekkel kapcsolatos fokozott tudatosság megteremtéséhez. Ez viszont javítja a pénzügyi szervezetek képességét annak megelőzésére, hogy a kiberfenyegetésekből valóban IKT-vonatkozású események váljanak, emellett lehetővé teszi a pénzügyi szervezetek számára az IKT-vonatkozású események hatásainak eredményesebb elszigetelését, továbbá a gyorsabb helyreállítást. Uniós szintű iránymutatás hiányában az eddigiek során a jelek szerint több tényező is gátolta az ilyen hírszerzés-megosztást, különösen az adatvédelmi, trösztellenes és felelősségi szabályokkal való összeegyeztethetőséggel kapcsolatos bizonytalanság.

(33) Emellett a hasznos információk visszatartásához vezetnek az olyan típusú információkkal kapcsolatos kétségek, amelyek megoszthatók más piaci szereplőkkel vagy nem felügyeleti hatóságokkal (így például elemzési input céljából az ENISA-val, vagy bűnüldözési célból az Europollal). Ezért az információmegosztás terjedelme és minősége továbbra is korlátozott és széttagolt, a releváns információk átadására többnyire helyi szinten (nemzeti kezdeményezések útján) kerül sor, és nincsenek az integrált pénzügyi rendszer igényeihez igazodó, egységes uniós szintű információmegosztási megállapodások. Ezért fontos megerősíteni az említett kommunikációs csatornákat.

(34) A pénzügyi szervezeteket ösztönözni kell arra, hogy – információmegosztási megállapodásokban való részvétel révén – kiberfenyegetettségi információkat és hírszerzést osszanak meg egymással, és hogy stratégiai, taktikai és operatív szinten is együttesen használják ki az egyes szervezeteknél meglévő ismereteket és gyakorlati tapasztalatokat annak érdekében, hogy növeljék képességüket a kiberfenyegetések megfelelő értékelésére, nyomon követésére, kivédésére és az arra való reagálásra. Ezért lehetővé kell tenni az önkéntes információmegosztási megállapodások mechanizmusainak uniós szintű megjelenését, mivel a megbízható környezetben átadott információk segítségével a pénzügyi szolgáltatási ágazat közössége megelőzhetné a kiberfenyegetéseket és együttesen háríthatná el azokat az IKT-kockázat terjedésének gyors lehatárolásával, valamint a pénzügyi csatornákon keresztüli esetleges átterjedés megakadályozásával. Az említett mechanizmusoknak meg kell felelniük az „Iránymutatás az Európai Unió működéséről szóló szerződés 101. cikkének a horizontális együttműködési megállapodásokra való alkalmazhatóságáról” című, 2011. január 14-i bizottsági közleményben meghatározott uniós alkalmazandó versenyjogi szabályoknak, valamint az uniós adatvédelmi szabályoknak, különösen az (EU) 2016/679 európai parlamenti és tanácsi rendeletnek ([13]). Működésüknek az említett rendelet 6. cikkében foglalt egy vagy több jogalap használatán kell alapulnia, így például a személyes adatok olyan kezelésével összefüggésben, amely az említett rendelet 6. cikke (1) bekezdésének f) pontjában említettek szerint az adatkezelő vagy valamely harmadik fél jogos érdekének céljából szükséges, valamint a személyes adatok olyan kezelésével összefüggésben is, amely az említett rendelet 6. cikke (1) bekezdésének c), illetve e) pontjában említettek szerint szükséges az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez, illetve szükséges valamely közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtásához.

([13]) 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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

(35) Annak érdekében, hogy a teljes pénzügyi ágazat magas szintű digitális működési rezilienciával rendelkezzen, ugyanakkor lépést tartson a technológiai fejlődéssel, e rendeletnek az IKT-szolgáltatások valamennyi típusából eredő kockázatokkal foglalkoznia kell. E célból az IKT-szolgáltatások fogalommeghatározását e rendelet összefüggésében tágan kell értelmezni, úgy, hogy az magában foglalja az IKT-rendszer útján egy vagy több belső vagy külső felhasználó részére folyamatosan nyújtott digitális és adatszolgáltatásokat. Az említett fogalommeghatározásnak például magában kell foglalnia az – elektronikus hírközlési szolgáltatások kategóriájába tartozó – úgynevezett „over-the-top" szolgáltatásokat is. A fogalommeghatározásból kizárólag a közcélú kapcsolt távbeszélő-hálózati szolgáltatásoknak, vezetékes szolgáltatásoknak, hagyományos telefonszolgáltatásoknak vagy vezetékes telefonszolgáltatásoknak minősülő, hagyományos analóg telefonszolgáltatások korlátozott kategóriáját kell kizárni.

(36) Az e rendeletben tervezett kiterjedt hatály ellenére a digitális működési rezilienciára vonatkozó szabályok alkalmazásakor figyelembe kell venni a pénzügyi szervezetek között a méretük és az általános kockázati profiljuk tekintetében fennálló jelentős különbségeket. Általános elvként az IKT-kockázatkezelési keretrendszer végrehajtására szánt erőforrások és képességek felosztásakor a pénzügyi szervezeteknek megfelelő egyensúlyt kell teremteniük IKT-szükségleteik, valamint méretük és általános kockázati profiljuk, továbbá szolgáltatásaik, tevékenységeik és műveleteik jellege, nagyságrendje és összetettsége között, míg az illetékes hatóságoknak folytatniuk kell az ilyen felosztási megközelítés értékelését és felülvizsgálatát.

(37) Az (EU) 2015/2366 irányelv 33. cikkének (1) bekezdésében említett, számlainformációkat összesítő szolgáltatók – figyelembe véve tevékenységeik sajátos jellegét és az azokból eredő kockázatokat – kifejezetten e rendelet hatálya alá tartoznak. Emellett a 2009/110/EK európai parlamenti és tanácsi irányelv ([14]) 9. cikkének (1) bekezdése és az (EU) 2015/2366 irányelv 32. cikkének (1) bekezdése alapján mentesített elektronikuspénz-kibocsátó intézmények és pénzforgalmi intézmények is e rendelet hatálya alá tartoznak, még akkor is, ha nem kaptak a 2009/110/EK irányelvnek megfelelően engedélyt elektronikus pénz kibocsátására, vagy ha nem kaptak az (EU) 2015/2366 irányelvnek megfelelően engedélyt pénzforgalmi szolgáltatások nyújtására és teljesítésére. Azonban a 2013/36/EU európai parlamenti és tanácsi ([15]) irányelv 2. cikke (5) bekezdésének 3. pontjában említett postai elszámolóközpontok ki vannak zárva e rendelet hatálya alól. Az (EU) 2015/2366 irányelv alapján mentesített pénzforgalmi intézmények, a 2009/110/EK irányelv alapján mentesített elektronikuspénz-kibocsátó intézmények és az (EU) 2015/2366 irányelv 33. cikkének (1) bekezdésében említett, számlainformációkat összesítő szolgáltatók illetékes hatósága az (EU) 2015/2366 irányelv 22. cikkével összhangban kijelölt illetékes hatóság.

(38) mivel a nagyobb pénzügyi szervezeteknek az erőforrások szélesebb köre állhat a rendelkezésére, és gyorsabban mozgósíthatnak forrásokat irányítási struktúrák kialakítására és különféle vállalati stratégiák kidolgozására, csak az e rendelet értelmében vett mikrovállalkozásnak nem minősülő pénzügyi szervezetek számára kell kötelezővé tenni az összetettebb irányítási rendszerek kidolgozását. Az ilyen szervezetek jobban képesek különösen arra, hogy célzott vezetői funkciókat alakítsanak ki a harmadik fél IKT-szolgáltatókkal kötött megállapodások felügyelete vagy a válságkezelés céljából, hogy a három védelmi vonalra épülő modell szerint szervezzék meg IKT-kockázatkezelésüket, vagy hogy kialakítsanak egy belső kockázatkezelési és kontrollmodellt, és hogy az IKT-kockázatkezelési keretrendszerüket belső auditoknak vessék alá.

(39) Egyes pénzügyi szervezetek mentességeket élveznek, vagy a releváns ágazatspecifikus uniós jogszabályok alapján nagyon enyhe szabályozási keret hatálya alá tartoznak. Az említett pénzügyi szervezetek közé tartoznak a 2011/61/EU európai parlamenti és tanácsi irányelv ([16]) 3. cikkének (2) bekezdésében említett alternatívbefektetésialap-kezelők, a 2009/138/EK európai parlamenti és tanácsi irányelv ([17]) 4. cikkében említett biztosítók és viszontbiztosítók, valamint azon foglalkoztatói nyugellátást szolgáltató intézmények, amelyek összesen legfeljebb 15 taggal rendelkező nyugdíjrendszereket működtetnek. E mentességek fényében nem lenne arányos az ilyen

([14]) Az Európai Parlament és a Tanács 2009/110/EK irányelve (2009. szeptember 16.) az elektronikuspénz-kibocsátó intézmények tevékenységének megkezdéséről, folytatásáról és prudenciális felügyeletéről, a 2005/60/EK és a 2006/48/EK irányelv módosításáról, valamint a 2000/46/EK irányelv hatályon kívül helyezéséről (HL L 267., 2009.10.10., 7. o.).

([15]) Az Európai Parlament és a Tanács 2013/36/EU irányelve (2013. június 26.) a hitelintézetek tevékenységéhez való hozzáférésről és a hitelintézetek prudenciális felügyeletéről, a 2002/87/EK irányelv módosításáról, a 2006/48/EK és a 2006/49/EK irányelv hatályon kívül helyezéséről (HL L 176., 2013.6.27., 338. o.).

([16]) Az Európai Parlament és a Tanács 2011/61/EU irányelve (2011. június 8.) az alternatívbefektetésialap-kezelőkről, valamint a 2003/41/EK és a 2009/65/EK irányelv, továbbá az 1060/2009/EK és az 1095/2010/EU rendelet módosításáról (HL L 174., 2011.7.1., 1. o.).

([17]) Az Európai Parlament és a Tanács 2009/138/EK irányelve (2009. november 25.) a biztosítási és viszontbiztosítási üzleti tevékenység megkezdéséről és gyakorlásáról (Szolvencia II) (HL L 335., 2009.12.17., 1. o.).

pénzügyi szervezeteket e rendelet hatálya alá vonni. Emellett ez a rendelet elismeri a biztosításközvetítési piac szerkezetének sajátosságait, így a mikrovállalkozásnak vagy kis- vagy középvállalkozásnak minősülő biztosítás-közvetítők, viszontbiztosítás-közvetítők és kiegészítő biztosításközvetítői tevékenységet végző személyek nem tartozhatnak e rendelet hatálya alá.

(40) mivel a 2013/36/EU irányelv 2. cikke (5) bekezdésének 4–23. pontjában említett jogalanyok nem tartoznak az említett irányelv hatálya alá, a tagállamok számára következésképpen lehetővé kell tenni annak eldöntését, hogy mentesítik-e e rendelet alkalmazása alól a saját területükön működő ilyen jogalanyokat.

(41) Hasonlóképpen, e rendeletnek a 2014/65/EU európai parlamenti és tanácsi irányelv ([18]) hatályához való hozzáigazítása érdekében helyénvaló kizárni e rendelet hatálya alól az említett irányelv 2. és 3. cikkében említett azon természetes és jogi személyeket is, akik vagy amelyek anélkül jogosultak befektetési szolgáltatások nyújtására, hogy a 2014/65/EU irányelv szerinti engedélyt meg kellene szerezniük. Azonban a 2014/65/EU irányelv 2. cikke azon szervezeteket – így a központi értéktárakat, a kollektív befektetési vállalkozásokat, vagy a biztosítókat és viszontbiztosítókat – is kizárja az irányelv hatálya alól, amelyek e rendelet alkalmazásában pénzügyi szervezetnek minősülnek. Az említett irányelv 2. és 3. cikkében említett személyek és szervezetek e rendelet hatálya alóli kizárása nem terjedhet ki az említett központi értéktárakra, kollektív befektetési vállalkozásokra, vagy biztosítókra és viszontbiztosítókra.

(42) Az ágazatspecifikus uniós jogszabályok értelmében egyes pénzügyi szervezetekre – a méretükkel vagy az általuk nyújtott szolgáltatásokkal összefüggő okokból – enyhébb követelmények vagy mentességek vonatkoznak. A pénzügyi szervezetek említett kategóriája magában foglalja a kis méretű és össze nem kapcsolt befektetési vállalkozásokat, az olyan, kis méretű foglalkoztatói nyugellátást szolgáltató intézményeket, amelyeket az érintett tagállam az (EU) 2016/2341 irányelv 5. cikkében meghatározott feltételek mellett kizárhat az említett irányelv hatálya alól, és amelyek összesen legfeljebb 100 taggal rendelkező nyugdíjrendszereket működtetnek, továbbá a 2013/36/EU irányelv szerint mentesített intézményeket. Ezért az arányosság elvével összhangban és az ágazatspecifikus uniós jogszabályok szellemének megőrzése érdekében helyénvaló az említett pénzügyi szervezeteket is az e rendelet szerinti egyszerűsített IKT-kockázatkezelési keretrendszer hatálya alá vonni. Az EFH-k által kidolgozandó szabályozástechnikai standardok nem módosíthatják az említett pénzügyi szervezetekre vonatkozó IKT-kockázatkezelési keretrendszer arányos jellegét. Ezenkívül, az arányosság elvével összhangban helyénvaló az (EU) 2015/2366 irányelv 32. cikkének (1) bekezdésében említett azon pénzforgalmi intézményeket és a 2009/110/EK irányelv 9. cikkében említett azon elektronikuspénz-kibocsátó intézményeket, amelyeket az említett uniós jogi aktusokat átültető nemzeti joggal összhangban mentesítettek, ugyancsak az e rendelet szerinti egyszerűsített IKT-kockázatkezelési keretrendszer hatálya alá vonni, míg azon pénzforgalmi intézményeknek és elektronikuspénz-kibocsátó intézményeknek, amelyekre az ágazati uniós jogot átültető nemzeti joggal összhangban nem vonatkozik mentesség, az e rendeletben meghatározott általános keretnek kell megfelelniük.

(43) Hasonlóképpen, a mikrovállalkozásnak minősülő, vagy az e rendelet szerinti egyszerűsített IKT-kockázatkezelési keretrendszer hatálya alá tartozó pénzügyi szervezetektől nem követelhető meg, hogy létrehozzanak egy feladatkört a harmadik fél IKT-szolgáltatókkal az IKT-szolgáltatások igénybevételéről kötött megállapodásaik nyomon követésére; vagy hogy kinevezzék a felső vezetés egy tagját a kapcsolódó kockázati kitettség és a releváns dokumentáció felvigyázásáért felelős személyként; hogy az IKT-kockázat kezelésére és felvigyázására vonatkozó felelősséget egy kontrollfunkcióra ruházzák, és az összeférhetetlenségek elkerülése érdekében biztosítsák az ilyen kontrollfunkció megfelelő függetlenségét; hogy dokumentálják és legalább évente egyszer felülvizsgálják az IKT-kockázatkezelési keretrendszert; hogy rendszeresen belső auditnak vessék alá az IKT-kockázatkezelési keretrendszert; hogy a hálózati és információsrendszer-infrastruktúrájában és folyamataiban bekövetkezett jelentős változásokat követően beható értékeléseket végezzenek; hogy rendszeresen elvégezzék az elavult IKT-rendszerek kockázatelemzését; hogy az IKT-reagálási és -helyreállítási tervek végrehajtását független belső audit felülvizsgálatoknak vessék alá; hogy válságkezelési funkcióval rendelkezzenek; hogy kiterjesszék az üzletmenet-folytonossági, reagálási és helyreállítási tervek tesztelését az elsődleges IKT-infrastruktúra és a tartalékeszközök közötti átállási forgatókönyvekre; hogy beszámoljanak az illetékes hatóságoknak – azok kérésére – a jelentős IKT-vonatkozású

([18]) Az Európai Parlament és a Tanács 2014/65/EU irányelve (2014. május 15.) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról (HL L 173., 2014.6.12., 349. o.).

eseményekből eredő összesített becsült éves költségekről és veszteségekről; hogy fenntartsák az IKT-tartalékkapacitásokat; hogy tájékoztassák az illetékes nemzeti hatóságokat az IKT-vonatkozású események utólagos felülvizsgálatát követően végrehajtott változtatásokról; hogy folyamatosan nyomon kövessék a releváns technológiai fejlesztéseket; hogy átfogó programot alakítsanak ki a digitális működési reziliencia tesztelésére az e rendeletben előírt IKT-kockázatkezelési keretrendszer integráns részeként; vagy hogy fogadjanak el a harmadik féltől eredő IKT-kockázatra vonatkozó stratégiát, és azt rendszeresen vizsgálják felül.Ezenkívül a mikrovállalkozásoknak a kockázati profiljukat alapul véve csak azt kell mérlegelniük, hogy szükséges-e ilyen IKT-tartalékkapacitásokat fenntartaniuk. A mikrovállalkozások számára a digitális működési reziliencia tesztelését szolgáló programok tekintetében rugalmasabb rendszert kell biztosítani. Amikor mérlegelik az elvégzendő tesztelés típusát és gyakoriságát, a mikrovállalkozásoknak megfelelő egyensúlyra kell törekedniük a magas szintű digitális működési reziliencia fenntartására irányuló célkitűzés, a rendelkezésre álló erőforrások és az általános kockázati profiljuk között. A mikrovállalkozásokat és az e rendelet szerinti egyszerűsített IKT-kockázatkezelési keretrendszer hatálya alá tartozó pénzügyi szervezeteket mentesíteni kell azon követelmény alól, hogy elvégezzék az IKT-eszközök, -rendszerek és -folyamatok olyan fejlett tesztelését, amely fenyegetés alapú behatolási tesztelésen (TLPT, threat-led penetration testing) alapul, mivel az ilyen tesztelés elvégzése csak az e rendeletben meghatározott kritériumoknak megfelelő pénzügyi szervezetek számára írható elő. Korlátozott képességeikre tekintettel, a mikrovállalkozások számára lehetővé kell tenni, hogy a harmadik fél IKT-szolgáltatóval megállapodjanak arról, hogy a pénzügyi szervezet hozzáférési, ellenőrzési és audit jogát átruházzák egy, a harmadik fél IKT-szolgáltató által kinevezendő független harmadik félre, feltéve, hogy a pénzügyi szervezet bármikor tájékoztatást és bizonyosságot kérhet a vonatkozó független harmadik féltől a harmadik fél IKT-szolgáltató teljesítményéről.

(44) mivel a fenyegetés alapú behatolási tesztelést csak a digitális működési reziliencia fejlett tesztelése céljából azonosított pénzügyi szervezetek számára kell előírni, az ilyen tesztek lefolytatásával járó igazgatási folyamatok és pénzügyi költségek terhét a pénzügyi szervezetek kis hányada kell, hogy viselje.

(45) A pénzügyi szervezeteknél egyfelől az üzleti stratégiák, és másfelől az IKT-kockázatkezelés teljeskörű összehangolása és általános összhangja érdekében a pénzügyi szervezetek vezető testületei számára elő kell írni, hogy vállaljanak lényeges és tevékeny szerepet az IKT-kockázatkezelési keretrendszer, valamint a digitális működési rezilienciára vonatkozó általános stratégia irányításában és alakításában. A vezető testületek által alkalmazandó megközelítésnek nem elegendő az IKT-rendszerek rezilienciáját biztosító eszközökre összpontosítania, hanem ki kell terjednie a személyekre és a folyamatokra is olyan szabályzatok útján, amelyek a vállalati struktúra minden rétegében, a személyzet valamennyi tagjára vonatkozóan hangsúlyozzák a kiberkockázatok erőteljes tudatosítását és a szigorú kiberhigiéniás normák betartása melletti elkötelezettséget. A pénzügyi szervezet IKT-kockázatának kezeléséért a vezető testületet terhelő végső felelősségnek egy olyan, az említett átfogó megközelítés részét képező általános elvnek kell lennie, amelynek az IKT-kockázatkezelés nyomon követésének kontrolljában való folyamatos vezető testületi részvétel formájában kell megnyilvánulnia.

(46) Ezenfelül a pénzügyi szervezet IKT-kockázatának kezeléséért a vezető testület által vállalt teljeskörű és végső felelősség elve együtt jár azzal, hogy olyan szinten kell biztosítani az IKT-vonatkozású beruházások és az általános költségvetés szintjét, amely képessé tenné a pénzügyi szervezetet a magas szintű digitális működési reziliencia megvalósítására.

(47) A releváns nemzetközi, nemzeti és ágazati legjobb gyakorlatokra, iránymutatásokra, ajánlásokra, valamint kiberkockázat-kezelési megközelítésekre építő rendelet olyan elveket mozdít elő, amelyek megkönnyítik az IKT-kockázatkezelés általános strukturálását. Következésképpen, mindaddig, amíg a pénzügyi szervezetek által bevezetett fő képességek kezelik az IKT-kockázatkezelés e rendeletben meghatározott különböző funkcióit (azonosítás, védelem és megelőzés, felderítés, reagálás és helyreállítás, tanulás és alkalmazkodás, valamint kommunikáció), a pénzügyi szervezeteknek szabadon kell tudniuk alkalmazni az eltérő keretek között vagy kategóriák mentén kidolgozott IKT-kockázatkezelési modelleket.

(48) Ahhoz, hogy lépést tarthassanak a kiberfenyegetettségi helyzet alakulásával, a pénzügyi szervezeteknek naprakész IKT-rendszereket kell fenntartaniuk, amelyek megbízhatóak, és képesek nemcsak garantálni a szolgáltatásaikhoz szükséges adatfeldolgozást, hanem biztosítani elegendő technológiai rezilienciát is, hogy lehetővé váljon számukra a piaci stresszhelyzet vagy egyéb kedvezőtlen helyzetek miatti további adatfeldolgozási igények megfelelő kezelése.

(49) Hatékony üzletmenet-folytonossági és helyreállítási tervekre van szükség ahhoz, hogy a pénzügyi szervezetek – összhangban biztonsági mentési szabályzatukkal – az IKT-vonatkozású eseményeket, különösen a kibertámadásokat haladéktalanul és gyorsan, a kár mérséklésével, a tevékenység újraindítását és a helyreállítási intézkedéseket előtérbe helyezve oldhassák meg. Azonban a tevékenység ilyen újraindítása semmilyen módon nem veszélyeztetheti a hálózati és információs rendszerek integritását és biztonságát, vagy az adatok rendelkezésre állását, hitelességét, integritását vagy bizalmas jellegét.

(50) Míg e rendelet lehetővé teszi a pénzügyi szervezetek számára, hogy a helyreállítási időre és a helyreállítási pontra vonatkozó célkitűzéseiket rugalmasan határozzák meg, és így az ilyen célkitűzéseket a releváns funkciók jellegének és kritikusságának, valamint a vonatkozó üzleti igényeknek a maradéktalan figyelembevételével határozzák meg, mindazonáltal elő kell írni számukra, hogy az ilyen célkitűzések meghatározásakor végezzék el a piaci hatékonyságra gyakorolt potenciális általános hatás értékelését.

(51) A kibertámadások terjesztői hajlamosak arra, hogy közvetlenül a forrásnál próbáljanak anyagi haszonra szert tenni, jelentős következményeknek téve így ki a pénzügyi szervezeteket. Annak megelőzése érdekében, hogy az IKT-rendszerek elveszítsék integritásukat, vagy elérhetetlenné váljanak, és így az adatvédelmi incidensek vagy a fizikai IKT-infrastruktúrában keletkező kár elkerülése érdekében számottevő mértékben javítani és észszerűsíteni kell a jelentős IKT-vonatkozású események pénzügyi szervezetek általi bejelentését. Az IKT-vonatkozású események bejelentését harmonizálni kell egy olyan kötelezettség bevezetése révén, amelynek értelmében minden pénzügyi szervezetnek közvetlenül a releváns illetékes hatósága felé kell bejelentést tennie. Amennyiben egy pénzügyi szervezet egynél több illetékes nemzeti hatóság felügyelete alá tartozik, a tagállamoknak egyetlen illetékes hatóságot kell megjelölniük az említett bejelentés címzettjeként. Az 1024/2013/EU tanácsi rendelet ([19]) 6. cikkének (4) bekezdése szerint jelentősnek minősített hitelintézeteknek az említett bejelentést az illetékes nemzeti hatóságok felé kell megtenniük, amelyeknek ezt követően továbbítaniuk kell a bejelentést az Európai Központi Banknak (EKB).

(52) A közvetlen bejelentés várhatóan lehetővé teszi a pénzügyi felügyeletek számára, hogy azonnal hozzáférjenek a jelentős IKT-vonatkozású eseményekkel kapcsolatos információkhoz. A pénzügyi felügyeleteknek viszont továbbítaniuk kell a jelentős IKT-vonatkozású események részleteit a nem pénzügyi állami hatóságok (így például az (EU) 2022/2555 irányelv szerinti illetékes hatóságok és egyedüli kapcsolattartó pontok, a nemzeti adatvédelmi hatóságok, valamint a bűncselekmény jellegű jelentős IKT-vonatkozású események kapcsán a bűnüldöző hatóságok) részére annak érdekében, hogy fokozzák az ilyen hatóságoknak az ilyen biztonsági eseményekkel kapcsolatos ismereteit, és a CSIRT-ek esetében megkönnyítsék az azonnali segítségnyújtást, amely adott esetben a pénzügyi szervezetek számára adható. Ezenfelül a tagállamok számára lehetővé kell tenni, hogy úgy határozzanak, hogy a pénzügyi szervezeteknek maguknak kelljen ilyen információkat a pénzügyi szolgáltatások területén kívül működő hatóságok rendelkezésére bocsátani. Az említett információáramlásoknak lehetővé kell tenniük a pénzügyi szervezetek számára, hogy gyorsan profitáljanak bármely releváns technikai inputból, a korrekciós intézkedésekre vonatkozó tanácsadásból, és az ilyen hatóságok későbbi utókövetéséből. A jelentős IKT-vonatkozású eseményekkel kapcsolatos információk áramlásának kétirányúnak kell lennie: a pénzügyi felügyeleteknek meg kell adniuk a szükséges visszajelzést és iránymutatást a pénzügyi szervezet részére, ugyanakkor az EFH-knak – a szélesebb körű kollektív védelem érdekében – meg kell osztaniuk a valamely eseményhez kapcsolódó kiberfenyegetésekre és sérülékenységekre vonatkozó anonimizált adatokat.

(53) Miközben az események bejelentését valamennyi pénzügyi szervezet számára elő kell írni, az említett követelmény várhatóan nem érinti valamennyit azonos módon. Valóban, a releváns lényegességi küszöbértékeket és a bejelentés ütemezését az EFH-k által kidolgozandó szabályozástechnikai standardokon alapuló, felhatalmazáson alapuló jogi aktusok keretében megfelelően ki kell igazítani annak érdekében, hogy azok csak a jelentős IKT-vonatkozású eseményekre vonatkozzanak. Emellett a bejelentési kötelezettségek ütemezésének meghatározásakor a pénzügyi szervezetek sajátosságait is figyelembe kell venni.

(54) E rendeletnek elő kell írnia a hitelintézetek, a pénzforgalmi intézmények, a számlainformációkat összesítő szolgáltatók és az elektronikuspénz-kibocsátó intézmények számára, hogy valamennyi – korábban az (EU) 2015/2366 irányelv alapján bejelentett – pénzforgalmi vonatkozású működési vagy biztonsági eseményt bejelentsék, függetlenül a zavar vagy az esemény IKT-jellegétől.

([19]) 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.).

(55) Az EFH-kat meg kell bízni azzal, hogy értékeljék az IKT-vonatkozású események bejelentése uniós szintű lehetséges központosításának megvalósíthatóságát és feltételeit. Az ilyen központosítás jelentheti egy olyan, a jelentős IKT-vonatkozású események bejelentésére szolgáló egységes uniós adatbázis létrehozását, amely vagy közvetlenül fogadná a vonatkozó bejelentéseket és automatikusan értesítené az illetékes nemzeti hatóságokat, vagy mindössze az illetékes nemzeti hatóságok által továbbított releváns bejelentéseket fogná össze, és ezáltal koordinációs szerepet látna el. Az EFH-kat meg kell bízni azzal, hogy – az EKB-val és az ENISA-val egyeztetve – készítsenek közös jelentést, amelyben megvizsgálják egy egységes európai uniós adatbázis létrehozásának megvalósíthatóságát.

(56) A magas szintű digitális működési reziliencia megvalósításához, valamint összhangban mind a releváns nemzetközi szabványokkal (pl. G7: A fenyegetés alapú behatolási tesztelés alapelemei), mind az Unióban alkalmazott olyan keretekkel, mint a TIBER-EU, a pénzügyi szervezeteknek rendszeresen tesztelniük kell az IKT-rendszereik és az IKT-vonatkozású feladatokat ellátó munkatársaik megelőzési, felderítési, reagálási és helyreállítási képességeinek hatékonyságát, hogy feltárhassák és kezelhessék a potenciális IKT-sérülékenységeket. Ahhoz, hogy figyelembe lehessen venni a különböző pénzügyi szolgáltatási alágazatok között és azokon belül az egyes pénzügyi szervezetek kiberbiztonsági felkészültsége tekintetében fennálló különbségeket, a tesztelésnek az eszközök és műveletek széles skáláját kell felölelnie, az alapvető követelmények felmérésétől kezdve (pl. sérülékenységi értékelések és vizsgálatok, nyílt forrású elemzések, hálózatbiztonsági értékelések, hiányelemzések, fizikai biztonsági felülvizsgálatok, kérdőívek és szoftveres megoldások vizsgálata, lehetőség szerint forráskódvizsgálatok, forgatókönyv-alapú tesztek, kompatibilitás-vizsgálat, teljesítmény-vizsgálat vagy végpontok közötti tesztek) egészen a TLPT útján végzett fejlettebb tesztelésig. Az ilyen fejlett tesztelést csak azon pénzügyi szervezetek esetében kell előírni, amelyek IKT-szempontból kellően érettek ahhoz, hogy képesek legyen megfelelően elvégezni azokat. A digitális működési reziliencia e rendelettel előírt tesztelésének tehát azon pénzügyi szervezetek esetében, amelyek teljesítik az e rendeletben meghatározott kritériumokat (például nagy rendszerszintű jelentőséggel bíró és IKT-érett hitelintézetek, értéktőzsdék, központi értéktárak és központi szerződő felek), más pénzügyi szervezetekhez képest szigorúbbnak kell lennie. Ugyanakkor, a digitális működési reziliencia TLPT útján történő tesztelésének az alapvető pénzügyi szolgáltatási alágazatokban (például pénzforgalom, banki tevékenység, elszámolás és kiegyenlítés) működő és rendszerszintű szerepet betöltő pénzügyi szervezetek esetében nagyobb, és más alágazatok (például eszközkezelők és hitelminősítő intézetek) esetében kisebb relevanciával kell bírnia.

(57) A határokon átnyúló tevékenységet végző és az Unióban a letelepedés vagy a szolgáltatásnyújtás szabadságát gyakorló pénzügyi szervezeteknek a székhelyük szerinti tagállamban egy egységes, fejlett tesztelési követelményrendszernek (azaz TLPT) kell megfelelniük, amelynek magában kell foglalnia az IKT-infrastruktúrákat valamennyi olyan joghatóságban, ahol a határokon átnyúló tevékenységet végző pénzügyi csoport működik az Unión belül, ily módon lehetővé téve az ilyen pénzügyi csoportok számára, hogy csak egy joghatóságban keletkezzenek kapcsolódó IKT-tesztköltségeik.

(58) Annak érdekében, hogy az egyes illetékes hatóságok korábban – mindenekelőtt a TIBER-EU keret végrehajtása tekintetében – megszerzett szakértelmét fel lehessen használni, e rendeletnek lehetővé kell tennie a tagállamok számára, hogy egyetlen hatóságot jelöljenek ki, amely nemzeti szinten a pénzügyi ágazatban valamennyi TLPT-vonatkozású ügyért felel, vagy – ilyen kijelölés hiányában – az illetékes hatóságok számára lehetővé kell tenni, hogy a TLPT-vonatkozású feladatok ellátását egy másik, pénzügyi területen működő illetékes nemzeti hatóságra ruházzák át.

(59) mivel e rendelet nem írja elő a pénzügyi szervezetek számára, hogy egyetlen fenyegetés alapú behatolási tesztelés minden kritikus vagy fontos funkcióra kiterjedjen, a pénzügyi szervezetek szabadon határozhatják meg, hogy mely és mennyi kritikus vagy fontos funkcióra terjedjen ki az ilyen teszt hatálya.

(60) Az e rendelet értelmében vett csoportos tesztelés – amely egy TLPT-ben több pénzügyi szervezet részvételét jelenti, és amelyre vonatkozóan egy harmadik fél IKT-szolgáltató közvetlenül szerződéses megállapodást köthet egy külső tesztelővel – csak akkor engedélyezhető, amennyiben a harmadik fél IKT-szolgáltató által az olyan ügyfelek, amelyek az e rendelet hatályán kívül eső szervezetek, részére nyújtott szolgáltatások minőségét vagy biztonságát, vagy az ilyen szolgáltatásokhoz kapcsolódó adatok bizalmas jellegét észszerűen várható módon káros hatás éri. A csoportos tesztelésre biztosítékoknak is kell vonatkozniuk (egyetlen kijelölt pénzügyi szervezet általi irányítás, a részt vevő pénzügyi szervezetek számának kalibrálása) annak érdekében, hogy – a TLPT e rendelet szerinti célkitűzéseinek megfelelő – szigorú tesztelési gyakorlatot biztosítsanak a részt vevő pénzügyi szervezetek számára.

(61) A vállalati szinten rendelkezésre álló belső erőforrások kihasználása érdekében e rendeletnek lehetővé kell tennie belső tesztelők igénybevételét a TLPT lefolytatása céljából, feltéve, hogy van felügyeleti jóváhagyás, nincsenek összeférhetetlenségek, és fennáll a belső és külső tesztelők rendszeres időközönkénti váltakozása (minden harmadik tesztet követően), előírva ugyanakkor azt is, hogy a TLPT során a fenyegetettséggel kapcsolatos hírszerzés szolgáltatójának minden esetben a pénzügyi szervezeten kívüli vállalkozásnak kell lennie. A TLPT elvégzésével kapcsolatos felelősségnek teljes mértékben a pénzügyi szervezetnél kell maradnia. A hatóságok által kiállított tanúsítványoknak kizárólag a kölcsönös elismerés célját kell szolgálniuk, továbbá azok nem zárhatnak ki semmi olyan IKT-kockázat kezeléséhez szükséges utókövetési intézkedést, amelynek a pénzügyi szervezet ki van téve, és nem tekinthetők a pénzügyi szervezet IKT-kockázatkezelési és -mérséklési képességei felügyeleti jóváhagyásának sem.

(62) Ahhoz, hogy biztosított legyen a pénzügyi ágazatban a harmadik féltől eredő IKT-kockázat megbízható nyomon követése, olyan elvalapú szabályok meghatározására van szükség, amelyek iránymutatásul szolgálnak a pénzügyi szervezetek számára azon kockázatok nyomon követése során, amelyek a harmadik fél IKT-szolgáltatókhoz kiszervezett funkciókkal, különösen a harmadik fél IKT-szolgáltatók által ellátott kritikus vagy fontos funkciókkal, valamint általánosabban a harmadik féltől való valamennyi IKT-függőséggel összefüggésben felmerülnek.

(63) Figyelembe véve az IKT-kockázat különböző forrásainak összetettségét, ugyanakkor a pénzügyi szolgáltatások zökkenőmentes nyújtását lehetővé tevő technológiai megoldások szolgáltatóinak nagy számát és sokféleségét is, e rendeletnek a harmadik fél IKT-szolgáltatók széles körére – köztük a felhőalapú számítástechnikai szolgáltatásokat, szoftvereket, adatelemzési szolgáltatásokat kínáló szolgáltatókra és az adatközpont-szolgáltatásokat nyújtó szolgáltatókra – kell vonatkoznia. Hasonlóképpen, mivel a pénzügyi szervezeteknek hatékonyan és koherens módon kell azonosítaniuk és kezelniük valamennyi kockázattípust, többek között a pénzügyi csoporton belül beszerzett IKT-szolgáltatásokkal összefüggésben, egyértelművé kell tenni, hogy azon vállalkozások, amelyek egy pénzügyi csoport részét képezik, és elsősorban az anyavállalatuk vagy az anyavállalatuk leányvállalatai vagy fióktelepei számára nyújtanak IKT-szolgáltatásokat, valamint azon pénzügyi szervezetek, amelyek egyéb pénzügyi szervezetek számára nyújtanak IKT-szolgáltatásokat, e rendelet értelmében szintén harmadik fél IKT-szolgáltatóknak tekintendők. Végül, tekintettel arra, hogy a pénzforgalmi szolgáltatások fejlődő piaca egyre nagyobb mértékben függ az összetett technikai megoldásoktól, valamint tekintettel a pénzforgalmi szolgáltatások és a pénzforgalmi vonatkozású megoldások újonnan megjelenő típusaira, a pénzforgalmi szolgáltatások ökoszisztémájának azon résztvevőit, amelyek fizetésfeldolgozási tevékenységet végeznek vagy fizetési infrastruktúrákat üzemeltetnek, e rendelet értelmében ugyancsak harmadik fél IKT-szolgáltatóknak kell tekinteni, kivéve a fizetési vagy értékpapír-kiegyenlítési rendszereket működtető központi bankokat, valamint az állami feladatok ellátása keretében IKT-vonatkozású szolgáltatásokat nyújtó hatóságokat.

(64) A pénzügyi szervezeteknek továbbra is mindenkor teljes felelősséggel kell tartozniuk az e rendeletben meghatározott kötelezettségeikért. A pénzügyi szervezeteknek arányos megközelítést kell alkalmazniuk a harmadik fél IKT-szolgáltatók szintjén felmerülő kockázatok arányos nyomon követésére, az IKT-vonatkozású függőségeik nagyságrendjének, összetettségének és fontosságának, továbbá a szerződéses megállapodás tárgyát képező szolgáltatások, folyamatok vagy funkciók kritikusságának vagy fontosságának kellő figyelembevételével, és végső soron a pénzügyi szolgáltatások folytonosságára és minőségére egyedi és csoportszinten gyakorolt bármely potenciális hatás körültekintő értékelése alapján.

(65) Az ilyen nyomon követés elvégzéséhez a harmadik féltől eredő IKT-kockázatra vonatkozó stratégiai megközelítést kell alkalmazni, amelyet a pénzügyi szervezet vezető testülete a harmadik féltől eredő IKT-kockázatra vonatkozó célzott stratégia elfogadásával tesz hivatalossá, és amely a harmadik féltől való IKT-függőségek folyamatos és teljeskörű szűrésén alapul. Ahhoz, hogy a felügyeleti hatóságok fokozottabban tudatában legyenek a harmadik féltől való IKT-függőségeknek, valamint az e rendelettel létrehozott felvigyázási keretrendszerrel összefüggésben végzett munka további támogatása érdekében, valamennyi pénzügyi szervezet számára elő kell írni, hogy vezessen nyilvántartást a harmadik fél IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételére vonatkozó valamennyi szerződéses megállapodásról. A pénzügyi felügyeletek számára lehetővé kell tenni, hogy bekérjék a teljes nyilvántartást, vagy annak egyes részeit, és így alapvető információkat szerezzenek a pénzügyi szervezetek IKT-függőségeinek szélesebb körű megértéséhez.

(66) A szerződéses megállapodások formális megkötését beható elemzésnek kell megelőznie és megalapoznia, különösen az olyan elemekre összpontosítva, mint a tervezett IKT-szerződés által támogatott szolgáltatások kritikussága vagy fontossága, a szükséges felügyeleti jóváhagyások és egyéb feltételek, az esetlegesen felmerülő koncentrációs kockázat, valamint a harmadik fél IKT-szolgáltatók kiválasztási és értékelési folyamata során a kellő gondosság alkalmazása, továbbá az esetleges összeférhetetlenségek értékelése. A kritikus vagy fontos funkciókra vonatkozó szerződéses megállapodások kapcsán a pénzügyi szervezeteknek figyelembe kell venniük, hogy a harmadik fél IKT-szolgáltatók a legfrissebb és legszigorúbb információbiztonsági szabványokat alkalmazzák-e. A szerződéses

megállapodások felmondását legalább egy sor olyan körülmény előidézheti, amely hiányosságokra enged következtetni a harmadik fél IKT-szolgáltató szintjén, így különösen a jogszabályok vagy a szerződéses feltételek jelentős megsértése, a szerződéses megállapodásokban meghatározott funkciók teljesítésének a lehetséges megváltozására utaló körülmények, a harmadik fél IKT-szolgáltató általános IKT-kockázatkezelésében mutatkozó gyengeségek jelei, vagy olyan körülmények, amelyek arra utalnak, hogy a releváns illetékes hatóság nem képes hatékonyan felügyelni a pénzügyi szervezetet.

(67) A harmadik fél IKT-szolgáltatók koncentrációs kockázata rendszerszintű hatásának kezelése érdekében e rendelet kiegyensúlyozott megoldást ösztönöz az ilyen koncentrációs kockázatra vonatkozó rugalmas és fokozatos megközelítés alkalmazásával, mivel bármely merev felső határ vagy szigorú korlátozás megállapítása akadályozhatja az üzletvitelt, és korlátozhatja a szerződési szabadságot. Azt, hogy mekkora valószínűséggel merülhet fel ilyen kockázat, a pénzügyi szervezeteknek a tervezett szerződéses megállapodásaik alapos vizsgálatával kell meg határozniuk, többek között az alvállalkozási megállapodások beható elemzésével, különösen akkor, ha azokat harmadik országban letelepedett, harmadik fél IKT-szolgáltatóval kötik. Ebben a szakaszban, a szerződési szabadság megőrzése és a pénzügyi stabilitás biztosítása közötti megfelelő egyensúly érdekében nem célszerű a harmadik féllel szembeni IKT-kockázati kitettségre vonatkozó szigorú felső határokkal és limitekkel kapcsolatos szabályokat meghatározni. A kritikus harmadik fél IKT-szolgáltatók tekintetében az e rendelet szerint kinevezett vezető felvigyázónak a felvigyázási keretrendszerrel összefüggésben különös figyelmet kell fordítania a kölcsönös függőségek mértékének megértésére, az olyan konkrét esetek feltárására, ahol a kritikus harmadik fél IKT-szolgáltatók Unión belüli magas koncentrációja valószínűleg megterheli az uniós pénzügyi rendszer stabilitását és integritását, valamint az említett konkrét kockázat azonosítása esetén párbeszédet kell folytatnia a kritikus harmadik fél IKT-szolgáltatókkal.

(68) Annak érdekében, hogy rendszeresen értékeljék és nyomon kövessék egy harmadik fél IKT-szolgáltató képességét arra, hogy a pénzügyi szervezet részére annak digitális működési rezilienciáját érő káros hatások nélkül, biztonságosan nyújtson szolgáltatásokat, a harmadik fél IKT-szolgáltatókkal kötött szerződések több kulcselemét a teljesítés egészére kiterjedően harmonizálni szükséges. Az ilyen harmonizációnak ki kell terjednie legalább azon területekre, amelyek elengedhetetlenek ahhoz, hogy a pénzügyi szervezet teljeskörűen nyomon követhesse a harmadik fél IKT-szolgáltatótól esetlegesen eredő kockázatokat a pénzügyi szervezet azon szükségletének szempontjából, hogy biztosítsa digitális rezilienciáját, mivel nagymértékben függ az igénybe vett IKT-szolgáltatások stabilitásától, funkciójától, rendelkezésre állásától és biztonságától.

(69) A szerződéses megállapodásoknak az e rendelet követelményeivel való összehangolást célzó újratárgyalása során a pénzügyi szervezeteknek és a harmadik fél IKT-szolgáltatóknak biztosítaniuk kell, hogy a megállapodások hatálya kiterjedjen az e rendeletben meghatározott főbb szerződéses rendelkezésekre.

(70) A „kritikus vagy fontos funkció” e rendeletben szereplő fogalommeghatározása magában foglalja a 2014/59/EU európai parlamenti és tanácsi irányelv ([20]) 2. cikke (1) bekezdésének 35. pontjában meghatározott „kritikus funkciókat”. Ennek megfelelően a 2014/59/EU irányelv alapján kritikusnak tekintett funkciók beletartoznak az e rendelet értelmében vett kritikus funkciók fogalommeghatározásába.

(71) A szerződéses megállapodásokban – függetlenül az IKT-szolgáltatások által támogatott funkció kritikusságától vagy fontosságától – pontosan meg kell határozni különösen a funkciók és szolgáltatások teljeskörű leírását, a funkciók teljesítésének és az adatkezelésnek a helyszíneit, valamint a szolgáltatási szintek teljeskörű leírását. Egyéb lényeges elemek annak lehetővé tételéhez, hogy a pénzügyi szervezet nyomon kövesse a harmadik féltől származó IKT-kockázatot, a következők: szerződéses rendelkezések, amelyek meghatározzák, hogy a harmadik fél IKT-szolgáltató hogyan biztosítja a személyes adatok hozzáférhetőségét, rendelkezésre állását, integritását, biztonságát és védelmét; rendelkezések, amelyek meghatározzák a harmadik fél IKT-szolgáltató fizetésképtelensége, szanálása vagy üzleti tevékenységének megszűnése esetén az adatokhoz való hozzáférést, azok behajtását és visszaszolgáltatását lehetővé tevő releváns garanciákat; rendelkezések, amelyek előírják a harmadik fél IKT-szolgáltató számára a nyújtott

([20]) Az Európai Parlament és a Tanács 2014/59/EU irányelve (2014. május 15.) a hitelintézetek és befektetési vállalkozások helyreállítását és szanálását célzó keretrendszer létrehozásáról és a 82/891/EGK tanácsi irányelv, a 2001/24/EK, 2002/47/EK, 2004/25/EK, 2005/56/EK, 2007/36/EK, 2011/35/EU, 2012/30/EU és 2013/36/EU irányelv, valamint az 1093/2010/EU és a 648/2012/EU európai parlamenti és tanácsi rendelet módosításáról (HL L 173., 2014.6.12., 190. o.).

szolgáltatásokkal kapcsolatos IKT-biztonsági események esetén a többletköltség nélkül vagy előzetesen meghatározott költség mellett történő segítségnyújtást; a harmadik fél IKT-szolgáltató azon kötelezettségére vonatkozó rendelkezések, hogy maradéktalanul együttműködjön a pénzügyi szervezet illetékes hatóságaival és szanálási hatóságaival; valamint a szerződéses megállapodások megszüntetésére vonatkozó felmondási jogokra és a kapcsolódó minimális felmondási időre vonatkozó rendelkezések, összhangban az illetékes hatóságok és a szanálási hatóságok elvárásaival.

(72) Az ilyen szerződéses rendelkezéseken túlmenően, és annak biztosítása érdekében, hogy a pénzügyi szervezetek megőrizzék a teljes kontrollt a harmadik felek szintjén bekövetkező, az IKT-biztonságukra nézve potenciálisan ártalmas valamennyi fejlemény felett, a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások nyújtására vonatkozó szerződéseknek a következőkről is rendelkezniük kell: a szolgáltatási szint teljeskörű leírásának pontos meghatározása pontos mennyiségi és minőségi teljesítménycélokkal együtt, hogy indokolatlan késedelem nélkül meg lehessen hozni a megfelelő korrekciós intézkedéseket, amennyiben az elfogadott szolgáltatási szintek nem teljesülnek; a harmadik fél IKT-szolgáltatóra vonatkozó releváns felmondási idők és a pénzügyi szervezettel szembeni adatszolgáltatási kötelezettségeik az olyan fejlemények esetén, amelyek lényeges hatást gyakorolhatnak a harmadik fél IKT-szolgáltató azon képességére, hogy eredményesen nyújtsa a vonatkozó IKT-szolgáltatásait; a harmadik fél IKT-szolgáltatóra vonatkozó azon követelmény, hogy vészhelyzeti terveket vezessen be és teszteljen, továbbá rendelkezzen olyan IKT-biztonsági intézkedésekkel, eszközökkel és szabályzatokkal, amelyek lehetővé teszik a biztonságos szolgáltatásnyújtást, valamint hogy részt vegyen és teljes mértékben együttműködjön a pénzügyi szervezet által végzett TLPT során.

(73) A kritikus vagy fontos funkciókat támogató IKT-szolgáltatások nyújtására vonatkozó szerződéseknek olyan rendelkezéseket is tartalmazniuk kell, amelyek biztosítják a pénzügyi szervezet vagy egy kinevezett harmadik fél általi hozzáférési, ellenőrzési és audit jogokat, valamint a másolatkészítés jogát, mint elengedhetetlen eszközeit annak, hogy a pénzügyi szervezet folyamatosan nyomon követhesse a harmadik fél IKT-szolgáltató teljesítését, ami egyúttal feltételezi a szolgáltató teljes mértékű együttműködését az ellenőrzések során. Hasonlóképpen, a pénzügyi szervezet illetékes hatóságának is jogosultsággal kell rendelkeznie arra, hogy értesítés alapján – a bizalmas jellegű adatok védelmére is figyelemmel – ellenőrzést és auditot végezzen a harmadik fél IKT-szolgáltatónál.

(74) Az említett szerződéses megállapodásoknak célzott kilépési stratégiákat is meg kell határozniuk, ez utóbbiakkal lehetővé téve különösen a kötelező átállási időszakokat, amelyek során a harmadik fél IKT-szolgáltatóknak folyamatosan biztosítaniuk kell a releváns szolgáltatásokat annak érdekében, hogy a zavarok pénzügyi szervezet szintjén való fellépésének a kockázata mérséklődjön, vagy a szervezet eredményesen átválthasson más harmadik fél IKT-szolgáltatók igénybevételére, vagy ehelyett saját, házon belüli megoldásokhoz folyamodhasson, a nyújtott IKT-szolgáltatás összetettségének megfelelően. A 2014/59/EU irányelv hatálya alá tartozó pénzügyi szervezeteknek továbbá biztosítaniuk kell, hogy az IKT-szolgáltatásokra vonatkozó releváns szerződések robusztus kialakításúak és az említett pénzügyi szervezetek szanálása esetén maradéktalanul érvényesíthetőek legyenek. Ezért az említett pénzügyi szervezeteknek a szanálási hatóságok elvárásaival összhangban biztosítaniuk kell, hogy az IKT-szolgáltatásokra vonatkozó releváns szerződések szanálás esetén reziliensek. Az említett pénzügyi szervezeteknek mindaddig, amíg továbbra is teljesítik fizetési kötelezettségeiket, egyéb követelmények mellett biztosítaniuk kell, hogy az IKT-szolgáltatásokra vonatkozó szerződések rendelkezéseket tartalmazzanak arra vonatkozóan, hogy szerkezetátalakítás vagy szanálás indokával a szerződés nem szüntethető meg, nem függeszthető fel, és nem módosítható.

(75) Ezenkívül, a felhőszolgáltatásokra vonatkozóan a hatóságok vagy az uniós intézmények által kidolgozott általános szerződéses rendelkezések – így különösen a Bizottság által kidolgozott szerződéses rendelkezések – önkéntes alkalmazása további garanciát nyújthat a pénzügyi szervezetek és a harmadik fél IKT-szolgáltatók számára azáltal, hogy – a pénzügyi szolgáltatásokra vonatkozó uniós jogban meghatározott követelményekkel és elvárásokkal teljes összhangban – fokozza a jogbiztonság-szintjüket a pénzügyi ágazatban igénybe vett felhőszolgáltatások tekintetében. Az általános szerződéses rendelkezések kidolgozásának alapját az azon 2018. évi pénzügyi technológiai cselekvési tervben már előirányzott intézkedések képezik, amelyben a Bizottság bejelentette a szándékát, hogy ösztönözze és elősegítse a pénzügyi szervezetek által igénybe vett kiszervezett felhőszolgáltatásokra vonatkozó általános szerződéses rendelkezések kidolgozását, támaszkodva a felhőszolgáltatásban érdekeltek azon ágazatközi erőfeszítéseire, amelyeket a pénzügyi ágazat segítségével a Bizottság elősegített.

(76) Annak érdekében, hogy előmozdítsák a pénzügyi ágazatban a harmadik féltől eredő IKT-kockázat kezelésekor alkalmazott felügyeleti megközelítések konvergenciáját és hatékonyságát, valamint megerősítsék az olyan pénzügyi szervezetek digitális működési rezilienciáját, amelyek a pénzügyi szolgáltatások nyújtását támogató IKT-szolgáltatásokat kritikus harmadik fél IKT-szolgáltatóktól veszik igénybe, és ezáltal hozzájáruljanak az uniós pénzügyi rendszer stabilitásának, valamint a pénzügyi szolgáltatások belső piaca integritásának megőrzéséhez, a kritikus harmadik fél IKT-szolgáltatóknak uniós felvigyázási keretrendszer hatálya alá kell tartozniuk. Míg a felvigyázási keretrendszer létrehozását indokolttá teszik az uniós szintű fellépés hozzáadott értéke, továbbá az IKT-

szolgáltatások pénzügyi szolgáltatásnyújtás terén történő igénybevételének velejáró szerepe és sajátosságai, emlékeztetni kell ugyanakkor arra, hogy ez a megoldás csak ezzel, a kifejezetten a pénzügyi ágazat digitális működési rezilienciájával foglalkozó rendelettel összefüggésben tűnik alkalmasnak. Egy ilyen felvigyázási keretrendszer azonban nem tekinthető új modellnek az uniós felügyelet számára a pénzügyi szolgáltatások és tevékenységek egyéb területein.

(77) A felvigyázási keretrendszer hatályának kizárólag a kritikus harmadik fél IKT-szolgáltatókra célszerű kiterjednie. Ezért be kell vezetni egy kijelölési mechanizmust, amely figyelembe veszi azt, hogy a pénzügyi ágazat milyen mértékben és jelleggel támaszkodik ilyen harmadik fél IKT-szolgáltatókra. Az említett mechanizmusnak tartalmaznia kell egy sor mennyiségi és minőségi kritériumot azon kritikussá minősítési paraméterek meghatározása céljából, amelyeken a felvigyázási keretrendszerbe foglalás alapul. Annak biztosítása érdekében, hogy ez az értékelés pontos legyen, és függetlenül a harmadik fél IKT-szolgáltató szervezeti felépítésétől, e kritériumoknak az olyan harmadik fél IKT-szolgáltatók esetében, amelyek egy nagyobb csoporthoz tartoznak, a harmadik fél teljes IKT-szolgáltatói csoport felépítését figyelembe kell venniük. Egyrészről az említett kritériumok alkalmazásával automatikusan nem kijelölt, kritikus harmadik fél IKT-szolgáltatók számára lehetővé kell tenni a felvigyázási keretrendszerben történő önkéntes részvételt, másrészről mentesíteni kell azon harmadik fél IKT-szolgáltatókat, amelyek már olyan felvigyázási mechanizmust alkotó keretek hatálya alá tartoznak, amelyek támogatják a Központi Bankok Európai Rendszerének az EUMSZ 127. cikkének (2) bekezdésében említett feladatai ellátását.

(78) Hasonlóképpen, az olyan pénzügyi szervezetek számára, amelyek más pénzügyi szervezeteknek nyújtanak IKT-szolgáltatásokat, miközben az e rendelet szerinti harmadik fél IKT-szolgáltatók kategóriájába tartoznak, szintén mentességet kell biztosítani a felvigyázási keretrendszer alól, mivel már a releváns uniós pénzügyi szolgáltatási jogszabályok által létrehozott felügyeleti mechanizmusok hatálya alá tartoznak. Az illetékes hatóságoknak a felügyeleti tevékenységeikkel összefüggésben adott esetben figyelembe kell venniük azon IKT-kockázatot, amelyet az IKT-szolgáltatásokat nyújtó pénzügyi szervezetek jelentenek a pénzügyi szervezetek számára. Hasonlóképpen, a kockázatfigyelési mechanizmusok csoportszintű meglétéből fakadóan ugyanilyen mentességet kell bevezetni az olyan harmadik fél IKT-szolgáltatók számára, amelyek túlnyomóan a saját csoportjukba tartozó szervezetek számára nyújtanak szolgáltatásokat. Az olyan harmadik fél IKT-szolgáltatókat, amelyek csak egy tagállamban nyújtanak IKT-szolgáltatásokat olyan pénzügyi szervezeteknek, amelyek tevékenységüket csak az említett tagállamban folytatják, tevékenységeik korlátozottsága és a határokon átnyúló hatás hiánya miatt szintén mentesíteni kell a kijelölési mechanizmus alól.

(79) A pénzügyi szolgáltatások területén tapasztalható digitális átalakulás következtében soha nem látott mértékűvé vált az IKT-szolgáltatások igénybevétele és az azoktól való függés. Mivel mára elképzelhetetlenné vált a felhőszolgáltatások, szoftveres megoldások és adatokkal kapcsolatos szolgáltatások igénybevétele nélküli pénzügyi szolgáltatásnyújtás, az Unió pénzügyi ökoszisztémája és bizonyos, IKT-szolgáltatók által nyújtott IKT-szolgáltatások között mostanra mély kölcsönös függőségi viszony alakult ki. Az említett szolgáltatók közül néhányan az IKT-alapú technológiák kifejlesztése és alkalmazása terén folytatott innovatori tevékenységüknél fogva jelentős szerepet töltenek be a pénzügyi szolgáltatások nyújtásában, vagy szervesen beépültek a pénzügyi szolgáltatási értékláncba. Így kritikussá váltak az uniós pénzügyi rendszer stabilitása és integritása szempontjából. Ez a kritikus harmadik fél IKT-szolgáltatók által nyújtott szolgáltatásoktól való széles körű függés – a különböző piaci szereplők információs rendszerei közötti kölcsönös függőséggel kombinálva – közvetlen és potenciálisan súlyos kockázatot jelent az Unió pénzügyi szolgáltatási rendszerére és a pénzügyi szolgáltatások nyújtásának folytonosságára nézve, ha a kritikus harmadik fél IKT-szolgáltatókat működési zavarok vagy jelentős kiberbiztonsági események érintenék. A kiberbiztonsági események egyik feltűnő képessége az, hogy a pénzügyi ágazatban figyelemmel kísért egyéb típusú kockázatoknál lényegesen gyorsabb ütemben sokszorozódhatnak és terjedhetnek a pénzügyi rendszerben, valamint átnyúlhatnak más ágazatokba és a földrajzi határokon túl is. Az ilyen események potenciálisan rendszerszintű válsággá szélesedhetnek, amennyiben megkopik a pénzügyi rendszerbe vetett bizalom a reálgazdaságot támogató funkciók zavara vagy jelentős pénzügyi veszteségek miatt, és ez olyan szintet ér el, amelyet a pénzügyi rendszer már nem bír el, vagy amely erőteljes sokkhatás-elnyelő intézkedéseket tesz szükségessé. Annak érdekében, hogy ilyen helyzetek ne következhessenek be – veszélyeztetve az Unió pénzügyi stabilitását és integritását –, alapvető fontosságú biztosítani a pénzügyi területen fennálló, harmadik féltől eredő IKT-kockázattal kapcsolatos felügyeleti gyakorlatok közötti konvergenciát, így különösen olyan új szabályok révén, amelyek lehetővé teszik a kritikus harmadik fél IKT-szolgáltatók feletti uniós szintű felvigyázást.

(80) A felvigyázási keretrendszer jelentős részben függ attól, hogy milyen mértékű az együttműködés a vezető felvigyázó és a pénzügyi szervezetek számára a pénzügyi szolgáltatások nyújtását befolyásoló szolgáltatásokat nyújtó, kritikus harmadik fél IKT-szolgáltató között. A felvigyázás sikere többek között a vezető felvigyázó azon képességén múlik, hogy hatékonyan el tudja-e végezni a kritikus harmadik fél IKT-szolgáltatók által alkalmazott szabályok, kontrollok és folyamatok értékelését célzó nyomonkövetési missziókat és ellenőrzéseket, továbbá fel tudja-e mérni az e szolgáltatók tevékenységei által a pénzügyi stabilitásra és a pénzügyi rendszer integritására gyakorolt potenciális kumulatív hatást. Kritikus jelentőségű ugyanakkor, hogy a kritikus harmadik fél IKT-szolgáltatók kövessék a vezető felvigyázó által megfogalmazott ajánlásokat, és megoldást találjanak az általa felvetett aggályokra. Mivel az együttműködés hiánya – így például a telephelyeire való belépés vagy az információszolgáltatás megtagadása – valamely, olyan szolgáltatásokat nyújtó, kritikus harmadik fél IKT-szolgáltató részéről, amelyek befolyásolják a pénzügyi szolgáltatások nyújtását, végső soron megfosztaná a vezető felvigyázót a harmadik féltől eredő IKT-kockázat felmérését lehetővé tevő alapvető eszközeitől, és káros hatásokkal járhatna a pénzügyi stabilitásra és a pénzügyi rendszer integritására nézve, szükséges rendelkezni egy arányos szankciórendszerről is.

(81) Mindezt szem előtt tartva, azon igényt, hogy a vezető felvigyázó a kritikus harmadik fél IKT-szolgáltatókat az e rendeletben meghatározott átláthatósági és hozzáféréssel kapcsolatos kötelezettségek teljesítésére kötelező büntető bírságokat szabhasson ki, nem veszélyeztethetik olyan nehézségek, amelyek az említett bírságoknak a harmadik országbeli székhellyel rendelkező, kritikus harmadik fél IKT-szolgáltatókkal szembeni végrehajtásából fakadnak. Az említett bírságok végrehajthatóságának biztosítása érdekében, valamint hogy gyorsan foganatosítani lehessen a kijelölési mechanizmussal és az ajánlások kibocsátásával összefüggésben a kritikus harmadik fél IKT-szolgáltatók védelemhez való jogának érvényesítését szolgáló eljárásokat, azon kritikus harmadik fél IKT-szolgáltatókat, amelyek pénzügyi szervezetek számára a pénzügyi szolgáltatások nyújtását befolyásoló szolgáltatásokat nyújtanak, kötelezni kell arra, hogy megfelelő üzleti jelenléttel rendelkezzenek az Unióban. A felvigyázás jellegéből és abból fakadóan, hogy más joghatóságokban nincs ezzel összehasonlítható szabályozás, nem állnak rendelkezésre olyan alternatív mechanizmusok, amelyek alkalmasak arra, hogy e célkitűzés elérését a harmadik országbeli pénzügyi felügyeletekkel történő hatékony együttműködés útján biztosítsák az olyan rendszerszintű jelentőséggel bíró harmadik fél IKT-szolgáltatók által képviselt digitális működési kockázatok hatásának figyelemmel kísérése vonatkozásában, amelyek harmadik országban letelepedett kritikus harmadik fél IKT-szolgáltatóknak minősülnek. Ezért egy olyan, harmadik országban letelepedett, harmadik fél IKT-szolgáltatónak, amelyet e rendelet értelmében kritikusnak jelöltek ki, ahhoz, hogy az Unióban továbbra is nyújthasson IKT-szolgáltatásokat pénzügyi szervezeteknek, az ekként való kijelölése időpontjától számított 12 hónapon belül minden szükséges lépést meg kell tennie – az uniós vívmányokban mindenütt alkalmazott, nevezetesen a 2013/34/EU európai parlamenti és tanácsi irányelvben ([21]) foglalt fogalommeghatározás szerinti leányvállalat létrehozása révén – az Unióban történő bejegyeztetése céljából.

(82) A leányvállalat Unióban való létrehozásának követelménye nem jelenti azt, hogy a kritikus harmadik fél IKT-szolgáltató nem nyújthat IKT-szolgáltatásokat és azokhoz kapcsolódó technikai támogatást az Unión kívül található létesítményekből és infrastruktúra révén. E rendelet nem ír elő adatlokalizálási kötelezettséget, mivel nem teszi kötelezővé, hogy az adattárolást- vagy kezelést az Unióban kell végezni.

(83) A kritikus harmadik fél IKT-szolgáltatók számára lehetővé kell tenni, hogy a világon bárhonnan tudjanak IKT-szolgáltatásokat nyújtani, vagyis nem szükségszerűen vagy nem csak az Unióban található telephelyekről. A felvigyázási tevékenységeket először az Unióban található telephelyeken, az Unióban található gazdasági szereplőkkel való kapcsolatfelvétel útján kell elvégezni – ideértve a kritikus harmadik fél IKT-szolgáltatók által az e rendelet szerint létrehozott leányvállalatokat is. Az ilyen, Unión belüli intézkedések azonban kevésnek bizonyulhatnak ahhoz, hogy a vezető felvigyázó maradéktalanul és hatékonyan el tudja látni az e rendelet szerinti feladatait. A vezető felvigyázónak ezért jogosultnak kell lennie a megfelelő felvigyázási hatáskörei harmadik országokban való gyakorlására is. Az említett hatáskörök harmadik országokban való gyakorlása keretében a vezető felvigyázónak meg kell tudnia vizsgálni azon létesítményeket, amelyekből a kritikus harmadik fél IKT-szolgáltató az IKT-szolgáltatásokat vagy a technikai támogató szolgáltatásokat ténylegesen nyújtja vagy irányítja, továbbá átfogó és operatív szintű átlátásra kell tudnia szert tenni a kritikus harmadik fél IKT-szolgáltató IKT-kockázatkezeléséről. A vezető felvigyázó uniós hivatalként történő, az Unió területén kívüli hatáskörgyakorlásának a lehetőségét megfelelően feltételekhez kell kötni – mindenekelőtt az érintett kritikus harmadik fél IKT-szolgáltató

([21]) Az Európai Parlament és a Tanács 2013/34/EU irányelve (2013. június 26.) a meghatározott típusú vállalkozások éves pénzügyi kimutatásairól, összevont (konszolidált) éves pénzügyi kimutatásairól és a kapcsolódó beszámolókról, a 2006/43/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 78/660/EGK és a 83/349/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 182., 2013.6.29., 19. o.).

hozzájárulásához. Hasonlóképpen feltétel, hogy a harmadik ország releváns hatóságait tájékoztassák a vezető felvigyázó tevékenységeinek a területükön történő gyakorlásáról, és hogy azok ne emeljenek kifogást. A hatékony végrehajtás biztosítása érdekében azonban – valamint az uniós intézmények és a tagállamok vonatkozó hatásköreinek sérelme nélkül – az ilyen hatásköröket az érintett harmadik ország releváns hatóságaival igazgatási együttműködési megállapodások megkötése révén teljeskörűen rögzíteni is kell. E rendeletben ezért lehetővé kell tenni az EFH-k számára, hogy a megfelelő harmadik országbeli hatóságokkal igazgatási együttműködési megállapodásokat kössenek, amelyek egyébként nem keletkeztethetnek az Unió és tagállamai vonatkozásában jogi kötelezettségeket.

(84) A vezető felvigyázóval való kommunikáció megkönnyítése és a megfelelő képviselet biztosítása érdekében azon kritikus harmadik fél IKT-szolgáltatóknak, amelyek valamely csoport tagjai, ki kell jelölniük egy jogi személyt a koordinációs pontjuk szerepének betöltésére.

(85) A felvigyázási keretrendszer nem sértheti a tagállamok azon hatáskörét, hogy lefolytassák saját felvigyázási vagy nyomonkövetési misszióikat azon harmadik fél IKT-szolgáltatók tekintetében, amelyeket e rendelet alapján nem jelöltek ki kritikusként, de amelyeket nemzeti szinten jelentősnek tekintenek.

(86) A pénzügyi szolgáltatások területét jellemző többrétegű intézményi struktúra kihasználása érdekében az EFH-k vegyes bizottságának – a kiberbiztonsággal kapcsolatos feladataival összhangban – továbbra is biztosítania kell az általános ágazatközi koordinációt az IKT-kockázatot érintő valamennyi kérdésben. Ennek során a vegyes bizottságot egy új albizottságnak kell támogatnia (a továbbiakban: a felvigyázási fórum), amely ellátja mind a kritikus harmadik fél IKT-szolgáltatókat érintő egyedi döntésekhez, mind a kollektív ajánlások kibocsátásához szükséges előkészítő munkát, különösen a kritikus harmadik fél IKT-szolgáltatókra vonatkozó felvigyázási programok összehasonlító teljesítményértékelése és az IKT-koncentrációs kockázattal kapcsolatos kérdéseket kezelő legjobb gyakorlatok azonosítása kapcsán.

(87) Annak biztosítása céljából, hogy a kritikus harmadik fél IKT-szolgáltatókra vonatkozóan megfelelő és hatékony uniós szintű felvigyázás érvényesüljön, e rendelet úgy rendelkezik, hogy a három EFH bármelyike kijelölhető vezető felvigyázóként. Az egyes konkrét kritikus harmadik fél IKT-szolgáltatókat annak értékelése alapján kell hozzárendelni a három EFH valamelyikéhez, hogy túlnyomóan milyen pénzügyi szervezetek működnek az említett EFH felelősségi körébe tartozó pénzügyi ágazatokban. E megközelítésnek a feladatoknak és a felelősségi köröknek a három EFH közötti kiegyensúlyozott elosztását kell eredményeznie a felvigyázási funkciók ellátása tekintetében, valamint biztosítania kell a három hatóságnál rendelkezésre álló emberi erőforrások és technikai szakértelem lehető legjobb kihasználását.

(88) A vezető felvigyázók számára biztosítani kell a vizsgálatok lefolytatásához, a kritikus harmadik fél IKT-szolgáltatók telephelyein és helyszínein a helyszíni és a helyszínen kívüli ellenőrzések elvégzéséhez, valamint a hiánytalan és naprakész információk beszerzéséhez szükséges hatásköröket. Az említett hatásköröknek képessé kell tenniük a vezető felvigyázót arra, hogy tényleges betekintést nyerjen a pénzügyi szervezeteket – és végső soron az Unió pénzügyi rendszerét – érintő, harmadik felektől eredő IKT-kockázat típusába, dimenziójába és hatásába. Az EFH-k vezető felvigyázási szereppel való felruházása szükséges előfeltétele az IKT-kockázat rendszerszintű dimenziója megértésének és kezelésének pénzügyi téren. A kritikus harmadik fél IKT-szolgáltatók által az uniós pénzügyi ágazatra gyakorolt hatás és az ezzel járó IKT-koncentrációs kockázat által okozott potenciális problémák miatt uniós szintű kollektív megközelítés alkalmazására van szükség. Ha számos illetékes hatóság párhuzamosan gyakorol többféle ellenőrzési és hozzáférési jogot egymástól elkülönülten, kismértékű egymás közötti koordináció mellett vagy annak teljes hiányában, az megakadályozná, hogy a pénzügyi felügyeletek teljes és átfogó áttekintésre tegyenek szert az Unióban meglévő, harmadik felektől eredő IKT-kockázatot illetően, ugyanakkor a kritikus harmadik fél IKT-szolgáltatók számára redundanciát, megterhelést és bonyolultságot is jelentene, ha számos nyomonkövetési és ellenőrzési kérés vonatkozna rájuk.

(89) Tekintettel arra, hogy a kritikusként való kijelölés jelentős hatásokkal jár, e rendelettel biztosítani kell a kritikus harmadik fél IKT-szolgáltatók jogainak a felvigyázási keretrendszer végrehajtása során történő tiszteletben tartását. Az ilyen szolgáltatóknak a kritikusként való kijelölésüket megelőzően például joguk kell, hogy legyen ahhoz, hogy a vezető felvigyázóhoz indokolással ellátott nyilatkozatot nyújtsanak be, amely tartalmaz minden, a kijelölésükkel kapcsolatos értékelés céljából releváns információt. Mivel a vezető felvigyázónak felhatalmazással kell rendelkeznie az IKT-kockázatot érintő kérdésekről és azok megfelelő korrekciós intézkedéseiről szóló ajánlások benyújtására, ami magában foglalja azon jogkört is, hogy kifogást emeljen bizonyos olyan szerződéses megállapodásokkal szemben, amelyek végső soron hátrányosan érintik valamely pénzügyi szervezet vagy a pénzügyi rendszer stabilitását, a kritikus harmadik fél IKT-szolgáltatók számára is biztosítani kell a lehetőséget, hogy az említett ajánlások véglegesítését megelőzően magyarázatot adjanak az ajánlásokban előirányzott megoldások várható hatásait illetően

az olyan ügyfelekre nézve, amelyek az e rendelet hatályán kívül eső szervezetek, és megoldásokat fogalmazzanak meg a kockázatok csökkentése érdekében. Az ajánlásokkal egyet nem értő, kritikus harmadik fél IKT-szolgáltatóknak indokolással ellátott magyarázatot kell benyújtaniuk az ajánlás jóvá nem hagyására irányuló szándékukról. Amennyiben nem nyújtanak be ilyen, indokolással ellátott magyarázatot, vagy az elégtelennek bizonyul, a vezető felvigyázónak nyilvános hirdetményt kell kiadnia, amelyben összefoglalva ismerteti a meg nem felelési ügyet.

(90) Az illetékes hatóságoknak a vezető felvigyázó által kibocsátott ajánlásoknak való érdemi megfelelés ellenőrzési feladatát megfelelően bele kell foglalniuk a pénzügyi szervezetek prudenciális felügyeletével kapcsolatos feladatkörükbe. Az illetékes hatóságoknak hatáskörrel kell rendelkezniük arra, hogy a vezető felvigyázó ajánlásaiban megjelölt kockázatok kezelése céljából további intézkedések megtételére kötelezzék a pénzügyi szervezeteket, és az illetékes hatóságoknak kellő időben ki kell adniuk erre irányuló értesítéseiket. Amikor a vezető felvigyázó olyan, kritikus harmadik fél IKT-szolgáltatóknak címzett ajánlásokat ad ki, amelyek az (EU) 2022/2555 irányelv szerinti felügyelet alá tartoznak, az illetékes hatóságoknak hatáskörrel kell rendelkezniük arra, hogy a további intézkedések megtétele előtt önkéntes alapon konzultáljanak az említett irányelv szerinti illetékes hatóságokkal annak érdekében, hogy elősegítsék a szóban forgó, kritikus harmadik fél IKT-szolgáltatókkal kapcsolatban a koordinált megközelítés mentén való ügyintézést.

(91) A felvigyázás gyakorlása során három operatív elvnek kell érvényesülnie, törekedve a következők biztosítására: a) szoros koordináció az EFH-k között vezető felvigyázási szerepük ellátásával összefüggésben, egy közös felvigyázási hálózaton (KFH) keresztül; b) összhang az (EU) 2022/2555 irányelv által létrehozott kerettel (az említett irányelv szerinti szervek közötti önkéntes konzultáció révén, a kritikus harmadik fél IKT-szolgáltatókra irányuló intézkedések közötti átfedések elkerülése érdekében); és c) gondosság alkalmazása a kritikus harmadik fél IKT-szolgáltatók által nyújtott szolgáltatások zavaraival kapcsolatos, olyan ügyfeleket érintő potenciális kockázatok minimalizálása érdekében, amelyek nem tartoznak e rendelet hatálya alá.

(92) A felvigyázási keretrendszer nem válthatja ki, vagy semmilyen módon és semmilyen részben nem helyettesítheti a pénzügyi szervezetekkel szembeni azon követelményt, hogy a harmadik fél IKT-szolgáltatók igénybevételével járó kockázatok kezeléséről maguk gondoskodjanak, ideértve azon kötelezettségüket, hogy fenntartsák a kritikus harmadik fél IKT-szolgáltatókkal létrejött szerződéses megállapodásaik folyamatos monitorozását. Hasonlóképpen, a felvigyázási keretrendszer nem érintheti a pénzügyi szervezetek azon teljes felelősségét, hogy megfeleljenek az e rendeletben és a pénzügyi szolgáltatásokra vonatkozó releváns jogszabályokban megállapított valamennyi jogi kötelezettségnek, és teljesítsék azokat.

(93) A párhuzamosságok és átfedések elkerülése érdekében az illetékes hatóságoknak tartózkodniuk kell olyan intézkedések egyenkénti meghozatalától, amelyek a kritikus harmadik fél IKT-szolgáltatók kockázatainak nyomon követésére irányulnak, és e tekintetben a vezető felvigyázó releváns értékelésére kell támaszkodniuk. A felvigyázási keretrendszerbe tartozó feladatok ellátásával összefüggésben minden intézkedést minden esetben egyeztetni kell a vezető felvigyázóval, és vele azokról előzetesen meg kell állapodni.

(94) A harmadik fél IKT-szolgáltatók digitáliskockázat-kezelésének felülvizsgálatával és nyomon követésével kapcsolatos bevált módszerek alkalmazása terén a nemzetközi konvergencia előmozdítása érdekében az EFH-kat arra kell ösztönözni, hogy kössenek együttműködési megállapodásokat a releváns, felügyeletet és szabályozást ellátó harmadik országbeli hatóságokkal.

(95) Az illetékes hatóságoknál, a három EFH-nál és – önkéntességi alapon – az (EU) 2022/2555 irányelv szerinti illetékes hatóságoknál működési és IKT-kockázatra szakosodott személyzet konkrét kompetenciáinak, technikai készségeinek és szakértelmének hasznosítása céljából a vezető felvigyázónak a nemzeti felügyeletek képességeire és tudására kell támaszkodnia, és célzott vizsgálócsoportokat kell létrehoznia minden egyes, kritikus harmadik fél IKT-szolgáltató tekintetében, multidiszciplináris csoportokat alkotva a felvigyázási tevékenységek előkészítésének és végrehajtásának a támogatására, ideértve az általános vizsgálatokat és a kritikus harmadik fél IKT-szolgáltatóknál végzett ellenőrzéseket is, valamint annak bármely szükséges utókövetése céljából.

(96) Míg a felvigyázási feladatokhoz kapcsolódó költségeket teljes mértékben a kritikus harmadik fél IKT-szolgáltatóknak felszámított díjak fedeznék, valószínű azonban, hogy az EFH-knál még a felvigyázási keretrendszer beindítása előtt felmerülnek olyan költségek, amelyek a jövőbeli felvigyázási tevékenységet támogató célzott IKT-rendszerek bevezetésével kapcsolatosak, mivel először ki kell alakítani és telepíteni kell célzott IKT-rendszereket. E rendelet ezért hibrid finanszírozási modell alkalmazását írja elő, ahol a felvigyázási keretrendszert magát teljes egészében díjakból kellene finanszírozni, míg az EFH-k IKT-rendszereinek kialakítását az Unió és az illetékes nemzeti hatóságok hozzájárulásaiból finanszíroznák.

(97) Az illetékes hatóságoknak rendelkezniük kell minden olyan felügyeleti, vizsgálati és szankcionálási hatáskörrel, amely az e rendelet szerinti feladataik ellátásához szükséges. Az általuk kiszabott közigazgatási szankciókról alapszabályként értesítést kell közzétenniük. Mivel a pénzügyi szervezetek és a harmadik fél IKT-szolgáltatók székhelye különböző tagállamokban is lehet, és azok különböző illetékes hatóságok felügyelete alá tartozhatnak, e rendelet alkalmazását meg kell könnyíteni egyfelől azáltal, hogy a releváns illetékes hatóságok szorosan együttműködnek egymással – ideértve az 1024/2013/EU tanácsi rendelettel ráruházott külön feladatok tekintetében az EKB-t is –, és másfelől azáltal, hogy konzultálnak az EFH-kkal a kölcsönös információcsere és a releváns felügyeleti tevékenységekkel összefüggésben történő segítségnyújtás révén.

(98) A kritikus harmadik fél IKT-szolgáltatókként való kijelöléséhez alapul szolgáló kritériumok mennyiségi és minőségi szempontjainak részletesebb meghatározása, valamint a felvigyázási díjak harmonizálása céljából a Bizottságot az EUMSZ 290. cikkével összhangban fel kell hatalmazni jogi aktusok elfogadására abból a célból, hogy e rendeletet kiegészítse a következők részletes meghatározása érdekében: egy harmadik fél IKT-szolgáltató meghibásodása vagy működési kiesése milyen rendszerszintű hatással jár azon pénzügyi szervezetekre nézve, amelyeknek IKT-szolgáltatásait nyújtja; azon globális rendszerszinten jelentős intézmények és egyéb rendszerszinten jelentős intézmények száma, amelyek a szóban forgó harmadik fél IKT-szolgáltatóra támaszkodnak; az adott piacon aktív harmadik fél IKT-szolgáltatók száma; mekkora költségekkel jár az adatok és az IKT-feladatok egy harmadik fél másik IKT-szolgáltatóhoz való átvitele; valamint a felvigyázási díjak összege, és a megfizetésük előírt módja. Különösen fontos, hogy a Bizottság az előkészítő munkája során megfelelő konzultációkat folytasson, többek között szakértői szinten is, és hogy e konzultációkra a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban ([22]) megállapított elvekkel összhangban kerüljön sor. Így különösen a felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlamentnek és a Tanácsnak a tagállamok szakértőivel egyidejűleg kell kézhez kapnia minden dokumentumot, és szakértőik számára lehetővé kell tenni a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein való rendszeres részvételt.

(99) A szabályozástechnikai standardoknak biztosítaniuk kell az e rendeletben megállapított követelmények következetes harmonizálását. Jelentős szakértelemmel rendelkező szervként betöltött szerepkörük részeként az EFH-knak kell kidolgozniuk azon Bizottság részére benyújtandó szabályozástechnikai standardtervezeteket, amelyek nem járnak szakpolitikai döntéshozatallal. Szabályozástechnikai standardokat kell kidolgozni az IKT-kockázatkezelés, a jelentős IKT-vonatkozású események bejelentése, tesztelése terén, valamint a harmadik féltől eredő IKT-kockázat megbízható nyomon követésére vonatkozó alapkövetelményekkel kapcsolatban. A Bizottságnak és az EFH-knak biztosítaniuk kell, hogy az említett standardokat és követelményeket valamennyi pénzügyi szervezet olyan módon tudja alkalmazni, amely arányban áll a méretével és általános kockázati profiljával, valamint szolgáltatásai, tevékenységei és műveletei jellegével, nagyságrendjével és összetettségével. A Bizottságot fel kell hatalmazni arra, hogy az EUMSZ 290. cikke szerinti felhatalmazáson alapuló jogi aktusok útján, valamint az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban elfogadja az említett szabályozás-technikai standardokat.

(100) A jelentős IKT-vonatkozású eseményekkel és a jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményekkel kapcsolatos bejelentések összehasonlíthatóságának megkönnyítése érdekében, valamint a harmadik fél IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokkal kapcsolatos átláthatóság biztosítása céljából az EFH-knak végrehajtás-technikai standardtervezeteket kell kidolgozniuk a jelentős IKT-vonatkozású eseményeknek és a jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményeknek a pénzügyi szervezetek általi bejelentésére szolgáló egységes mintadokumentumok, űrlapok és eljárások, továbbá az információk nyilvántartásához szükséges egységes mintadokumentumok létrehozása céljából. Az említett standardok kidolgozása során az EFH-knak figyelembe kell venniük a pénzügyi szervezet méretét és általános kockázati profilját, valamint a szolgáltatásai, tevékenységei és műveletei jellegét, nagyságrendjét és összetettségét. A Bizottságot fel kell hatalmazni arra, hogy az EUMSZ 291. cikke szerinti végrehajtási jogi aktusok útján, valamint az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 15. cikkével összhangban elfogadja az említett végrehajtás-technikai standardokat.

([22]) HL L 123., 2016.5.12., 1. o.

(101) mivel korábban már sor került további követelmények felhatalmazáson alapuló és végrehajtási jogi aktusok útján történő meghatározására az 1060/2009/EK ([23]), a 648/2012/EU ([24]), a 600/2014/EU ([25]) és a 909/2014/EU ([26]) európai parlamenti és tanácsi rendeletben foglalt szabályozás-technikai és végrehajtás-technikai standardok alapján, helyénvaló felhatalmazni az EFH-kat, hogy akár önállóan, akár a vegyes bizottság keretében együttesen szabályozás-technikai és végrehajtás-technikai standardokat terjesszenek a Bizottság elé azon felhatalmazáson alapuló és végrehajtási jogi aktusok elfogadása céljából, amelyek továbbviszik és aktualizálják a meglévő IKT-kockázatkezelési szabályokat.

(102) mivel ez a rendelet az (EU) 2022/2556 európai parlamenti és tanácsi irányelvvel ([27]) együtt maga után vonja a pénzügyi szolgáltatásokra vonatkozó uniós vívmányok számos rendeletében és irányelvében, többek között az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU és a 909/2014/EU rendeletben, valamint az (EU) 2016/1011 ([28]) európai parlamenti és tanácsi rendeletben foglalt, az IKT-kockázatkezelésre vonatkozó rendelkezések egységes szerkezetbe foglalását, a teljes következetesség biztosítása érdekében az említett rendeleteket módosítani kell annak egyértelművé tétele céljából, hogy az alkalmazandó, IKT-kockázatkezeléssel kapcsolatos rendelkezéseket e rendelet állapítja meg.

(103) Következésképpen az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendeletben a működési kockázattal kapcsolatos azon releváns cikkek hatályát, amelyek a felhatalmazáson alapuló és a végrehajtási jogi aktusok elfogadására vonatkozó felhatalmazást tartalmazták, le kell szűkíteni annak érdekében, hogy e rendeletbe kerüljenek át mindazon rendelkezések, amelyek jelenleg az említett rendeletek részét képező, a digitális működési rezilienciával kapcsolatos aspektusokat szabályozzák.

(104) A fizetési rendszerek működtetését és a fizetésfeldolgozási tevékenységek ellátását lehetővé tevő IKT-infrastruktúrák használatával kapcsolatos potenciális rendszerszintű kiberkockázatokat uniós szinten megfelelően kezelni kell a digitális működési rezilienciára vonatkozó harmonizált szabályok útján. E célból a Bizottságnak mielőbb fel kell mérnie, hogy szükség van-e e rendelet hatályának felülvizsgálatára – amely felülvizsgálat egyúttal összehangolandó az (EU) 2015/2366 irányelvben előirányzott átfogó felülvizsgálat eredményével. Az elmúlt évtizedben elkövetett számos nagyszabású támadás mutatja, hogyan váltak a fizetési rendszerek a kiberfenyegetéseknek kitetté. Mivel központi helyzetben vannak a pénzforgalmi szolgáltatási láncban, és erőteljesen összekapcsolódnak az általános pénzügyi rendszerrel, a fizetési rendszerek és a fizetésfeldolgozási tevékenységek kritikus jelentőségre tettek szert az uniós pénzügyi piacok működése szempontjából. Az ilyen rendszerek elleni kibertámadások súlyos működési zavarokat okozhatnak az üzletmenetben, amelyek közvetlenül kihathatnak a legfőbb gazdasági funkciókra – így például a fizetések megkönnyítésére –, és a kapcsolódó gazdasági folyamatokra közvetett hatást gyakorolhatnak. Amíg létre nem jön egy harmonizált rendszer, és meg nem valósul a fizetésirendszer-üzemeltetők és a fizetésfeldolgozó szervezetek feletti uniós szintű felügyelet, a tagállamok – hasonló piaci gyakorlatok alkalmazása céljából – a saját joghatóságuk alatt felügyelt fizetésirendszer-üzemeltetőkre és fizetésfeldolgozó szervezetekre vonatkozó szabályok alkalmazásakor inspirációt nyerhetnek az e rendelettel meghatározott, a digitális működési rezilienciára vonatkozó követelményekből.

([23]) Az Európai Parlament és a Tanács 1060/2009/EK rendelete (2009. szeptember 16.) a hitelminősítő intézetekről (HL L 302., 2009.11.17., 1. o.).

([24]) 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.).

([25]) Az Európai Parlament és a Tanács 600/2014/EU rendelete (2014. május 15.) a pénzügyi eszközök piacairól és a 648/2012/EU rendelet módosításáról (HL L 173., 2014.6.12., 84. o.).

([26]) 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 a 98/26/EK és a 2014/65/EU irányelv, valamint a 236/2012/EU rendelet módosításáról (HL L 257., 2014.8.28., 1. o.).

([27]) Az Európai Parlament és a Tanács (EU) 2022/2556 irányelve (2022. december 14.) a 2009/65/EK, 2009/138/EK, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 és (EU) 2016/2341 irányelvnek a pénzügyi ágazat digitális működési rezilienciája tekintetében történő módosításáról (lásd e Hivatalos Lap 153. oldalát).

([28]) Az Európai Parlament és a Tanács (EU) 2016/1011 rendelete (2016. június 8.) a pénzügyi eszközökben és pénzügyi ügyletekben referenciamutatóként vagy a befektetési alapok teljesítményének méréséhez felhasznált indexekről, valamint a 2008/48/EK és a 2014/17/EU irányelv, továbbá az 596/2014/EU rendelet módosításáról (HL L 171., 2016.6.29., 1. o.).

(105) mivel e rendelet célját – nevezetesen a szabályozott pénzügyi szervezetek számára magas szintű digitális működési reziliencia megvalósítását – a tagállamok nem tudják kielégítően megvalósítani, mert az számos különböző uniós és nemzeti jogszabály harmonizálását követeli meg, az Unió szintjén azonban e cél nagyságrendje és hatása miatt jobban megvalósítható, az Unió intézkedéseket hozhat a szubszidiaritásnak az Európai Unióról szóló szerződés 5. cikkében foglalt elvével összhangban. Az arányosságnak az említett cikkben foglalt elvével összhangban ez a rendelet nem lépi túl az e cél eléréséhez szükséges mértéket.

(106) Az európai adatvédelmi biztossal az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([29]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos 2021. május 10-én véleményt nyilvánított ([30]),

ELFOGADTA EZT A RENDELETET:

I. FEJEZET

Általános rendelkezések

1. cikk

Tárgy

(1) Az egységesen magas szintű digitális működési reziliencia elérése érdekében e rendelet egységes követelményeket állapít meg a pénzügyi szervezetek üzleti folyamatait támogató hálózati és információs rendszerek biztonságára vonatkozóan, a következők szerint:

a) a pénzügyi szervezetekre a következőkkel kapcsolatban alkalmazandó követelmények:

   i. az információs és kommunikációs technológiák (IKT) kockázatkezelése;

   ii. a jelentős IKT-vonatkozású események bejelentése és a jelentős kiberfenyegetésekre vonatkozó – önkéntes alapon történő – értesítés az illetékes hatóságok felé;

   iii. a jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményeknek a 2. cikk (1) bekezdésének a)–d) pontjában említett pénzügyi szervezetek általi bejelentése az illetékes hatóságoknál;

   iv. a digitális működési reziliencia tesztelése;

   v. a kiberfenyegetésekkel és sérülékenységekkel kapcsolatos információk és hírszerzés megosztása;

   vi. a harmadik féltől eredő IKT-kockázat megbízható kezelését célzó intézkedések;

b) a harmadik fél IKT-szolgáltatók és a pénzügyi szervezetek között létrejött szerződéses megállapodásokkal kapcsolatos követelmények;

c) a pénzügyi szervezetek részére szolgáltatást nyújtó, kritikus harmadik fél IKT-szolgáltatók tekintetében a felvigyázási keretrendszer létrehozására és végzésére vonatkozó szabályok;

d) az illetékes hatóságok közötti együttműködés szabályai, valamint az illetékes hatóságok felügyeleti és végrehajtási tevékenységére vonatkozó szabályok az e rendeletben szabályozott kérdésekben.

(2) Az (EU) 2022/2555 irányelv 3. cikkét átültető nemzeti szabályok értelmében alapvető vagy fontos szervezetként azonosított pénzügyi szervezetek tekintetében ez a rendelet az említett irányelv 4. cikkének alkalmazásában ágazatspecifikus uniós jogi aktusnak minősül.

(3) E rendelet nem érinti a tagállamoknak a közbiztonságra, védelemre és nemzetbiztonságra vonatkozó alapvető állami funkciók tekintetében az uniós joggal összhangban fennálló felelősségét.

([29]) 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.).

([30]) HL C 229., 2021.6.15., 16. o.

2. cikk

Hatály

(1) A (3) és a (4) bekezdés sérelme nélkül, e rendelet a következő jogalanyokra alkalmazandó:

a) hitelintézetek;

b) pénzforgalmi intézmények, ideértve az (EU) 2015/2366 irányelv alapján mentességet élvező pénzforgalmi intézményeket is;

c) számlainformációkat összesítő szolgáltatók;

d) elektronikuspénz-kibocsátó intézmények, ideértve a 2009/110/EK irányelv alapján mentesített elektronikuspénz-kibocsátó intézményeket is;

e) befektetési vállalkozások;

f) a kriptoeszközök piacairól, valamint az 1093/2010/EU és az 1095/2010/EU rendelet, továbbá a 2013/36/EU és az (EU) 2019/1937 irányelv módosításáról szóló európai parlamenti és tanácsi rendelet (a továbbiakban: a kriptoeszközök piacairól szóló rendelet) alapján engedélyezett kriptoeszköz-szolgáltatók, valamint az eszközalapú tokenek kibocsátói;

g) központi értéktárak;

h) központi szerződő felek;

i) kereskedési helyszínek;

j) kereskedési adattárak;

k) alternatívbefektetésialap-kezelők;

l) alapkezelő társaságok;

m) adatszolgáltatók;

n) biztosítók és viszontbiztosítók;

o) biztosításközvetítők, viszontbiztosítás-közvetítők és a kiegészítő biztosításközvetítői tevékenységet végző személyek;

p) foglalkoztatói nyugellátást szolgáltató intézmények;

q) hitelminősítő intézetek;

r) kritikus referenciamutatók kezelői;

s) közösségi finanszírozási szolgáltatók;

t) értékpapírosítási adattárak;

u) harmadik fél IKT-szolgáltatók.

(2) E rendelet alkalmazásában az (1) bekezdés a)–t) pontjában említett szervezetek együttes megnevezése: „pénzügyi szervezetek”.

(3) Ez a rendelet nem alkalmazandó a következőkre:

a) a 2011/61/EU irányelv 3. cikkének (2) bekezdésében említett alternatívbefektetésialap-kezelők;

b) a 2009/138/EK irányelv 4. cikkében említett biztosítók és viszontbiztosítók;

c) olyan nyugdíjkonstrukciókat működtető foglalkoztatói nyugellátást szolgáltató intézmények, amely nyugdíjkonstrukciók összesen nem rendelkeznek tizenötnél több taggal;

d) a 2014/65/EU irányelv 2. és 3. cikke alapján mentességet élvező természetes vagy jogi személyek;

e) mikrovállalkozásnak vagy kis- vagy középvállalkozásnak minősülő biztosításközvetítők, viszontbiztosítás-közvetítők és kiegészítő biztosításközvetítői tevékenységet végző személyek;

f) a 2013/36/EU irányelv 2. cikke (5) bekezdésének 3. pontjában említett postai elszámolóközpontok.

(4) A tagállamok kizárhatják e rendelet hatálya alól a 2013/36/EU irányelv 2. cikke (5) bekezdésének 4–23. pontjában említett, saját területükön található jogalanyokat. Amennyiben valamely tagállam él az ilyen lehetőséggel, arról – valamint az ezzel kapcsolatos minden későbbi változásról is – tájékoztatja a Bizottságot. A Bizottság honlapján vagy egyéb könnyű hozzáférést biztosító úton nyilvánosságra hozza az említett információkat.

3. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „digitális működési reziliencia”: a pénzügyi szervezet képessége arra, hogy kiépítse, biztosítsa és felülvizsgálja működési integritását és megbízhatóságát azáltal, hogy harmadik fél IKT-szolgáltatók által nyújtott szolgáltatások igénybevételével közvetlenül vagy közvetetten biztosítja azon hálózati és információs rendszerek biztonságának kezeléséhez szükséges IKT-vonatkozású képességek teljes körét, amelyeket a pénzügyi szervezet használ, és amelyek a pénzügyi szolgáltatások folyamatos nyújtását és minőségét támogatják, többek között zavarok fennállásakor is;

2. „hálózati és információs rendszer”: az (EU) 2022/2555 irányelv 6. cikkének 1. pontjában meghatározott hálózati és információs rendszer;

3. „elavult IKT-rendszer”: olyan IKT-rendszer, amely elérte életciklusának végét (kifutási szakaszban van), amely technológiai vagy kereskedelmi okokból már nem alkalmas frissítésre vagy javításra, vagy amelyhez értékesítője vagy harmadik fél IKT-szolgáltató már nem nyújt támogatást, amely azonban még használatban van, és támogatja a pénzügyi szervezet funkcióit;

4. „hálózati és információs rendszerek biztonsága”: az (EU) 2022/2555 irányelv 6. cikkének 2. pontjában meghatározott hálózati és információs rendszerek biztonsága;

5. „IKT-kockázat”: minden olyan, a hálózati és információs rendszerek használata kapcsán észszerűen azonosítható körülmény, amely, ha bekövetkezik, veszélyeztetheti a hálózati és információs rendszerek, valamely technológiafüggő eszköz vagy folyamat, vagy egyéb műveletek és folyamatok vagy a szolgáltatásnyújtás biztonságát azáltal, hogy káros hatásokkal jár a digitális vagy a fizikai környezetre nézve;

6. „információs vagyonelem”: információk olyan tárgyi vagy immateriális gyűjteménye, amely védelemre érdemes;

7. „IKT-eszköz”: a pénzügyi szervezet által használt hálózati és információs rendszerek részét képező szoftver- vagy hardvereszköz;

8. „IKT-vonatkozású esemény”: olyan, a pénzügyi szervezet által nem tervezett egyedi esemény vagy egymással összefüggő események sorozata, amely veszélyezteti a hálózati és információs rendszerek biztonságát, és káros hatása van az adatok rendelkezésre állására, hitelességére, integritására vagy bizalmas jellegére, vagy a pénzügyi szervezet által nyújtott szolgáltatásokra;

9. „pénzforgalmi vonatkozású működési vagy biztonsági esemény”: olyan, a 2. cikk (1) bekezdésének a) d) pontjában említett pénzügyi szervezetek által nem tervezett, akár IKT-vonatkozású, akár egyéb egyedi esemény vagy egymással összefüggő események sorozata, amelynek káros hatása van a pénzforgalmi vonatkozású adatok rendelkezésre állására, hitelességére, integritására vagy bizalmas jellegére, vagy a pénzügyi szervezet által nyújtott pénzforgalmi vonatkozású szolgáltatásokra;

10. „jelentős IKT-vonatkozású esemény”: olyan IKT-vonatkozású esemény, amelynek jelentős káros hatása van a pénzügyi szervezet kritikus vagy fontos funkcióit támogató hálózati és információs rendszerekre;

11. „jelentős pénzforgalmi vonatkozású működési vagy biztonsági esemény”: olyan pénzforgalmi vonatkozású működési vagy biztonsági esemény, amelynek jelentős káros hatása van a pénzügyi szervezetek által nyújtott pénzforgalmi vonatkozású szolgáltatásokra;

12. „kiberfenyegetés”: az (EU) 2019/881 rendelet 2. cikkének 8. pontjában meghatározott kiberfenyegetés;

13. „jelentős kiberfenyegetés”: olyan kiberfenyegetés, amelynek technikai sajátosságai azt jelzik, hogy potenciálisan jelentős IKT-vonatkozású eseményt vagy jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményt eredményezhet;

14. „kibertámadás”: rosszindulatú IKT-vonatkozású esemény, amelynek során valamely fenyegető szereplő valamely eszköz megsemmisítésére, felfedésére, módosítására, használhatatlanná tételére, eltulajdonítására, az eszközhöz való illetéktelen hozzáférésre, vagy annak illetéktelen felhasználására tesz kísérletet;

15. „fenyegetettséggel kapcsolatos hírszerzés”: azzal a céllal összesített, átalakított, elemzett, értelmezett vagy tovább gazdagított információk, hogy biztosítsák a döntéshozatalhoz szükséges kontextust, és lehetővé tegyék a valamely IKT-vonatkozású esemény vagy kiberfenyegetés hatásainak enyhítéséhez szükséges releváns és elégséges szintű megértést, ideértve valamely kibertámadás technikai részleteit, a támadásért felelősök kilétét, valamint az elkövetés módját és indítékait;

16. „sérülékenység”: valamely vagyonelem, rendszer, folyamat vagy kontroll kihasználható gyengesége, érzékenysége vagy hibája;

17. „fenyegetés alapú behatolási tesztelés (threat led penetration testing, TLPT)”: olyan keret, amely utánozza egy tényleges kiberfenyegetés forrásának tekintett, valós fenyegetést jelentő szereplők taktikáját, módszereit és eljárásait, és amely elvégzi a pénzügyi szervezet kritikus éles rendszereinek kontrollált, testreszabott, hírszerzésen alapuló (red team) tesztelését;

18. „harmadik féltől eredő IKT-kockázat”: a pénzügyi szervezetnél azzal összefüggésben felmerülő esetleges IKT-kockázat, hogy harmadik fél IKT-szolgáltatók vagy azok alvállalkozói által nyújtott szolgáltatásokat vesz igénybe, ideértve a kiszervezés útján igénybe vett IKT-szolgáltatásokat is;

19. „harmadik fél IKT-szolgáltató”: IKT-szolgáltatásokat nyújtó vállalkozás;

20. „csoporton belüli IKT-szolgáltató”: olyan vállalkozás, amely egy pénzügyi csoport részét képezi, és főként az ugyanazon csoportba vagy ugyanazon intézményvédelmi rendszerhez tartozó pénzügyi szervezeteknek – többek között az anyavállalatának, leányvállalatainak és fióktelepeinek, vagy más, közös tulajdonban vagy közös ellenőrzés alatt álló szervezeteknek – történő IKT-szolgáltatásnyújtással foglalkozik;

21. „IKT-szolgáltatások”: IKT-rendszerek útján egy vagy több belső vagy külső felhasználó részére folyamatos jelleggel nyújtott digitális és adatszolgáltatások, ideértve a hardvert mint szolgáltatást és a hardverszolgáltatásokat, ami magában foglalja a hardverszolgáltató általi szoftver- vagy belsőrendszervezérlőprogram-(firmware-)frissítéseket is, ide nem értve a hagyományos analóg telefonszolgáltatásokat;

22. „kritikus vagy fontos funkció”: olyan funkció, amelynek zavara lényegesen rontaná a pénzügyi szervezet pénzügyi teljesítményét, vagy szolgáltatásai és tevékenységei megbízhatóságát vagy folytonosságát, vagy az említett funkció kiesése, hibás vagy meghiúsult működése lényegesen rontaná a pénzügyi szervezet képességét az engedélyében foglalt feltételek és kötelezettségek, valamint a pénzügyi szolgáltatásokra vonatkozó jogszabályokban előírt egyéb kötelezettségei folyamatos teljesítésére;

23. „kritikus harmadik fél IKT-szolgáltató”: a 31. cikkel összhangban kritikusként kijelölt, harmadik fél IKT-szolgáltató;

24. „harmadik országban letelepedett, harmadik fél IKT-szolgáltató”: harmadik országban letelepedett, jogi személyiséggel rendelkező, harmadik fél IKT-szolgáltató, amely egy pénzügyi szervezettel IKT-szolgáltatások nyújtásáról szóló szerződéses megállapodást kötött;

25. „leányvállalat”: a 2013/34/EU irányelv 2. cikke 10. pontjának és 22. cikkének értelmében vett leányvállalkozás;

26. „csoport”: a 2013/34/EU irányelv 2. cikkének 11. pontjában meghatározott csoport;

27. „anyavállalat”: a 2013/34/EU irányelv 2. cikkének 9. pontja és 22. cikke értelmében vett anyavállalat;

28. „harmadik országban letelepedett IKT-alvállalkozó”: harmadik országban letelepedett, jogi személyiséggel rendelkező IKT-alvállalkozó, amely harmadik fél IKT-szolgáltatóval vagy harmadik országban letelepedett, harmadik fél IKT-szolgáltatóval szerződéses megállapodást kötött;

29. „IKT-koncentrációs kockázat”: egyetlen vagy több kapcsolódó kritikus harmadik fél IKT-szolgáltatóval szembeni kitettség, amely az ilyen szolgáltatóktól való olyan mértékű függőséget teremt, hogy egy ilyen szolgáltató rendelkezésre nem állása, meghibásodása vagy egyéb típusú hiányossága potenciálisan veszélyeztetheti a pénzügyi szervezet kritikus vagy fontos funkciók ellátására való képességét, vagy számára más típusú káros hatásokat – többek között nagy veszteségeket – okozhat, vagy veszélyeztetheti az Unió egészének pénzügyi stabilitását;

30. „vezető testület”: a 2014/65/EU irányelv 4. cikke (1) bekezdésének 36. pontjában, a 2013/36/EU irányelv 3. cikke (1) bekezdésének 7. pontjában, a 2009/65/EK európai parlamenti és tanácsi irányelv ([31]) 2. cikke (1) bekezdésének s. pontjában, a 909/2014/EU rendelet 2. cikke (1) bekezdésének 45. pontjában, az (EU) 2016/1011 rendelet 3. cikke (1) bekezdésének 20. pontjában és a kriptoeszközök piacairól szóló rendelet releváns rendelkezéseiben meghatározott vezető testület, vagy annak tagjaival egyenértékű személyek csoportja, akik ténylegesen működtetik a szervezetet, vagy a releváns uniós vagy nemzeti jogszabályokkal összhangban kulcsfontosságú funkciókat látnak el;

31. „hitelintézet”: az 575/2013/EU európai parlamenti és tanácsi rendelet ([32]) 4. cikke (1) bekezdésének 1. pontjában meghatározott hitelintézet;

32. „a 2013/36/EU irányelv alapján mentesített intézmény”: valamely, a 2013/36/EU irányelv 2. cikke (5) bekezdésének 4–23. pontjában említett jogalany;

33. „befektetési vállalkozás”: a 2014/65/EU irányelv 4. cikke (1) bekezdésének 1. pontjában meghatározott befektetési vállalkozás;

34. „kis méretű és össze nem kapcsolt befektetési vállalkozás”: olyan befektetési vállalkozás, amely megfelel az (EU) 2019/2033 európai parlamenti és tanácsi rendelet ([33]) 12. cikkének (1) bekezdésében megállapított feltételeknek;

35. „pénzforgalmi intézmény”: az (EU) 2015/2366 irányelv 4. cikkének 4. pontjában meghatározott pénzforgalmi intézmény;

36. „az (EU) 2015/2366 irányelv alapján mentesített pénzforgalmi intézmény”: az (EU) 2015/2366 irányelv 32. cikkének (1) bekezdése értelmében mentességet élvező pénzforgalmi intézmény;

37. „számlainformációkat összesítő szolgáltató”: az (EU) 2015/2366 irányelv 33. cikkének (1) bekezdésében említett számlainformációkat összesítő szolgáltató;

38. „elektronikuspénz-kibocsátó intézmény”: a 2009/110/EK európai parlamenti és tanácsi irányelv 2. cikkének 1. pontjában meghatározott elektronikuspénz-kibocsátó intézmény;

39. „a 2009/110/EK irányelv alapján mentesített elektronikuspénz-kibocsátó intézmény”: a 2009/110/EK irányelv 9. cikkének (1) bekezdésében foglaltak szerinti, mentességet élvező elektronikuspénz-kibocsátó intézmény;

40. „központi szerződő fél”: a 648/2012/EU rendelet 2. cikkének 1. pontjában meghatározott központi szerződő fél;

41. „kereskedési adattár”: a 648/2012/EU rendelet 2. cikkének 2. pontjában meghatározott kereskedési adattár;

42. „központi értéktár”: a 909/2014/EU rendelet 2. cikke (1) bekezdésének 1. pontjában meghatározott központi értéktár;

43. „kereskedési helyszín”: a 2014/65/EU irányelv 4. cikke (1) bekezdésének 24. pontjában meghatározott kereskedési helyszín;

44. „alternatívbefektetésialap-kezelő”: a 2011/61/EU irányelv 4. cikke (1) bekezdésének b) pontjában meghatározott alternatívbefektetésialap-kezelő;

45. „alapkezelő társaság”: a 2009/65/EK irányelv 2. cikke (1) bekezdésének b) pontjában meghatározott alapkezelő társaság;

46. „adatszolgáltató”: a 600/2014/EU rendelet értelmében vett, annak 2. cikk (1) bekezdésének 34–36. pontjában említett adatszolgáltató;

47. „biztosító”: a 2009/138/EK irányelv 13. cikkének 1. pontjában meghatározott biztosító;

48. „viszontbiztosító”: a 2009/138/EK irányelv 13. cikkének 4. pontjában meghatározott viszontbiztosító;

([31]) Az Európai Parlament és a Tanács 2009/65/EK irányelve (2009. július 13.) az átruházható értékpapírokkal foglalkozó kollektív befektetési vállalkozásokra (ÁÉKBV) vonatkozó törvényi, rendeleti és közigazgatási rendelkezések összehangolásáról (HL L 302., 2009.11.17., 32. o.).

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

([33]) Az Európai Parlament és a Tanács (EU) 2019/2033 rendelete (2019. november 27.) a befektetési vállalkozásokra vonatkozó prudenciális követelményekről, valamint az 1093/2010/EU, az 575/2013/EU, a 600/2014/EU és a 806/2014/EU rendelet módosításáról (HL L 314., 2019.12.5., 1. o.).

49. „biztosításközvetítő”: az (EU) 2016/97 európai parlamenti és tanácsi irányelv ([34]) 2. cikke (1) bekezdésének 3. pontjában meghatározott biztosításközvetítő;

50. „kiegészítő biztosításközvetítői tevékenységet végző személy”: az (EU) 2016/97 irányelv 2. cikke (1) bekezdésének 4. pontjában meghatározott kiegészítő biztosításközvetítői tevékenységet végző személy;

51. „viszontbiztosítás-közvetítő”: az (EU) 2016/97 irányelv 2. cikke (1) bekezdésének 5. pontjában meghatározott viszontbiztosítás-közvetítő;

52. „foglalkoztatói nyugellátást szolgáltató intézmény”: az (EU) 2016/2341 irányelv 6. cikkének 1. pontjában meghatározott foglalkoztatói nyugellátást szolgáltató intézmény;

53. „kis méretű foglalkoztatói nyugellátást szolgáltató intézmény”: olyan nyugdíjkonstrukciókat működtető foglalkoztatói nyugellátást szolgáltató intézmény, amely nyugdíjkonstrukciók összesen nem rendelkeznek száznál több taggal;

54. „hitelminősítő intézet”: az 1060/2009/EK rendelet 3. cikke (1) bekezdésének b) pontjában meghatározott hitelminősítő intézet;

55. „kriptoeszköz-szolgáltató”: a kriptoeszközök piacairól szóló rendelet releváns rendelkezéseiben meghatározott kriptoeszköz-szolgáltató;

56. „eszközalapú tokenek kibocsátója”: a kriptoeszközök piacairól szóló rendelet releváns rendelkezéseiben meghatározott eszközalapú tokenek kibocsátója;

57. „kritikus referenciamutatók kezelője”: az (EU) 2016/1011 rendelet 3. cikke (1) bekezdésének 25. pontjában meghatározott »kritikus referenciamutatók« kezelője;

58. „közösségi finanszírozási szolgáltató”: az (EU) 2020/1503 európai parlamenti és tanácsi rendelet ([35]) 2. cikke (1) bekezdésének e) pontjában meghatározott közösségi finanszírozási szolgáltató;

59. „értékpapírosítási adattár”: az (EU) 2017/2402 európai parlamenti és tanácsi rendelet ([36]) 2. cikkének 23. pontjában meghatározott értékpapírosítási adattár;

60. „mikrovállalkozás”: a kereskedési helyszínektől, a központi szerződő felektől, a kereskedési adattáraktól és a központi értéktáraktól eltérő olyan pénzügyi szervezet, amely kevesebb mint 10 főt foglalkoztat, és éves árbevétele és/vagy éves mérlegfőösszege nem haladja meg a 2 millió EUR-t;

61. „vezető felvigyázó”: az e rendelet 31. cikke (1) bekezdésének b) pontjával összhangban kinevezett európai felügyeleti hatóság;

62. „vegyes bizottság”: az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 54. cikkében említett bizottság;

63. „kisvállalkozás”: olyan pénzügyi szervezet, amely 10 vagy több főt, de kevesebb mint 50 főt foglalkoztat, és 2 millió EUR-t meghaladó, de 10 millió EUR-t meg nem haladó éves árbevétellel és/vagy éves mérlegfőösszeggel rendelkezik;

64. „középvállalkozás”: olyan pénzügyi szervezet, amely nem kisvállalkozás, kevesebb mint 250 főt foglalkoztat, és 50 millió EUR-t meg nem haladó éves árbevétellel és/vagy 43 millió EUR-t meg nem haladó éves mérlegfőösszeggel rendelkezik;

65. „hatóság”: bármely kormányzati vagy egyéb közigazgatási szerv, ideértve a nemzeti központi bankokat is.

([34]) Az Európai Parlament és a Tanács (EU) 2016/97 irányelve (2016. január 20.) a biztosítási értékesítésről (HL L 26., 2016.2.2., 19. o.).

([35]) Az Európai Parlament és a Tanács (EU) 2020/1503 rendelete (2020. október 7.) az európai közösségi finanszírozási üzleti szolgáltatókról, valamint az (EU) 2017/1129 rendelet és az (EU) 2019/1937 irányelv módosításáról (HL L 347., 2020.10.20., 1. o.).

([36]) Az Európai Parlament és a Tanács (EU) 2017/2402 rendelete (2017. december 12.) az értékpapírosítás általános keretrendszerének meghatározásáról, az egyszerű, átlátható és egységesített értékpapírosítás egyedi keretrendszerének létrehozásáról, valamint a 2009/65/EK, a 2009/138/EK és a 2011/61/EU irányelv és az 1060/2009/EK és a 648/2012/EU rendelet módosításáról (HL L 347., 2017.12.28., 35. o.).

4. cikk

Arányossági elv

(1) A pénzügyi szervezetek a II. fejezetben megállapított szabályokat az arányosság elvével összhangban hajtják végre, figyelembe véve méretüket és általános kockázati profiljukat, valamint szolgáltatásaik, tevékenységeik és működésük jellegét, nagyságrendjét és összetettségét.

(2) Ezenkívül, a III. és a IV. fejezet, valamint az V. fejezeten belüli I. szakasz pénzügyi szervezetek általi alkalmazásának arányban kell állnia méretükkel és általános kockázati profiljukkal, valamint szolgáltatásaik, tevékenységeik és működésük jellegével, nagyságrendjével és összetettségével, amint azt az említett fejezetek releváns szabályai konkrétan előírják.

(3) Az illetékes hatóságoknak figyelembe kell venniük az arányossági elv pénzügyi szervezetek általi alkalmazását, amikor felülvizsgálják az IKT-kockázatkezelési keretrendszer következetességét az illetékes hatóságok kérésére a 6. cikk (5) bekezdésének és a 16. cikk (2) bekezdésének alapján benyújtott jelentések alapján.

II. FEJEZET

IKT-kockázatkezelés

I. szakasz

5. cikk

Irányítás és szervezés

(1) A pénzügyi szervezeteknek rendelkezniük kell egy olyan belső irányítási és kontrollkerettel, amely biztosítja az IKT-kockázat eredményes és prudens kezelését a 6. cikk (4) bekezdésével összhangban, a digitális működési reziliencia magas szintjének elérése érdekében.

(2) A pénzügyi szervezet vezető testületének kell meghatároznia, jóváhagynia és felvigyáznia a 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszerrel összefüggő valamennyi intézkedést, és viselnie a felelősséget azok végrehajtásáért.

Az első albekezdés alkalmazásában a vezető testület:

a) viseli a végső felelősséget a pénzügyi szervezet IKT-kockázatainak kezeléséért;

b) bevezet az adatok rendelkezésre állására, hitelességére, integritására és bizalmas kezelésére vonatkozó magas szintű normák fenntartását biztosítani célzó politikákat;

c) egyértelmű feladat- és felelősségi köröket jelöl ki valamennyi IKT-vonatkozású funkcióval összefüggésben, és létrehozza az említett funkciók közötti hatékony és jól időzített kommunikációt, együttműködést és koordinációt biztosító, megfelelő irányítási rendszert;

d) viseli a 6. cikk (8) bekezdésében említett, digitális működési rezilienciára vonatkozó stratégia létrehozásával és jóváhagyásával kapcsolatos általános felelősséget, ideértve a pénzügyi szervezet megfelelő IKT-kockázati tolerancia-szintjének a 6. cikk (8) bekezdésének b) pontjában említett megállapítását is;

e) jóváhagyja, felvigyázza és időszakonként felülvizsgálja a pénzügyi szervezetnek a 11. cikk (1), illetve (3) bekezdésében említett IKT-üzletmenetfolytonossági politikáját, illetve IKT-reagálási és -helyreállítási tervét, amelyeknek elfogadására sor kerülhet a pénzügyi szervezet átfogó üzletmenet-folytonossági politikájának, valamint reagálási és helyreállítási tervének integráns részét képező célzott egyedi szabályzat formájában is;

f) jóváhagyja és időszakonként felülvizsgálja a pénzügyi szervezet IKT-vonatkozású belső ellenőrzési terveit, IKT-ellenőrzéseit és azok lényeges módosításait;

g) megállapítja és időszakonként felülvizsgálja a pénzügyi szervezet digitális működési rezilienciával kapcsolatos szükségleteinek kielégítését biztosító költségvetést minden erőforrástípus tekintetében, ideértve a személyzet valamennyi tagja számára biztosítandó, a 13. cikk (6) bekezdésében említett releváns, IKT-biztonsági tudatosságot elősegítő programokat és digitális működési rezilienciával kapcsolatos képzéseket, valamint IKT-készségeket;

h) jóváhagyja és időszakonként felülvizsgálja a pénzügyi szervezetnek a harmadik fél IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételéről szóló megállapodásokkal kapcsolatos szabályait;

i) vállalati szinten létrehozza a következőkkel kapcsolatos megfelelő tájékozódást lehetővé tevő bejelentési csatornákat:

   i. a harmadik fél IKT-szolgáltatókkal az IKT-szolgáltatások igénybevételére vonatkozóan kötött megállapodások;

   ii. bármely releváns, a harmadik fél IKT-szolgáltatókra vonatkozó tervezett lényeges változtatás;

   iii. az ilyen változtatások potenciális hatása az említett megállapodásokkal érintett kritikus vagy fontos funkciókra, ideértve az említett változtatások hatását értékelő kockázatelemzés-összefoglalót, továbbá legalább a jelentős IKT-vonatkozású események és azok hatásai, valamint reagálási, helyreállítási és korrekciós intézkedések.

(3) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek létre kell hozniuk egy feladatkört a harmadik fél IKT-szolgáltatókkal az IKT-szolgáltatások alkalmazásáról kötött megállapodások nyomon követése érdekében, vagy ki kell jelölniük a felső vezetés egy tagját a kapcsolódó kockázati kitettség és a releváns dokumentáció feletti felvigyázásért felelős személyként.

(4) A pénzügyi szervezet vezető testülete tagjainak aktívan tájékozódniuk kell az aktuális információkról annak érdekében, hogy rendelkezésükre álljanak az ahhoz szükséges megfelelő ismeretek és készségek, hogy át tudják látni és értékelni tudják az IKT-kockázatot és annak a pénzügyi szervezet működésére gyakorolt hatását, többek között a kezelés alatt álló IKT-kockázattal arányos, célirányos képzés rendszeres végzése révén.

II. szakasz

6. cikk

IKT-kockázatkezelési keretrendszer

(1) A pénzügyi szervezeteknek általános kockázatkezelési rendszerük részeként megbízható, átfogó és jól dokumentált IKT-kockázatkezelési keretrendszerrel kell rendelkezniük, amely lehetővé teszi számukra az IKT-kockázat gyors, hatékony és átfogó kezelését, továbbá a digitális működési reziliencia magas szintjének biztosítását.

(2) Az IKT-kockázatkezelési keretrendszer magában foglalja legalább azon stratégiákat, szabályzatokat, eljárásokat, IKT-protokollokat és -eszközöket, amelyek szükségesek valamennyi információs vagyonelem és IKT-eszköz – többek között a számítógépes szoftverek, hardvereszközök és szerverek – kellő és adekvát védelméhez, valamint valamennyi releváns fizikai rendszerelem és infrastruktúra – így például a telephelyek, az adatközpontok és kijelölt érzékeny területek – védelméhez annak biztosítására, hogy valamennyi információs vagyonelem és IKT-eszköz megfelelő védelmet kapjon a kockázatokkal – köztük a káreseménnyel, valamint az illetéktelen hozzáféréssel és használattal – szemben.

(3) A pénzügyi szervezeteknek az IKT-kockázatkezelési keretrendszerükkel összhangban, megfelelő stratégiák, szabályzatok, eljárások, protokollok és eszközök bevezetésével minimalizálniuk kell az IKT-kockázat hatását. Az IKT-kockázatról és az IKT-kockázatkezelési keretrendszerükről teljeskörű és naprakész tájékoztatást kell nyújtaniuk az illetékes hatóságok számára, azok kérésére.

(4) A mikrovállalkozásnak nem minősülő pénzügyi szervezetek az IKT-kockázat kezelésére és felvigyázására vonatkozó felelősséget egy kontrollfunkcióhoz rendelik hozzá, és az összeférhetetlenségek elkerülése érdekében biztosítják az ilyen kontrollfunkció megfelelő szintű függetlenségét. A pénzügyi szervezetek biztosítják az IKT-kockázatkezelési funkciók, kontrollfunkciók és belső ellenőrzési funkciók megfelelő elkülönítését és függetlenségét a három védelmi vonalra épülő modellnek vagy egy belső kockázatkezelési és kontrollmodellnek megfelelően.

(5) Az IKT-kockázatkezelési keretrendszert dokumentálni kell, és legalább évente egyszer – vagy mikrovállalkozások esetében időszakonként – felül kell vizsgálni, továbbá jelentős IKT-vonatkozású események bekövetkezésekor, valamint a digitális működési reziliencia tesztelésére vagy ellenőrzésére irányuló releváns folyamatokból származó felügyeleti utasításokat és következtetéseket követően. A keretet folyamatosan fejleszteni kell a végrehajtás és a nyomon követés során szerzett tapasztalatok alapján. Az illetékes hatóság kérésére jelentést kell benyújtani számára az IKT-kockázatkezelési keretrendszer felülvizsgálatáról.

(6) A mikrovállalkozásnak nem minősülő pénzügyi szervezetek IKT-kockázatkezelési keretrendszerére ellenőrök általi, rendszeres, a pénzügyi szervezetek ellenőrzési tervével összhangban végzendő belső ellenőrzési kötelezettség vonatkozik. Az említett ellenőröknek elegendő ismerettel, készségekkel és szakértelemmel kell rendelkezniük az IKT-kockázat terén, valamint megfelelő függetlenséggel. Az IKT-ellenőrzések gyakoriságának és fókuszpontjának arányban kell állnia a pénzügyi szervezet IKT-kockázatával.

(7) A pénzügyi szervezetnek a belső ellenőrzési felülvizsgálat következtetései alapján formális utókövetési folyamatot kell kialakítania, beleértve a kritikus IKT-audit megállapítások kellő időben történő igazolására és a hiányosságok korrekciójára vonatkozó szabályokat.

(8) Az IKT-kockázatkezelési keretrendszernek magában kell foglalnia egy digitális működési rezilienciára vonatkozó stratégiát is, amely meghatározza, hogy hogyan hajtandó végre a keret. E célból a digitális működési rezilienciára vonatkozó stratégiának magában kell foglalnia az IKT-kockázat kezelésére és a konkrét IKT-célkitűzések megvalósítására irányuló módszereket, a következők révén:

a) ki kell fejteni, hogy az IKT-kockázatkezelési keretrendszer hogyan támogatja a pénzügyi szervezet üzleti stratégiáját és célkitűzéseit;

b) meg kell határozni az IKT-kockázati toleranciaszintet a pénzügyi szervezet kockázatvállalási hajlandóságával összhangban, továbbá elemezni kell az IKT-zavarok hatásaival kapcsolatos toleranciát;

c) egyértelmű információbiztonsági célokat kell kitűzni, megállapítva a fő teljesítménymutatókat és kockázati mérőszámokat is;

d) ismertetni kell az IKT-referenciaarchitektúrát az egyes konkrét üzleti célkitűzések eléréséhez szükséges változtatásokkal együtt;

e) fel kell vázolni azon különböző mechanizmusokat, amelyeket az IKT-vonatkozású események észlelése, hatásaik megelőzése és az azzal szembeni védelem céljából vezettek be;

f) a bejelentett jelentős IKT-vonatkozású események számát és a megelőző intézkedések eredményességét alapul véve, bizonyítékokkal alá kell támasztani a digitális működési reziliencia aktuális helyzetét;

g) e rendelet IV. fejezetével összhangban el kell végezni a digitális működési reziliencia tesztelését;

h) fel kell vázolni az IKT-vonatkozású események esetén alkalmazandó kommunikációs stratégiát, amelynek közzététele a 14. cikkel összhangban kötelező.

(9) A pénzügyi szervezetek a (8) bekezdésben említett, digitális működési rezilienciára vonatkozó stratégia keretében meghatározhatnak egy több szolgáltatóra épülő, holisztikus IKT-stratégiát is – akár csoport-, akár szervezeti szinten –, amely bemutatja a harmadik fél IKT-szolgáltatóktól való főbb függőségeket, és kifejti a harmadik fél IKT-szolgáltatóknál alkalmazott beszerzési mix indokait.

(10) A pénzügyi szervezetek az uniós és a nemzeti ágazati jogszabályokkal összhangban kiszervezhetik az IKT-kockázatkezelési követelményeknek való megfelelés ellenőrzésének feladatait csoporton belüli vagy külső vállalkozásokhoz. Kiszervezés esetén a pénzügyi szervezet továbbra is teljes felelősséggel tartozik az IKT-kockázatkezelési követelményeknek való megfelelés ellenőrzéséért.

7. cikk

IKT-rendszerek, -protokollok és -eszközök

A pénzügyi szervezetek az IKT-kockázat kezelése érdekében olyan naprakész IKT-rendszereket, -protokollokat és -eszközöket alkalmaznak és tartanak fenn, amelyek:

a) az arányosságnak a 4. cikkben említett elvével összhangban megfelelnek a tevékenységeik folytatását támogató műveletek nagyságrendjének;

b) megbízhatóak;

c) elegendő kapacitással rendelkeznek a tevékenységek elvégzéséhez és a szolgáltatások időben történő nyújtásához szükséges adatok pontos feldolgozására, továbbá szükség szerint a kiugróan magas megbízások, üzenetküldési vagy ügyleti volumenek kezelésére, többek között amennyiben új technológia bevezetésére kerül sor;

d) technológiai szempontból reziliensek annak érdekében, hogy szükség szerint, piaci stresszhelyzetben vagy egyéb kedvezőtlen helyzetekben megfelelően kezeljék a további információs feldolgozási igényeket.

8. cikk

Azonosítás

(1) A 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezeteknek azonosítaniuk, osztályozniuk és megfelelően dokumentálniuk kell valamennyi, az IKT-ra támaszkodó üzleti funkciót, feladat- és felelősségi kört, az említett funkciókat támogató információs vagyonelemeket és IKT-eszközöket, valamint azok IKT-kockázattal kapcsolatos feladatkörét és függőségeit. A pénzügyi szervezeteknek szükség szerint, de legalább évente felül kell vizsgálniuk ezen osztályozás és minden releváns dokumentáció megfelelőségét.

(2) A pénzügyi szervezeteknek folyamatosan azonosítaniuk kell az IKT-kockázat valamennyi forrását, különösen a más pénzügyi szervezetekkel szembeni és azoktól eredő kockázati kitettséget, továbbá értékelniük kell az IKT-ra támaszkodó üzleti funkcióik, információs vagyonelemeik és IKT-eszközeik szempontjából releváns kiberfenyegetéseket és IKT-sérülékenységeket. A pénzügyi szervezeteknek rendszeresen, de legalább évente felül kell vizsgálniuk az őket érintő kockázati forgatókönyveket.

(3) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek a hálózati és információsrendszer-infrastruktúrában, az IKT-ra támaszkodó üzleti funkcióikat, információs vagyonelemeiket és IKT-eszközeiket érintő folyamatokban és eljárásokban bekövetkezett minden jelentős változást követően kockázatértékelést kell végezniük.

(4) A pénzügyi szervezeteknek azonosítaniuk kell valamennyi információs vagyonelemet és IKT-eszközt, ideértve a távoli helyeken találhatókat is, továbbá a hálózati erőforrásokat és a hardvereszközöket, és fel kell térképezniük, hogy melyek tekinthetők kritikusnak. Fel kell térképezniük az információs vagyonelemek és IKT-eszközök konfigurációját, valamint a különböző információs vagyonelemek és IKT-eszközök közötti kapcsolatokat és kölcsönös függőségeket.

(5) A pénzügyi szervezeteknek azonosítaniuk és dokumentálniuk kell a harmadik fél IKT-szolgáltatóktól függő valamennyi folyamatot, valamint azonosítaniuk kell a kritikus vagy fontos funkciókat támogató szolgáltatást nyújtó, harmadik fél IKT-szolgáltatókkal meglévő összeköttetéseket.

(6) Az (1), (4) és (5) bekezdés alkalmazásában a pénzügyi szervezeteknek releváns nyilvántartásokat kell vezetniük, valamint azokat időszakonként és minden alkalommal, amikor a (3) bekezdésben említett jelentős változás következik be, frissíteniük kell.

(7) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek rendszeresen, de legalább évente, továbbá a technológiák, alkalmazások vagy rendszerek összekapcsolása előtt és után minden esetben célzottan értékelniük kell valamennyi elavult IKT-rendszer IKT-kockázatait.

9. cikk

Védelem és megelőzés

(1) Az IKT-rendszerek megfelelő védelme céljából és a válaszintézkedések megszervezése érdekében a pénzügyi szervezetek folyamatosan nyomon követik és ellenőrzik az IKT-rendszerek és -eszközök biztonságát és működését, és minimalizálják az IKT-rendszereket érintő IKT-kockázat hatását megfelelő IKT-biztonsági eszközök, szabályzatok és eljárások bevezetésével.

(2) A pénzügyi szervezetek megtervezik, beszerzik és bevezetik azon IKT-biztonsági stratégiákat, szabályzatokat, eljárásokat, protokollokat és eszközöket, amelyek célja biztosítani az IKT-rendszerek rezilienciáját, folytonosságát és rendelkezésre állását – különös tekintettel azokra, amelyek kritikus vagy fontos funkciókat támogatnak –, továbbá fenntartani az adatok rendelkezésre állására, hitelességére, integritására és bizalmas kezelésére vonatkozó magas szintű normákat, legyen szó használaton kívüli, használatban lévő vagy továbbítás alatt álló adatokról.

(3) A (2) bekezdésben említett célkitűzések elérése érdekében a pénzügyi szervezetek olyan IKT-megoldásokat és -folyamatokat alkalmaznak, amelyek a 4. cikkel összhangban megfelelőek. Az említett IKT-megoldásoknak és -folyamatoknak:

a) garantálniuk kell az adattovábbítási eszközök biztonságát;

b) minimalizálniuk kell az adatsérülés és -vesztés, a jogosulatlan hozzáférés, valamint az üzleti tevékenységet akadályozható technikai hibák kockázatát;

c) meg kell akadályozniuk az adatok rendelkezésre állásának hiányát, hitelességének és integritásának sérülését, bizalmas kezelésének megsértését és az adatvesztést;

d) biztosítaniuk kell az adatoknak az adatgazdálkodás során felmerülő kockázatokkal szembeni védelmét, ideértve a nem megfelelő kezelést, a feldolgozással kapcsolatos kockázatokat és az emberi hibát is.

(4) A 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezetek:

a) információs biztonsági szabályzatot dolgoznak ki és dokumentálnak, amely meghatározza az adatok, az információs vagyonelemek és az IKT-eszközök – ideértve adott esetben az ügyfeleikét is – rendelkezésre állását, hitelességét, integritását és bizalmas kezelését védeni célzó szabályokat;

b) kockázatalapú megközelítést követve, létrehoznak egy megbízható hálózati és infrastruktúra-menedzsment struktúrát, megfelelő technikákat, módszereket és protokollokat alkalmazva, amelyek magukban foglalhatják automatizált mechanizmusok végrehajtását is, az érintett információs vagyonelemek kibertámadás esetén történő elszigetelése érdekében;

c) olyan szabályzatokat hajtanak végre, amelyek az információs vagyonelemekhez és az IKT-eszközökhöz való fizikai vagy logikai hozzáférést kizárólag a jogszerű és jóváhagyott funkciókhoz és tevékenységekhez szükséges mértékűre korlátozzák, és e célból olyan szabályzatokat, eljárásokat és kontrollokat határoznak meg, amelyek szabályozzák a hozzáférés-kezelési jogosultságokat, és biztosítják azok megbízható adminisztrációját;

d) erős hitelesítési mechanizmusokat szolgáló szabályzatokat és protokollokat vezetnek be releváns normák és célzott kontrollrendszerek alapján, valamint a kriptográfiai kulcsokhoz kapcsolódó védelmi intézkedéseket hajtanak végre, ahol az adatok jóváhagyott adatminősítési és IKT-kockázatértékelési folyamatok eredményei alapján kerülnek titkosításra;

e) az IKT-változás többek között a szoftver-, hardver- és belsővezérlőprogram-összetevőket, -rendszert vagy -biztonságot érintő változások kezelését szolgáló, olyan dokumentált szabályzatokat, eljárásokat és kontrollokat vezetnek be, amelyek kockázatértékelési megközelítésen alapulnak, és integráns részét képezik a pénzügyi szervezet általános változásmenedzsment-folyamatának, annak biztosítása érdekében, hogy az IKT-rendszerekben bekövetkező valamennyi változást kontrollált módon rögzítsék, teszteljék, értékeljék, hagyják jóvá, hajtsák végre és ellenőrizzék;

f) megfelelő és átfogó, dokumentált szabályzatokkal rendelkeznek a hibajavító csomagokra és frissítésekre vonatkozóan.

A b) pont első albekezdésének alkalmazásában a pénzügyi szervezetek a hálózati kapcsolati infrastruktúrát azonnali megszakításra vagy szakaszokra bontásra alkalmas módon alakítják ki annak érdekében, hogy minimalizálják és megelőzzék az átterjedést, különösen az összekapcsolt pénzügyi folyamatok esetében.

Az e) pont első albekezdésének alkalmazásában az IKT-vonatkozású változásmenedzsment-folyamatot a megfelelő vezetői szintnek kell jóváhagynia, és annak konkrét protokollokkal kell rendelkeznie.

10. cikk

Észlelés

(1) A pénzügyi szervezeteknek rendelkezniük kell azt lehetővé tevő mechanizmusokkal, hogy a 17. cikknek megfelelően azonnal észleljék a rendellenes tevékenységeket – beleértve az IKT-hálózatok teljesítményproblémáit és az IKT-vonatkozású eseményeket is –, továbbá hogy azonosítsák a potenciális lényeges egyedi meghibásodási pontokat.

Az első albekezdésben említett valamennyi észlelési mechanizmust a 25. cikkel összhangban rendszeresen tesztelnie kell.

(2) Az (1) bekezdésben említett észlelési mechanizmusoknak lehetővé kell tenniük a többszintű kontrollt, valamint meg kell határozniuk az IKT-vonatkozású események válaszfolyamatait kiváltó és elindító riasztási értékhatárokat és kritériumokat, ideértve az automatikus riasztási mechanizmusokat az IKT-vonatkozású eseményekre való reagálásért felelős, releváns személyzet számára.

(3) A pénzügyi szervezeteknek elegendő erőforrásokat és képességeket kell biztosítaniuk a felhasználói tevékenységek, valamint az IKT-vonatkozású rendellenességek és biztonsági események, különösen a kibertámadások előfordulásának nyomon követéséhez.

(4) Az adatszolgáltatóknak ezenkívül rendelkezniük kell olyan rendszerekkel, amelyek eredményesen ellenőrizhetik a kereskedési jelentéseket azok teljeskörűsége szempontjából, azonosíthatják a kihagyásokat és a nyilvánvaló hibákat, és kérhetik az említett jelentések újraküldését.

11. cikk

Reagálás és helyreállítás

(1) A 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként, a 8. cikkben említett azonosítási követelmények alapján a pénzügyi szervezeteknek átfogó IKT-üzletmenetfolytonossági politikát kell bevezetniük, amelyet a pénzügyi szervezet átfogó üzletmenet-folytonossági politikájának integráns részét képező célzott egyedi szabályzatként is elfogadhatnak.

(2) A pénzügyi szervezeteknek az IKT-üzletmenetfolytonossági politikát célzott, megfelelő és dokumentált intézkedések, tervek, eljárások és mechanizmusok útján kell végrehajtaniuk, a következők céljából:

a) a folytonosság biztosítása a pénzügyi szervezet kritikus vagy fontos funkcióinak ellátásában;

b) valamennyi IKT-vonatkozású eseményre gyors, megfelelő és eredményes reagálás és annak megoldása a kár mérséklésével, a tevékenység újraindítását és a helyreállítási intézkedéseket előtérbe helyezve;

c) célzott tervek haladéktalan aktiválása, amelyek lehetővé teszik az IKT-vonatkozású események egyes típusainak megfelelő, elszigetelésre irányuló intézkedések, folyamatok és technológiák alkalmazását, a további károk megelőzését, valamint a 12. cikkel összhangban kialakított célzott reagálási és helyreállítási intézkedéseket;

d) előzetes hatások, károk és veszteségek felmérése;

e) olyan kommunikációs és válságkezelési intézkedések meghatározása, amelyek biztosítják a naprakész információk eljuttatását a releváns belső személyzet valamennyi tagja és valamennyi külső érdekelt fél részére a 14. cikk, valamint az illetékes hatóságok részére a 19. cikk szerint.

(3) A 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezeteknek kapcsolódó IKT-vonatkozású reagálási és helyreállítási terveket kell bevezetniük, amelyeket a mikrovállalkozásnak nem minősülő pénzügyi szervezetek esetében független belső felülvizsgálatnak kell alávetni.

(4) A pénzügyi szervezeteknek – különösen a harmadik fél IKT-szolgáltatókkal kötött megállapodások keretében kiszervezett vagy megbízásba adott kritikus vagy lényeges funkciókra vonatkozóan – megfelelő IKT-üzletmenetfolytonossági terveket kell bevezetniük és fenntartaniuk, amelyeket időszakonként tesztelniük kell.

(5) Az átfogó üzletmenet-folytonossági politika részeként a pénzügyi szervezeteknek üzleti hatáselemzést (BIA) kell végezniük az üzletmenetben okozott súlyos zavaroknak való kitettségükről. Az üzleti hatáselemzés keretében a pénzügyi szervezeteknek mennyiségi és minőségi kritériumok alapján értékelniük kell az üzletmenetben okozott súlyos zavarok lehetséges hatását, adott esetben belső és külső adatok és forgatókönyv-elemzés felhasználásával. Az üzleti hatáselemzésnek tekintetbe kell vennie az azonosított és felvázolt üzleti funkcióknak, támogatási folyamatoknak, harmadik felektől való függőségeknek és információs vagyonelemeknek, valamint azok kölcsönös függőségeinek a kritikusságát. A pénzügyi szervezeteknek biztosítaniuk kell, hogy az IKT-eszközöket és IKT-szolgáltatásokat az üzleti hatáselemzéssel teljes összhangban alakítsák ki és használják, különösen valamennyi kritikus összetevő redundanciájának megfelelő biztosítása tekintetében.

(6) Átfogó IKT-kockázatkezelésük keretében a pénzügyi szervezeteknek:

a) tesztelniük kell az IKT-üzletmenetfolytonossági terveket és az IKT-reagálási és -helyreállítási terveket a valamennyi funkciót támogató IKT-rendszerekhez kapcsolódóan legalább évente, valamint a kritikus vagy fontos funkciókat támogató IKT-rendszereket érintő bármely jelentős változás bekövetkezése esetén;

b) tesztelniük kell a 14. cikknek megfelelően kialakított válsághelyzeti kommunikációs terveket.

Az első albekezdés a) pontjának alkalmazásában a mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek a tesztelési terveikben szerepeltetniük kell a kibertámadásokra, továbbá az elsődleges IKT-infrastruktúrájuk és a 12. cikkben meghatározott kötelezettségek teljesítéséhez szükséges tartalékkapacitás, biztonsági mentések és tartalékeszközök közötti átállásokra vonatkozó forgatókönyveket.

A pénzügyi szervezeteknek rendszeresen felül kell vizsgálniuk az IKT-üzletmenetfolytonossági politikájukat, valamint az IKT-reagálási és -helyreállítási terveiket, figyelembe véve az első albekezdés szerint elvégzett tesztek eredményeit, valamint az ellenőrzések és felügyeleti felülvizsgálatok alapján megfogalmazott ajánlásokat.

(7) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek olyan válságkezelési funkcióval kell rendelkezniük, amely az IKT-üzletmenet-folytonossági terveik vagy az IKT-reagálási és helyreállítási terveik aktiválása esetén a 14. cikkel összhangban többek között egyértelmű eljárásokat határoz meg a belső és külső válsághelyzeti kommunikáció kezelésére vonatkozóan.

(8) A pénzügyi szervezeteknek az olyan, zavart okozó eseményeket megelőzően és azok időtartama alatt végzett tevékenységekről, amikor az IKT-üzletmenetfolytonossági terveik és az IKT-reagálási és -helyreállítási terveik aktiválására kerül sor, könnyen hozzáférhető nyilvántartást kell vezetniük.

(9) A központi értéktáraknak az illetékes hatóságok rendelkezésére kell bocsátaniuk az IKT-vonatkozású üzletmenet-folytonossági tesztek vagy hasonló műveletek eredményeinek másolatát.

(10) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek az illetékes hatóságok kérésére jelentést kell tenniük a jelentős IKT-vonatkozású események által okozott költségek és veszteségek összesített éves becsléséről.

(11) Az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 16. cikkével összhangban az EFH-knak a vegyes bizottság keretében 2024. július 17-ig közös iránymutatásokat kell kidolgozniuk a (10) bekezdésben említett költségek és veszteségek összesített éves becslésére vonatkozóan.

12. cikk

Biztonsági mentési szabályzatok és eljárások, visszaállítási és helyreállítási eljárások és módszerek

(1) Annak biztosítása céljából, hogy IKT-rendszereiket és adataikat minimális leállási időt, valamint korlátozott mértékű zavart és veszteséget követően állíthassák helyre, a pénzügyi szervezeteknek – IKT-kockázatkezelési keretrendszerük részeként – ki kell dolgozniuk és dokumentálniuk kell a következőket:

a) olyan biztonsági mentési szabályzatok és eljárások, amelyek az információk kritikussága vagy az adatok bizalmassági szintje alapján meghatározzák a biztonsági mentéssel érintett adatok körét és a biztonsági mentés minimális gyakoriságát;

b) visszaállítási és helyreállítási eljárások és módszerek.

(2) A pénzügyi szervezeteknek létre kell hozniuk biztonsági mentési rendszereket, amelyek aktiválhatók a biztonsági mentési szabályzatoknak és eljárásoknak megfelelően, valamint a visszaállítási és helyreállítási eljárásokat és módszereket. A biztonsági mentési rendszerek aktiválása nem veszélyeztetheti a hálózati és információs rendszerek biztonságát, vagy az adatok rendelkezésre állását, hitelességét, integritását vagy bizalmas kezelését. A biztonsági mentési eljárásokat, valamint a visszaállítási és helyreállítási eljárásokat és módszereket időszakonként tesztelni kell.

(3) Az adatok biztonsági mentés alapján, saját rendszerekkel végzett helyreállításához a pénzügyi szervezeteknek olyan IKT-rendszereket kell használniuk, amelyek fizikailag és logikailag elkülönülnek a forrásoldali IKT-rendszertől. Az IKT-rendszereket védeni kell minden illetéktelen hozzáféréssel vagy IKT-sérüléssel szemben, és lehetővé kell tenni a szolgáltatások időben történő visszaállítását az adatok és a rendszer biztonsági mentéseinek szükség szerinti felhasználásával.

A központi szerződő felek esetében a helyreállítási terveknek lehetővé kell tenniük a zavar bekövetkezésekor folyamatban lévő valamennyi tranzakció helyreállítását, hogy a központi szerződő fél biztonsággal folytatni tudja működését, és a tervezett időben le tudja zárni az ügyleteket.

Az adatszolgáltatóknak emellett megfelelő erőforrásokat kell fenntartaniuk, valamint biztonsági mentési és helyreállítási eszközökkel kell rendelkezniük annak érdekében, hogy mindenkor kínálhassák és fenntarthassák szolgáltatásaikat.

(4) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek olyan IKT-tartalékkapacitásokat kell fenntartaniuk, amelyek biztosítják az üzleti igények ellátásához elégséges és megfelelő erőforrásokat, képességeket és funkciókat. A mikrovállalkozásoknak kockázati profiljukat alapul véve, mérlegelniük kell, hogy szükséges-e ilyen IKT-tartalékkapacitásokat fenntartaniuk.

(5) A központi értéktáraknak fenn kell tartaniuk legalább egy másodlagos adatfeldolgozó helyszínt, amely rendelkezik az üzleti igényeik ellátásához szükséges megfelelő erőforrásokkal, képességekkel, funkciókkal és személyi feltételekkel.

A másodlagos adatfeldolgozási helyszínnek:

a) olyan földrajzi távolságra kell elhelyezkednie az elsődleges adatfeldolgozási helyszíntől, amely biztosítja, hogy attól elkülönülő kockázati profillal rendelkezzen, és ne érintsék az elsődleges helyszínt érintő esemény hatásai;

b) képesnek kell lennie arra, hogy biztosítsa a kritikus vagy fontos funkcióknak az elsődleges helyszínnel azonos folytonosságát, vagy az ahhoz szükséges szolgáltatási szintet, hogy a pénzügyi szervezet működési folyamatai teljesítsék a helyreállítási célkitűzéseket;

c) azonnal elérhetőnek kell lennie a pénzügyi szervezet személyzete számára, biztosítandó a kritikus vagy fontos funkciók folytonosságát abban az esetben, ha az elsődleges adatfeldolgozási helyszín elérhetetlenné vált.

(6) Az egyes funkciókhoz kapcsolódó helyreállítási időre és helyreállítási pontra vonatkozó célkitűzések megállapításakor a pénzügyi szervezeteknek figyelembe kell venniük, hogy kritikus vagy fontos funkcióról van-e szó, valamint a piaci hatékonyságra potenciálisan gyakorolt általános hatást. Az ilyen, időre vonatkozó célkitűzéseknek biztosítaniuk kell a megállapodás szerinti szolgáltatási szintek teljesítését rendkívüli helyzetekben.

(7) IKT-vonatkozású eseményt követő helyreállítás során a pénzügyi szervezeteknek el kell végezniük a szükséges ellenőrzéseket – ideértve az esetleges többszörös ellenőrzést és adategyeztetést –, hogy fenntartsák az adatok legmagasabb szintű integritását. A szervezeteknek az adatok külső érdekelti forrásból való rekonstruálása esetén is el kell végezniük ezen ellenőrzéseket, hogy biztosítsák valamennyi adat rendszerek közötti következetességét.

13. cikk

Tanulás és alkalmazkodás

(1) A pénzügyi szervezeteknek rendelkezniük kell képességekkel és személyzettel ahhoz, hogy információkat gyűjtsenek a sérülékenységekről és kiberfenyegetésekről, valamint az IKT-vonatkozású eseményekről – különösen a kibertámadásokról –, és elemezzék azok valószínű hatását a szervezet digitális működési rezilienciájára.

(2) A pénzügyi szervezetek az alaptevékenységeiket megzavaró, jelentős IKT-vonatkozású eseményeket követően elvégzik az IKT-vonatkozású események utólagos felülvizsgálatát, elemezve a zavar okait, és azonosítva az IKT-műveletekben vagy a 11. cikkben említett IKT-üzletmenetfolytonossági politikában teendő szükséges javításokat.

A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek kérésre tájékoztatniuk kell az illetékes hatóságokat az IKT-vonatkozású események első albekezdésben említett utólagos felülvizsgálatát követően végrehajtott változásokról.

Az IKT-vonatkozású események első albekezdésben említett utólagos felülvizsgálata keretében meg kell állapítani, hogy a kialakított eljárásokat követték-e, és a megtett intézkedések eredményesek voltak-e többek között a következők vonatkozásában:

a) a biztonsági riasztásokra való reagálásnak, valamint az IKT-vonatkozású események hatása és súlyossága megállapításának a gyorsasága;

b) adott esetben az igazságügyi szakértői elemzés elvégzésének minősége és sebessége;

c) a biztonsági események pénzügyi szervezeten belüli eszkalációjának eredményessége;

d) a belső és külső kommunikáció eredményessége.

(3) A digitális működési reziliencia 26. és 27. cikkel összhangban végzett tesztéséből, a valós IKT-vonatkozású eseményekből, ezen belül különösen a kibertámadásokból, továbbá az IKT-üzletmenetfolytonossági tervek és az IKT-reagálási és -helyreállítási tervek aktiválása során felmerült kihívásokból, valamint a partnerekkel kicserélt és a felügyeleti felülvizsgálatok során értékelt információkból származó tapasztalatokat a szervezetnek megfelelően és folyamatosan be kell építenie az IKT-kockázatértékelés folyamatába. Az említett megállapítások képezik a 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer releváns összetevői megfelelő felülvizsgálatának alapját.

(4) A pénzügyi szervezetek nyomon követik a 6. cikk (8) bekezdésében meghatározott, a digitális működési rezilienciára vonatkozó stratégiájuk végrehajtásának eredményességét. Felvázolják az IKT-kockázat időbeli alakulását, elemzik az IKT-vonatkozású események – így különösen a kibertámadások és mintázataik – gyakoriságát, típusait, nagyságát és alakulását, abból a célból, hogy megértsék az IKT-kockázati kitettség szintjét – különösen a kritikus vagy fontos funkciókkal kapcsolatban –, és javítsák a pénzügyi szervezet kiberbiztonsági érettségét és felkészültségét.

(5) A vezető IKT-munkatársaknak legalább évente be kell számolniuk a vezető testületnek a (3) bekezdésben említett megállapításokról, és javaslatokat kell előterjeszteniük.

(6) A pénzügyi szervezeteknek a személyzetük képzési rendszerének részét képező kötelező modulokként IKT-biztonsági tudatosságot elősegítő programokat és a digitális működési rezilienciával kapcsolatos képzéseket kell kidolgozniuk. Az említett programok és képzések valamennyi munkavállalóra és a felső vezetés valamennyi tagjára alkalmazandók, és azok összetettségi szintjét a munkavállalók feladatköreihez kell igazítani. Adott esetben a pénzügyi szervezeteknek harmadik fél IKT-szolgáltatókat is be kell vonniuk a releváns képzési programjaikba a 30. cikk (2) bekezdésének i) pontjával összhangban.

(7) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek folyamatosan nyomon kell követniük a releváns technológiai fejleményeket többek között annak megértése céljából, hogy az új technológiák bevezetésének milyen hatása lehet az IKT-biztonsági követelményekre és a digitális működési rezilienciára. Lépést kell tartaniuk a legkorszerűbb IKT-kockázatkezelési folyamatokkal, hogy eredményesen léphessenek fel a kibertámadások meglévő és új formáival szemben.

14. cikk

Kommunikáció

(1) A 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezeteknek válsághelyzeti kommunikációs tervvel kell rendelkezniük, amely legalább a jelentős IKT-vonatkozású eseményekről és sérülékenységekről lehetővé teszi az ügyfelek, partnerek, valamint adott esetben a nyilvánosság felelős tájékoztatását.

(2) Az IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezeteknek a saját személyzetükre és a külső érdekeltekre vonatkozó kommunikációs szabályzatot kell bevezetniük. A személyzetre vonatkozó kommunikációs szabályzatban figyelembe kell venni annak szükségességét, hogy különbséget tegyenek az IKT-kockázatkezelésért, különösen a reagálásért és helyreállításért felelős munkatársak, valamint a tájékoztatást igénylő munkatársak között.

(3) A pénzügyi szervezeten belül legalább egy személyt meg kell bízni az IKT-vonatkozású eseményekre vonatkozó kommunikációs stratégia végrehajtásával, akinek e célból a nyilvánossággal és a médiával kapcsolatos feladatot is el kell látnia.

15. cikk

Az IKT-kockázatkezelési eszközök, módszerek, folyamatok és szabályzatok további harmonizációja

Az EFH-knak a vegyes bizottság keretében, az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA) egyeztetve. közös szabályozástechnikai standardtervezeteket kell kidolgozniuk annak érdekében, hogy:

a) meghatározzák azon további elemeket, amelyeket a 9. cikk (2) bekezdésében említett IKT-biztonsági szabályzatoknak, eljárásoknak, protokolloknak és eszközöknek tartalmazniuk kell a hálózatok biztonságának garantálása, a behatolások és az adatokkal való visszaélés elleni megfelelő biztosítékok lehetővé tétele, az adatok rendelkezésre állásának, hitelességének, integritásának és bizalmas jellegének többek között kriptográfiai technikákkal történő megőrzése, továbbá a garantáltan pontos és gyors, jelentős zavaroktól és indokolatlan késedelemtől mentes adattovábbítás érdekében;

b) kidolgozzák a hozzáférés-kezelési jogosultságokra vonatkozó, a 9. cikk (4) bekezdésének c) pontjában említett kontrollok további összetevőit és a kapcsolódó humánerőforrás-politikát, amely meghatározza a hozzáférési jogosultságokat, a jogosultságok kiosztására és visszavonására, az IKT-kockázattal kapcsolatos rendellenes magatartásformák megfelelő többek között hálózathasználati mintákra, időbeosztásra, IT-tevékenységre és ismeretlen eszközökre vonatkozó mutatókon keresztül történő nyomon követésére vonatkozó eljárásokat;

c) részletesen kidolgozzák a 10. cikk (1) bekezdésében meghatározott, a rendellenes tevékenységek azonnali észlelésére szolgáló mechanizmusokat, valamint a 10. cikk (2) bekezdésében megállapított azon kritériumokat, amelyek alapján az IKT-vonatkozású események észlelési és válaszfolyamatainak beindítására sor kerül;

d) részletesen meghatározzák a 11. cikk (1) bekezdésében említett IKT-üzletmenetfolytonossági politika összetevőit;

e) részletesen meghatározzák az IKT-üzletmenetfolytonossági tervek 11. cikk (6) bekezdésében említett tesztelését annak biztosítására, hogy az ilyen tesztelés kellőképpen figyelembe vegyen olyan forgatókönyveket, amelyek szerint egy kritikus vagy lényeges funkció ellátása elfogadhatatlan színvonalúra csökken vagy meghiúsul, és kellőképpen tekintetbe vegye bármely releváns harmadik fél IKT-szolgáltató fizetésképtelenségének vagy egyéb hiányosságainak potenciális hatásait, valamint adott esetben a vonatkozó szolgáltatók joghatósági területén fennálló politikai kockázatokat;

f) részletesen meghatározzák a 11. cikk (3) bekezdésében említett IKT-reagálási és -helyreállítási tervek összetevőit;

g) részletesen meghatározzák a 6. cikk (5) bekezdésében említett, az IKT-kockázatkezelési keretrendszer felülvizsgálatáról szóló jelentés tartalmát és formátumát.

Az említett szabályozástechnikai standardtervezetek kidolgozása során az európai felügyeleti hatóságoknak figyelembe kell venniük a pénzügyi szervezet méretét és általános kockázati profilját, valamint szolgáltatásainak, tevékenységeinek és műveleteinek jellegét, nagyságrendjét és összetettségét, ugyanakkor kellően tekintetbe kell venniük a különböző pénzügyi szolgáltatási ágazatokban végzett tevékenységek eltérő jellegéből eredő sajátos jellemzőket.

Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. január 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban az első bekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

16. cikk

Egyszerűsített IKT-kockázatkezelési keretrendszer

(1) E rendelet 5–15. cikke nem alkalmazandó a következőkre: az (EU) 2015/2366 irányelv alapján mentesített kis méretű és össze nem kapcsolt befektetési vállalkozások, pénzforgalmi intézmények; a 2013/36/EU irányelv alapján mentesített azon intézmények, amelyek tekintetében a tagállamok úgy döntöttek, hogy nem alkalmazzák az e rendelet 2. cikkének (4) bekezdésében említett opciót; a 2009/110/EK irányelv alapján mentesített elektronikuspénz-kibocsátó intézmények; és a kis méretű foglalkoztatói nyugellátást szolgáltató intézmények.

Az első albekezdés sérelme nélkül az első albekezdésben felsorolt szervezeteknek:

a) megbízható és dokumentált IKT-kockázatkezelési keretrendszert kell létrehozniuk és fenntartaniuk, amely részletezi az IKT-kockázat gyors, hatékony és átfogó kezelését célzó mechanizmusokat és intézkedéseket, többek között a releváns fizikai összetevők és infrastruktúrák védelme érdekében;

b) folyamatosan nyomon kell követniük valamennyi IKT-rendszer biztonságát és működését;

c) minimalizálniuk kell az IKT-kockázat hatását olyan megbízható, reziliens és naprakész IKT-rendszerek, -protokollok és -eszközök alkalmazásával, amelyek alkalmasak tevékenységeik végzésének és a szolgáltatások nyújtásának támogatására, valamint a hálózati és információs rendszerekben tárolt adatok rendelkezésre állásának, hitelességének, integritásának és bizalmas jellegének megfelelő fenntartására;

d) lehetővé kell tenniük a hálózati és információs rendszerekben jelentkező IKT-kockázat és -rendellenességek forrásainak azonnali azonosítását és felderítését, valamint az IKT-vonatkozású események gyors kezelését;

e) azonosítaniuk kell a harmadik fél IKT-szolgáltatóktól való főbb függőségeket;

f) biztosítaniuk kell a kritikus vagy lényeges funkciók folytonosságát olyan üzletmenet-folytonossági tervek, valamint reagálási és helyreállítási intézkedések révén, amelyek magukban foglalják legalább a biztonsági mentést és helyreállítást biztosító intézkedéseket;

g) rendszeresen tesztelniük kell az f) pontban említett terveket és intézkedéseket, valamint az a) és c) pontnak megfelelően végrehajtott kontrollok hatékonyságát;

h) adott esetben be kell építeniük az IKT-kockázatértékelési folyamatba a g) pontban említett tesztekből és a biztonsági események utólagos elemzéséből származó releváns operatív következtetéseket, és az igényeknek és az IKT-kockázati profilnak megfelelően IKT-biztonsági tudatosságnövelő programokat és digitális működési reziliencia-képzéseket kell kidolgozniuk a személyzet és a vezetés számára.

(2) Az (1) bekezdés második albekezdésének a) pontjában említett IKT-kockázatkezelési keretrendszert dokumentálni kell, és a felügyeleti utasításoknak megfelelően időszakonként és minden jelentős IKT-vonatkozású esemény bekövetkezésekor felül kell vizsgálni. A keretet folyamatosan fejleszteni kell a végrehajtás és a nyomon követés során szerzett tapasztalatok alapján. Az illetékes hatóság számára – a kérésére – jelentést kell benyújtani az IKT-kockázatkezelési keretrendszer felülvizsgálatáról.

(3) Az EFH-knak a vegyes bizottság keretében, az ENISA-val egyeztetve, közös szabályozástechnikai standardtervezeteket kell kidolgozniuk annak érdekében, hogy:

a) részletesen meghatározzák az (1) bekezdés második albekezdésének a) pontjában említett IKT-kockázatkezelési keretrendszerbe foglalandó elemeket;

b) részletesen meghatározzák az (1) bekezdés második albekezdésének c) pontjában említett, az IKT-kockázat hatásának minimalizálását szolgáló rendszerekkel, protokollokkal és eszközökkel kapcsolatos elemeket a hálózatok biztonságának garantálása érdekében, lehetővé téve a behatolások és az adatokkal való visszaélés elleni megfelelő biztosítékokat, valamint megőrizve az adatok rendelkezésre állását, hitelességét, integritását és bizalmas jellegét;

c) részletesen meghatározzák az (1) bekezdés második albekezdésének f) pontjában említett IKT-üzletmenetfolytonossági tervek összetevőit;

d) részletesen meghatározzák az üzletmenet-folytonossági tervek tesztelésére vonatkozó szabályokat, és biztosítsák az (1) bekezdés második albekezdésének g) pontjában említett kontrollok hatékonyságát, és biztosítsák, hogy az ilyen tesztelés során kellő figyelmet kapjanak az olyan helyzetek, amikor egy kritikus vagy fontos funkció ellátása elfogadhatatlan színvonalúra csökken vagy meghiúsul;

e) részletesen meghatározzák a (2) bekezdésben említett, az IKT-kockázatkezelési keretrendszer felülvizsgálatáról szóló jelentés tartalmát és formátumát.

Az említett szabályozástechnikai standardtervezetek kidolgozása során az EFH-knak figyelembe kell venniük a pénzügyi szervezet méretét és általános kockázati profilját, valamint szolgáltatásai, tevékenységei és műveletei jellegét, nagyságrendjét és összetettségét.

Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. január 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban az első albekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

III. FEJEZET

Az IKT-vonatkozású események kezelése, osztályozása és bejelentése

17. cikk

Az IKT-vonatkozású események kezelési folyamata

(1) A pénzügyi szervezeteknek meg kell határozniuk, ki kell alakítaniuk és végre kell hajtaniuk az IKT-vonatkozású események észlelésére, kezelésére és bejelentésére szolgáló folyamatot.

(2) A pénzügyi szervezetek nyilvántartanak valamennyi IKT-vonatkozású eseményt és jelentős kiberfenyegetést. A pénzügyi szervezetek megfelelő eljárásokat és folyamatokat alakítanak ki, hogy biztosítsák az IKT-vonatkozású események következetes és integrált monitorozását, kezelését és utókövetését, biztosítsák a kiváltó okok azonosítását, dokumentálását és kezelését az ilyen események előfordulásának megelőzése érdekében.

(3) Az IKT-vonatkozású események (1) bekezdésben említett kezelési folyamata keretében:

a) korai előrejelző mutatókat kell bevezetni;

b) a 18. cikk (1) bekezdésében meghatározott kritériumok alapján meg kell határozni az IKT-vonatkozású események azonosítását, nyomon követését, naplózását, kategorizálását és osztályozását biztosító, az események prioritásának és súlyosságának és az érintett szolgáltatások kritikusságának megfelelő eljárásokat;

c) ki kell jelölni azon szerep- és felelősségi köröket, amelyeket az IKT-vonatkozású események egyes típusai és forgatókönyvei tekintetében aktiválni kell;

d) meg kell határozni a személyzettel, a külső érdekelt felekkel és a médiával a 14. cikkel összhangban folytatott kommunikációra, az ügyfelek értesítésére, a belső eszkalációs eljárásokra – ideértve az IKT-vonatkozású ügyfélpanaszok kezelését is –, továbbá adott esetben a partner pénzügyi szervezetek tájékoztatására vonatkozó terveket;

e) biztosítani kell, hogy legalább a jelentős IKT-vonatkozású eseményeket bejelentik a releváns felső vezetésnek, és tájékoztatni kell a vezető testületet legalább a jelentős IKT-vonatkozású eseményekről, ismertetve az ilyen IKT-vonatkozású események eredményeként megállapítandó hatást, reagálást és további kontrollokat;

f) meg kell határozni az IKT-vonatkozású eseményekre való reagálást célzó eljárásokat a hatások enyhítése, valamint annak biztosítása érdekében, hogy a szolgáltatások mielőbb működőképessé és biztonságossá váljanak.

18. cikk

Az IKT-vonatkozású események és a kiberfenyegetések osztályozása

(1) A pénzügyi szervezeteknek a következő kritériumok alapján kell osztályozniuk az IKT-vonatkozású eseményeket, és megállapítaniuk azok hatását:

a) az IKT-vonatkozású esemény által érintett ügyfelek vagy pénzügyi partnerek száma és/vagy relevanciája, és – adott esetben – az érintett tranzakciók mennyisége vagy száma, valamint az, hogy az IKT-vonatkozású eseménynek van-e a hírnevet érintő hatása;

b) az IKT-vonatkozású esemény időtartama, beleértve a leállási időt is;

c) az IKT-vonatkozású esemény földrajzi kiterjedése az érintett területek vonatkozásában, különösen, ha az esemény kettőnél több tagállamot érint;

d) az IKT-vonatkozású eseménnyel járó adatvesztések az adatok rendelkezésre állásához, hitelességéhez, integritásához vagy bizalmas jellegéhez kapcsolódóan;

e) az érintett szolgáltatások kritikussága, beleértve a pénzügyi szervezet ügyleteit és működését is;

f) az IKT-vonatkozású esemény gazdasági hatása – ideértve különösen a közvetlen és közvetett költségeket és veszteségeket – abszolút és relatív értelemben egyaránt.

(2) A pénzügyi szervezetek a kiberfenyegetéseket jelentősnek minősítik a kockázatnak kitett szolgáltatások kritikussága alapján, ideértve a pénzügyi szervezet ügyleteit és műveleteit, a megcélzott ügyfelek vagy pénzügyi partnerek számát és/vagy relevanciáját, valamint a kockázatnak kitett területek földrajzi eloszlását.

(3) Az EFH-knak a vegyes bizottság keretében, az EKB-val és az ENISA-val egyeztetve, közös szabályozástechnikai standardtervezeteket kell kidolgozniuk, amelyekben részletesen meghatározzák a következőket:

a) az (1) bekezdésben meghatározott kritériumok, ideértve azon lényegességi küszöbértékeket, amelyek alapján megállapíthatók azon jelentős IKT-vonatkozású események, vagy adott esetben jelentős pénzforgalmi vonatkozású működési vagy biztonsági események, amelyek a 19. cikk (1) bekezdésében előírt bejelentési kötelezettség alá tartoznak;

b) azon kritériumok, amelyek alapján az illetékes hatóságok értékelik a jelentős IKT-vonatkozású események vagy adott esetben a jelentős pénzforgalmi vonatkozású működési vagy biztonsági események relevanciáját más tagállamokban a releváns illetékes hatóságok szempontjából, továbbá a jelentős IKT-vonatkozású eseményekkel vagy adott esetben a jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményekkel kapcsolatos bejelentések azon részletei, amelyeket a 19. cikk (6) és (7) bekezdésének megfelelően meg kell osztaniuk más illetékes hatóságokkal;

c) az e cikk (2) bekezdésében meghatározott kritériumok, beleértve a jelentős kiberfenyegetések meghatározására vonatkozó, magasnak minősülő lényegességi küszöbértékeket.

(4) Az e cikk (3) bekezdésében említett közös szabályozástechnikai standardtervezetek kidolgozása során az EFH-knak figyelembe kell venniük a 4. cikk (2) bekezdésében meghatározott kritériumokat, valamint a nemzetközi szabványokat, az ENISA által kidolgozott és közzétett iránymutatásokat és specifikációkat, ideértve adott esetben a más gazdasági ágazatokra vonatkozó specifikációkat is. A 4. cikk (2) bekezdésében meghatározott kritériumok alkalmazása céljából az EFH-knak megfelelően figyelembe kell venniük a mikrovállalkozások és a kis- és középvállalkozások azon igényét, hogy elegendő erőforrást és kapacitást mozgósítsanak az IKT-vonatkozású események gyors kezelésének biztosítása érdekében.

Az EFH-knak az említett közös szabályozástechnikai standardtervezeteket 2024. január 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban a (3) bekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

19. cikk

A jelentős IKT-vonatkozású események bejelentése és a jelentős kiberfenyegetésekről szóló önkéntes értesítés

(1) A pénzügyi szervezeteknek a jelentős IKT-vonatkozású eseményeket az e cikk (4) bekezdésével összhangban be kell jelenteniük a 46. cikkben említett releváns illetékes hatóságnak.

Amennyiben egy pénzügyi szervezet a 46. cikkben említett illetékes nemzeti hatóságok közül egynél több felügyelete alá tartozik, a tagállamok egyetlen illetékes hatóságot jelölnek ki az e cikkben előírt funkciók és kötelezettségek végrehajtásáért felelős releváns illetékes hatóságként.

Az 1024/2013/EU rendelet 6. cikkének (4) bekezdésével összhangban jelentősnek minősített hitelintézetek bejelentik a jelentős IKT-vonatkozású eseményeket a 2013/36/EU irányelv 4. cikkével összhangban kijelölt releváns illetékes nemzeti hatóságnak, amely haladéktalanul továbbítja az említett jelentést az EKB-nak.

Az első albekezdés alkalmazásában a pénzügyi szervezeteknek a releváns információk összegyűjtését és elemzését követően a 20. cikkben említett sablonok felhasználásával el kell készíteniük az e cikk (4) bekezdésében említett kezdeti értesítést és jelentéseket, és be kell nyújtaniuk azokat az illetékes hatóságnak. Abban az esetben, ha technikai okokból lehetetlen a kezdeti értesítés mintadokumentum használatával történő benyújtása, a pénzügyi szervezeteknek alternatív módon kell értesíteniük arról az illetékes hatóságot.

A (4) bekezdésben említett kezdeti értesítésnek és jelentéseknek tartalmazniuk kell minden olyan információt, amelyre az illetékes hatóságnak szüksége van a jelentős IKT-vonatkozású esemény jelentőségének megállapításához és esteleges határokon átnyúló hatásainak értékeléséhez.

A pénzügyi szervezet által a releváns illetékes hatóság felé történő, az első albekezdés alapján történő bejelentés sérelme nélkül a tagállamok megállapíthatják továbbá, hogy a pénzügyi szervezetek egy részének vagy mindegyikének az e cikk (4) bekezdésében említett kezdeti értesítést és minden egyes jelentést be kell nyújtaniuk a 20. cikkben említett sablonok felhasználásával az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságoknak vagy számítógép-biztonsági eseményekre reagáló csoportoknak (CSIRT-ek) is.

(2) A pénzügyi szervezetek önkéntes alapon értesíthetik a releváns illetékes hatóságot a jelentős kiberfenyegetésekről, amennyiben úgy ítélik meg, hogy a fenyegetés relevanciával bír a pénzügyi rendszer, a szolgáltatás igénybevevői vagy az ügyfelek számára. A releváns illetékes hatóság átadhatja az ilyen információkat a (6) bekezdésben említett egyéb releváns hatóságoknak.

Az 1024/2013/EU rendelet 6. cikkének (4) bekezdésével összhangban jelentősnek minősített hitelintézetek önkéntes alapon értesíthetik a jelentős kiberfenyegetésekről a 2013/36/EU irányelv 4. cikkével összhangban kijelölt, releváns illetékes nemzeti hatóságot, amelynek haladéktalanul továbbítania kell az értesítést az EKB-nak.

A tagállamok dönthetnek úgy, hogy azon pénzügyi szervezetek, amelyek az első albekezdéssel összhangban önkéntes alapon értesítést küldenek, az említett értesítést az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott CSIRT-eknek is továbbíthatják.

(3) Amennyiben jelentős IKT-vonatkozású esemény következik be, és hatással van az ügyfelek pénzügyi érdekeire, a pénzügyi szervezeteknek – amint az eseményt észlelik – indokolatlan késedelem nélkül tájékoztatniuk kell az ügyfeleiket a jelentős IKT-vonatkozású eseményről és az ilyen esemény káros hatásainak enyhítésére tett intézkedésekről.

Jelentős kiberfenyegetés esetén a pénzügyi szervezeteknek adott esetben tájékoztatniuk kell a potenciálisan érintett ügyfeleiket minden olyan megfelelő védelmi intézkedésről, amelyek meghozatalát az utóbbiak mérlegelhetik.

(4) A pénzügyi szervezeteknek a 20. cikk első bekezdése a) pontjának ii. alpontjával összhangban megállapítandó határidőkön belül be kell nyújtaniuk a releváns illetékes hatóságnak a következőket:

a) kezdeti értesítés;

b) időközi jelentés az a) pontban említett kezdeti értesítést követően, amint az eredeti biztonsági esemény állapota jelentősen megváltozik, vagy a jelentős IKT-vonatkozású esemény kezelése a rendelkezésre álló új információk alapján módosul, amelyet adott esetben aktualizált bejelentéseknek kell követniük minden olyan alkalommal, amikor releváns állapotfrissítés áll rendelkezésre, valamint az illetékes hatóság külön kérésére;

c) zárójelentés, amikor lezárult a kiváltó okok elemzése, függetlenül attól, hogy enyhítő intézkedések végrehajtására sor került-e már, és amikor rendelkezésre állnak a hatással kapcsolatban a becslések helyettesítésére alkalmas tényadatok.

(5) A pénzügyi szervezetek az uniós és nemzeti ágazati jogszabályokkal összhangban kiszervezhetik az e cikk szerinti bejelentési kötelezettségeket harmadik fél szolgáltatónak. Az ilyen kiszervezés esetén a pénzügyi szervezet továbbra is teljes felelősséggel tartozik a biztonsági eseményre vonatkozó bejelentési követelmények teljesítéséért.

(6) A (4) bekezdésben említett kezdeti értesítés és minden egyes jelentés átvételét követően az illetékes hatóságnak kellő időben részletes tájékoztatást kell nyújtania a jelentős IKT-vonatkozású eseményről a következő címzetteknek – adott esetben – a vonatkozó hatáskörük alapján:

a) az EBH, az ESMA vagy az EIOPA;

b) a 2. cikk (1) bekezdésének a), b) és d) pontjában említett pénzügyi szervezetek esetében az EKB;

c) az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságok, egyedüli kapcsolattartó pontok vagy CSIRT-ek;

d) a 2014/59/EU irányelv 3. cikkében említett szanálási hatóságok és az Egységes Szanálási Testület (ESZT) a 806/2014/EU európai parlamenti és tanácsi rendelet ([37]) 7. cikkének (2) bekezdésében említett szervezetek, valamint a 806/2014/EU rendelet 7. cikke (4) bekezdésének b) pontjában és (5) bekezdésében említett szervezetek és csoportok tekintetében, ha az ilyen adatok olyan eseményekre vonatkoznak, amelyek kockázatot jelentenek a 2014/59/EU irányelv 2. cikkének 35. pontja értelmében vett kritikus funkciók biztosítására nézve; és

e) a nemzeti jog szerinti egyéb releváns hatóságok.

(7) Az információk (6) bekezdés szerinti kézhezvételét követően az EBH, az ESMA vagy az EIOPA, valamint az EKB – az ENISA-val egyeztetve és a releváns illetékes hatósággal együttműködve – értékeli, hogy a jelentős IKT-vonatkozású esemény releváns-e más tagállamok illetékes hatóságai számára. Az említett értékelést követően az EBH, az ESMA vagy az EIOPA ennek megfelelően a lehető leghamarabb értesíti más tagállamokban a releváns illetékes hatóságokat. Az EKB értesítést küld a Központi Bankok Európai Rendszere tagjainak a fizetési rendszer szempontjából releváns kérdésekről. Az értesítés alapján az illetékes hatóságoknak adott esetben meg kell hozniuk minden szükséges intézkedést a pénzügyi rendszer közvetlen stabilitásának megóvása érdekében.

([37]) Az Európai Parlament és a Tanács 806/2014/EU rendelete (2014. július 15.) a hitelintézeteknek és bizonyos befektetési vállalkozásoknak az Egységes Szanálási Mechanizmus keretében történő szanálására vonatkozó egységes szabályok és egységes eljárás kialakításáról, valamint az Egységes Szanálási Alap létrehozásáról és az 1093/2010/EU rendelet módosításáról (HL L 225., 2014.7.30., 1. o.).

(8) Az ESMA által e cikk (7) bekezdése alapján küldendő értesítés nem érinti az illetékes hatóság azon felelősségét, hogy sürgősen továbbítsa a jelentős IKT-vonatkozású esemény részleteit a fogadó tagállambeli releváns hatóságnak, amennyiben valamely központi értéktár jelentős határokon átnyúló tevékenységet folytat a fogadó tagállamban, a jelentős IKT-vonatkozású esemény valószínűleg súlyos következményekkel jár a fogadó tagállam pénzügyi piacaira nézve, és amennyiben az illetékes hatóságok között együttműködési megállapodások vannak érvényben a pénzügyi szervezetek felügyeletéhez kapcsolódóan.

20. cikk

A bejelentések tartalmának és a sablonjainak harmonizációja

Az EFH-k a vegyes bizottság keretében, valamint az ENISA-val és az EKB-val konzultálva, kidolgozzák a következőket:

a) közös szabályozástechnikai standardtervezetek, amelyek:

   i. megállapítják a jelentős IKT-vonatkozású eseményekre vonatkozó jelentések tartalmát, hogy azok tükrözzék a 18. cikk (1) bekezdésében meghatározott kritériumokat, és további elemeket építenek be, így például a bejelentés más tagállamok számára való relevanciájának megállapítására vonatkozó részleteket, valamint azt, hogy az esemény jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseménynek minősül-e vagy sem;

   ii. meghatározzák a 19. cikk (4) bekezdésében említett kezdeti értesítésre és minden egyes jelentésre vonatkozó határidőket;

   iii. meghatározzák a jelentős kiberfenyegetésekről szóló értesítés tartalmát.

   Az említett szabályozástechnikai standardtervezetek kidolgozása során az EFH-knak figyelembe kell venniük a pénzügyi szervezet méretét és általános kockázati profilját, valamint a szolgáltatásai, tevékenységei és műveletei jellegét, nagyságrendjét és összetettségét és különösen annak biztosítása céljából, hogy e bekezdés a) pontja ii. alpontjának alkalmazásában a különböző határidők adott esetben tükrözhessék a pénzügyi ágazatok sajátosságait az IKT-vonatkozású események e rendelet és az (EU) 2022/2555 irányelv alapján történő bejelentésére vonatkozó következetes megközelítés fenntartásának sérelme nélkül. Az EFH-knak adott esetben meg kell indokolniuk, amennyiben eltérnek az említett irányelvvel összefüggésben alkalmazott megközelítésektől.

b) közös végrehajtás-technikai standardtervezetek, amelyek a pénzügyi szervezetek számára rögzítik a jelentős IKT-vonatkozású esemény bejelentésére és a jelentős kiberfenyegetésről szóló értesítésre szolgáló szabványos űrlapokat, sablonokat és eljárásokat.

Az EFH-knak az első bekezdés a) pontjában említett közös szabályozástechnikai standardtervezeteket és az első bekezdés b) pontjában említett közös végrehajtás-technikai standardtervezeteket 2024. július 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban az első bekezdés a) pontjában említett közös szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 15. cikkével összhangban elfogadja az első bekezdés b) pontjában említett közös végrehajtás-technikai standardokat.

21. cikk

A jelentős IKT-vonatkozású események központosított bejelentése

(1) Az EFH-knak a vegyes bizottság keretében, valamint az EKB-val és az ENISA-val konzultálva, közös jelentésben értékelniük kell annak lehetőségét, hogy az eseménybejelentést még nagyobb mértékben központosítsák azáltal, hogy egységes uniós központi adatbázist hoznak létre a jelentős IKT-vonatkozású események pénzügyi szervezetek általi bejelentése céljára. A közös jelentésben meg kell vizsgálni, hogy a felügyeleti konvergencia növelése érdekében milyen lehetőségek vannak az IKT-vonatkozású események bejelentésével kapcsolatos információáramlás megkönnyítésére, a járulékos költségek csökkentésére, valamint a tematikus elemzések megalapozására.

(2) Az (1) bekezdésben említett közös jelentésnek legalább a következő elemeket kell magában foglalnia:

a) az egységes európai uniós adatbázis létrehozásának előfeltételei;

b) az előnyök, a korlátok és a kockázatok, ideértve az érzékeny információk magas koncentrációjához kapcsolódó kockázatokat is;

c) az egyéb releváns bejelentési rendszerekkel kapcsolatos átjárhatóság biztosításához szükséges képesség;

d) az üzemeltetés elemei;

e) a tagság feltételei;

f) az egységes uniós adatbázishoz a pénzügyi szervezetek és az illetékes nemzeti hatóságok által való hozzáférés technikai feltételei;

g) az egységes uniós adatbázist támogató működési platform kialakításával felmerülő pénzügyi költségek előzetes értékelése, ideértve a szükséges szakértelmet is.

(3) Az EFH-knak az (1) bekezdésben említett jelentést 2025. január 17-ig be kell nyújtaniuk az Európai Parlamentnek, a Tanácsnak és a Bizottságnak.

22. cikk

Felügyeleti visszajelzés

(1) Az (EU) 2022/2555 irányelv szerinti CSIRT-ek által – adott esetben – a nemzeti joggal összhangban biztosítható technikai input, tanácsadás vagy korrekciós intézkedések, valamint későbbi utókövetés sérelme nélkül az illetékes hatóságnak a 19. cikk (4) bekezdésében említett kezdeti értesítés és minden egyes jelentés átvételekor vissza kell igazolnia azok kézhezvételét, és – amennyiben megvalósítható – kellő időben releváns és arányos visszajelzést vagy magas szintű iránymutatást nyújthat a pénzügyi szervezetnek, különösen a hasonló fenyegetésekkel kapcsolatos releváns anonimizált adatok és hírszerzés rendelkezésre bocsátásával, továbbá megvitathatja a pénzügyi szervezet szintjén alkalmazott korrekciós intézkedéseket, valamint a pénzügyi ágazat egészét érintő káros hatások minimalizálását és csökkentését célzó módokat. A pénzügyi szervezetek továbbra is teljes felelősséggel tartoznak a 19. cikk (1) bekezdése szerint bejelentett IKT-vonatkozású események kezeléséért és következményeiért, a kapott felügyeleti visszajelzések sérelme nélkül.

(2) Az EFH-knak a vegyes bizottság keretében anonimizált és összesített formában évente be kell számolniuk a jelentős IKT-vonatkozású eseményekről, amelyekről az illetékes hatóságoknak a 19. cikk (6) bekezdésével összhangban részletes tájékoztatást kell nyújtaniuk, meghatározva legalább a jelentős IKT-vonatkozású események számát, jellegét és a pénzügyi szervezetek vagy ügyfelek működésére gyakorolt hatását, a meghozott korrekciós intézkedéseket és a keletkezett költségeket.

Az EFH-knak figyelmeztetéseket kell kibocsátaniuk és magas szintű statisztikákat készíteniük, hogy támogassák az IKT-fenyegetési és -sérülékenységi értékeléseket.

23. cikk

Hitelintézeteket, pénzforgalmi intézményeket, számlainformációkat összesítő szolgáltatókat és elektronikuspénz-kibocsátó intézményeket érintő, pénzforgalmi vonatkozású működési vagy biztonsági események

Az e fejezetben megállapított követelmények alkalmazandók a pénzforgalmi vonatkozású működési vagy biztonsági eseményekre, valamint a jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményekre is, amennyiben azok hitelintézeteket, pénzforgalmi intézményeket, számlainformációkat összesítő szolgáltatókat és elektronikuspénz-kibocsátó intézményeket érintenek.

IV. FEJEZET

A digitális működési reziliencia tesztelése

24. cikk

A digitális működési reziliencia tesztelésének végrehajtására vonatkozó általános követelmények

(1) Az IKT-vonatkozású események kezelésére való felkészültség értékelése, a digitális működési reziliencia gyengeségeinek, hiányosságainak és lefedetlenségeinek azonosítása, valamint a korrekciós intézkedések gyors végrehajtása érdekében a mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek a 4. cikk (2) bekezdésében meghatározott kritériumok figyelembevételével a digitális működési reziliencia tesztelésére megbízható és átfogó programot kell kialakítaniuk, fenntartaniuk és felülvizsgálniuk, a 6. cikkben említett IKT-kockázatkezelési keretrendszer integráns részeként.

(2) A digitális működési reziliencia tesztelését szolgáló programnak magában kell foglalnia a 25. és 26. cikkel összhangban alkalmazandó értékeléseket, teszteket, módszertanokat, gyakorlatokat és eszközöket.

(3) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek az e cikk (1) bekezdésében említett, a digitális működési reziliencia tesztelését szolgáló program lefolytatása során – a 4. cikk (2) bekezdésében meghatározott kritériumokat figyelembe véve – kockázatalapú megközelítést kell követniük, kellően tekintetbe véve az IKT-kockázat változó környezetét, minden olyan konkrét kockázatot, amelynek az érintett pénzügyi szervezet ki van vagy ki lehet téve, az információs vagyonelemek és a nyújtott szolgáltatások kritikusságát, valamint a pénzügyi szervezet által megfelelőnek tartott bármely egyéb tényezőt.

(4) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek biztosítaniuk kell, hogy a teszteket független belső vagy külső fél hajtsa végre. Amennyiben a teszteket belső tesztelő végzi, a pénzügyi szervezeteknek elegendő erőforrást kell elkülöníteniük, és biztosítaniuk kell, hogy a teszt tervezési és végrehajtási szakaszában ne legyenek összeférhetetlenségek.

(5) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek eljárásokat és szabályzatokat kell kialakítaniuk a tesztek lefolytatása során feltárt valamennyi probléma rangsorolása, osztályozása és orvoslása céljából, továbbá ki kell alakítaniuk azon belső validálási módszertanokat, amelyekkel megerősíthető, hogy a szervezet maradéktalanul kezelte az azonosított gyengeségeket és hiányosságokat.

(6) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek legalább évente biztosítaniuk kell, hogy megfelelő teszteket végezzenek a kritikus vagy fontos funkciókat támogató valamennyi IKT-rendszeren és -alkalmazáson.

25. cikk

Az IKT-eszközök és -rendszerek tesztelése

(1) A 24. cikkben említett, a digitális működési reziliencia tesztelését szolgáló programnak – a 4. cikk (2) bekezdésében meghatározott kritériumokkal összhangban – biztosítania kell olyan megfelelő tesztek elvégzését, mint például sérülékenységi értékelések és ellenőrzések, nyílt forrású elemzések, hálózatbiztonsági értékelések, eltéréselemzések, fizikai biztonsági felülvizsgálatok, kérdőívek és szoftveres átvilágítási megoldások, lehetőség szerint forráskódvizsgálatok, forgatókönyv-alapú tesztek, kompatibilitás-tesztelés, teljesítmény-tesztelés, végpontok közötti tesztelés és behatolási tesztelés.

(2) A központi értéktáraknak és a központi szerződő feleknek sérülékenységi vizsgálatokat kell végezniük a pénzügyi szervezet kritikus vagy fontos funkcióit támogató új vagy meglévő alkalmazások és infrastrukturális összetevők, valamint IKT-szolgáltatások bevezetése vagy újbóli bevezetése előtt.

(3) A mikrovállalkozásoknak az (1) bekezdésben említett teszteket a kockázatalapú megközelítést az IKT-tesztelés stratégiai tervezésével kombinálva kell végrehajtaniuk, kellően figyelembe véve, hogy kiegyensúlyozott megközelítést kell fenntartani egyrészt az e cikkben előírt IKT-tesztelésre fordítandó erőforrás-nagyságrend és idő, másrészt a sürgősség, a kockázat típusa, az információs vagyonelemek és nyújtott szolgáltatások kritikussága, valamint bármely egyéb releváns tényező között, beleértve a pénzügyi szervezet számításba vett kockázatok vállalására való képességét is.

26. cikk

Az IKT-eszközök, -rendszerek és -folyamatok TLPT-n alapuló fejlett tesztelése

(1) A 16. cikk (1) bekezdésének első albekezdésében említett szervezetektől eltérő és mikrovállalkozásnak nem minősülő, az e cikk (8) bekezdésének harmadik albekezdésével összhangban azonosított pénzügyi szervezeteknek legalább 3 évente fejlett tesztelést kell végezniük a TLPT útján. Az illetékes hatóság a pénzügyi szervezet kockázati profilja alapján és a működési körülményeket figyelembe véve, szükség esetén felkérheti a pénzügyi szervezetet, hogy csökkentse vagy növelje a tesztelés gyakoriságát.

(2) Minden egyes fenyegetés alapú behatolási tesztelésnek ki kell terjednie a pénzügyi szervezet számos vagy valamennyi kritikus vagy fontos funkciójára, és azt az ilyen funkciókat támogató éles rendszereken kell lefolytatni.

A pénzügyi szervezeteknek azonosítaniuk kell a kritikus vagy fontos funkciókat támogató valamennyi releváns, alapul szolgáló IKT-rendszert, -folyamatot és -technológiát, továbbá valamennyi releváns IKT-szolgáltatást, beleértve azokat, amelyek a harmadik fél IKT-szolgáltatókhoz kiszervezett vagy azoknak megbízásba adott kritikus vagy fontos funkciókat támogatják.

A pénzügyi szervezeteknek értékelniük kell, hogy mely kritikus vagy fontos funkciókra szükséges kiterjednie a TLPT-nek. Ezen értékelés eredménye határozza meg a TLPT pontos terjedelmét, és azt az illetékes hatóságoknak validálniuk kell.

(3) Amennyiben a TLPT harmadik fél IKT-szolgáltatókra is kiterjed, a pénzügyi szervezetnek meg kell hoznia a szükséges intézkedéseket és biztosítékokat az ilyen harmadik fél IKT-szolgáltatók TLPT-ben való részvételének biztosítása érdekében, és mindenkor teljes felelősséget kell viselnie az e rendeletnek való megfelelés biztosításáért.

(4) A (2) bekezdés első és második albekezdésének sérelme nélkül, amennyiben egy harmadik fél IKT-szolgáltatónak a (3) bekezdésben említett, TLPT-ben való közreműködéséről észszerűen feltételezhető, hogy az káros hatást gyakorol a harmadik fél IKT-szolgáltató által az e rendelet hatályán kívül eső ügyfeleknek nyújtott szolgáltatások minőségére vagy biztonságára, vagy az ilyen szolgáltatásokhoz kapcsolódó adatok bizalmasságára, a pénzügyi szervezet és a harmadik fél IKT-szolgáltató írásban megállapodhat arról, hogy a harmadik fél IKT-szolgáltató közvetlenül szerződéses megállapodást köt egy külső tesztelővel abból a célból, hogy egyetlen kijelölt pénzügyi szervezet irányítása alatt csoportos TLPT-t végezzen el több olyan pénzügyi szervezet részvételével, amelyek részére a harmadik fél IKT-szolgáltató IKT-szolgáltatásokat nyújt.

Az említett csoportos tesztelés kiterjed a pénzügyi szervezetek által a vonatkozó harmadik fél IKT-szolgáltatónak megbízásba adott kritikus vagy fontos funkciókat támogató IKT-szolgáltatások releváns körére. A csoportos tesztelést a csoportos tesztelésben részt vevő pénzügyi szervezetek által végzett TLPT-nek kell tekinteni.

A csoportos tesztelésben részt vevő pénzügyi szervezetek számát megfelelően, az érintett szolgáltatások összetettségét és típusát figyelembe véve kell kalibrálni.

(5) A pénzügyi szervezeteknek harmadik fél IKT-szolgáltatók és más érintett felek – ideértve a tesztelőket, de kizárva az illetékes hatóságokat – közreműködésével eredményes kockázatkezelési kontrollok útján mérsékelniük kell az adatokat érő bármilyen hatás, az eszközökben keletkező kár és a kritikus vagy fontos funkciók, szolgáltatások vagy műveletek zavarának kockázatát magánál a pénzügyi szervezetnél, annak partnereinél, valamint a pénzügyi ágazat egészében.

(6) A teszt befejezésekor, a jelentések és korrekciós tervek jóváhagyását követően a pénzügyi szervezet és adott esetben a külső tesztelők a (9) vagy (10) bekezdéssel összhangban kijelölt hatóság rendelkezésére bocsátják a releváns megállapítások összefoglalását, a korrekciós terveket és azon dokumentációt, amely bemutatja, hogy a TLPT-t a követelményeknek megfelelően végezték el.

(7) A hatóságoknak igazolást kell kiadniuk a pénzügyi szervezetek részére, amely megerősíti, hogy a tesztet a dokumentációban igazoltak szerint a követelményeknek megfelelően hajtották végre, annak érdekében, hogy az illetékes hatóságok között lehetővé váljon a fenyegetés alapú behatolási tesztelés kölcsönös elismerése. A pénzügyi szervezet értesíti a releváns illetékes hatóságot az igazolásról, a releváns megállapítások összefoglalásáról és a korrekciós tervekről.

Az ilyen igazolást nem érintve, a pénzügyi szervezetek mindenkor teljes felelősséggel tartoznak a (4) bekezdésben említett tesztek hatásáért.

(8) A pénzügyi szervezeteknek a 27. cikkel összhangban szerződést kell kötniük a tesztelőkkel a TLPT elvégzése céljából. Amennyiben a pénzügyi szervezetek belső tesztelőket vesznek igénybe a TLPT elvégzésének céljából, három tesztenként külső tesztelőt kell megbízniuk.

Az 1024/2013/EU rendelet 6. cikke (4) bekezdésének megfelelően jelentősnek minősített hitelintézetek a 27. cikk (1) bekezdése a)–e) pontjának megfelelően csak külső tesztelőket alkalmazhatnak.

Az illetékes hatóságoknak a 4. cikk (2) bekezdésében meghatározott kritériumok figyelembevételével, a következők értékelése alapján kell kiválasztaniuk a TLPT elvégzésére kötelezett pénzügyi szervezeteket:

a) hatás-vonatkozású tényezők, így különösen az a mérték, amennyire a pénzügyi szervezet által nyújtott szolgáltatások és elvégzett tevékenységek hatnak a pénzügyi ágazatra;

b) esetleges pénzügyi stabilitási megfontolások, ideértve a pénzügyi szervezet uniós vagy nemzeti léptékű rendszerszintű jellegét, az esettől függően;

c) a pénzügyi szervezet vagy az érintett technológiai elemek egyedi IKT-kockázati profilja és IKT-érettségi szintje.

(9) A tagállamok kijelölhetnek egyetlen hatóságot a pénzügyi szektorban, hogy feleljen a pénzügyi szektorban nemzeti szinten a TLPT-vonatkozású ügyekért, és az e célból szükséges valamennyi hatáskörrel és feladattal megbízzák azt.

(10) Az e cikk (9) bekezdésének megfelelő kijelölés hiányában és a TLPT elvégzésére kötelezett pénzügyi szervezetek kiválasztására vonatkozó hatáskör sérelme nélkül, az illetékes hatóság az e cikkben és a 27. cikkben említett feladatok egy részének vagy mindegyikének ellátását átruházhatja egy másik nemzeti hatóságra a pénzügyi szektorban.

(11) Az EFH-knak az EKB-val egyetértésben közös szabályozástechnikai standardtervezeteket kell kidolgozniuk a TIBER–EU keretnek megfelelően, a következők részletes meghatározása érdekében:

a) a (8) bekezdés második albekezdésének alkalmazása céljából használt kritériumok;

b) a belső tesztelők igénybevételére vonatkozó követelmények és standardok;

c) a következőkre vonatkozó követelmények:

   i. a (2) bekezdésben említett TLPT hatóköre;

   ii. a tesztelési folyamat egyes szakaszaiban követendő tesztelési módszertan és megközelítés;

   iii. a tesztelés eredményei, lezárása és korrekciós szakaszai;

d) az egynél több tagállamban működő pénzügyi szervezetek körében elvégzendő TLPT végrehajtásához és e tesztelés kölcsönös elismerésének az elősegítéséhez szükséges felügyeleti és egyéb releváns együttműködés típusa a megfelelő szintű felügyeleti részvétel, valamint a pénzügyi alágazatok vagy a helyi pénzügyi piacok sajátos igényeihez igazodó, rugalmas végrehajtás biztosítása érdekében.

Az említett szabályozástechnikai standardtervezetek kidolgozása során az EFH-knak kellő figyelmet kell fordítaniuk a különböző pénzügyi szolgáltatási ágazatok tevékenységeinek eltérő jellegéből eredő sajátosságokra.

Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. július 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban az első albekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

27. cikk

A TLPT lefolytatására vonatkozó, a tesztelőknek előírt követelmények

(1) A pénzügyi szervezetek a TLPT lefolytatására csak olyan tesztelőket vehetnek igénybe:

a) amelyek a legnagyobb fokú alkalmassággal és szakmai hírnévvel rendelkeznek;

b) amelyek rendelkeznek technikai és szervezeti képességekkel, valamint speciális szakértelmet mutatnak fel a fenyegetettséggel kapcsolatos hírszerzés, a behatolási tesztelés és a saját támadóerős (red team) tesztelés terén;

c) amelyeket egy tagállambeli akkreditációs testület tanúsított, vagy amelyek formális magatartási kódexek vagy etikai keretek szerint járnak el;

d) amelyek független bizonyosságot vagy audit jelentést biztosítanak a TLPT lefolytatásával összefüggő kockázatok megbízható kezelésével kapcsolatban, ideértve a pénzügyi szervezet bizalmas adatainak kellő védelmét és a pénzügyi szervezet üzleti kockázataival kapcsolatos jogorvoslatot is;

e) amelyek releváns szakmai felelősségbiztosítások révén megfelelően és teljeskörűen biztosítva vannak, többek között a szakmai kötelezettségmulasztás és a gondatlanság kockázataival szemben.

(2) A belső tesztelők igénybevétele során a pénzügyi szervezeteknek biztosítaniuk kell, hogy az (1) bekezdésben foglalt követelmények mellett, a következő feltételek is teljesüljenek:

a) az ilyen igénybevételt a releváns illetékes hatóság vagy a 26. cikk (9) és (10) bekezdésével összhangban kijelölt egyetlen hatóság jóváhagyta;

b) a releváns illetékes hatóság meggyőződött arról, hogy a pénzügyi szervezet elegendő célzott forrást különített el, és biztosította az összeférhetetlenség elkerülését a teszt tervezési és végrehajtási szakaszában; és

c) a fenyegetettséggel kapcsolatos hírszerzés nyújtója a pénzügyi szervezeten kívül működik.

(3) A pénzügyi szervezeteknek biztosítaniuk kell, hogy a külső tesztelőkkel kötött szerződések előírják a TLPT eredményeinek megbízható kezelését, továbbá azt, hogy az adatkezelés, ezen belül az adatok előállítása, tárolása, összesítése, előkészítése, bejelentése, közlése vagy megsemmisítése ne járjon kockázattal a pénzügyi szervezet számára.

V. FEJEZET

A harmadik féltől eredő IKT-kockázat kezelése

I. szakasz

A harmadik féltől eredő IKT-kockázat megbízható kezelésének alapelvei

28. cikk

Általános elvek

(1) A pénzügyi szervezeteknek a harmadik féltől eredő IKT-kockázatot az IKT-kockázat integráns összetevőjeként kell kezelniük a 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszerükön belül és a következő elvekkel összhangban:

a) azon pénzügyi szervezeteknek, amelyek üzleti tevékenységük folytatásához IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodást kötöttek, mindenkor teljes felelősséggel kell tartozniuk az e rendeletben és az alkalmazandó, pénzügyi szolgáltatásokra vonatkozó jogszabályokban előírt kötelezettségeknek való megfelelésért;

b) a pénzügyi szervezeteknek a harmadik féltől eredő IKT-kockázat kezelését az arányosság elvének megfelelően, a következők figyelembevételével kell megvalósítaniuk:

i. az IKT-vonatkozású függőségek jellege, nagyságrendje, összetettsége és fontossága;

ii. a harmadik fél IKT-szolgáltatókkal kötött, IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokból eredő kockázatok, figyelembe véve a vonatkozó szolgáltatás, folyamat vagy funkció kritikusságát vagy fontosságát, valamint a pénzügyi szolgáltatások és tevékenységek folytonosságára és rendelkezésre állására egyedi és csoportszinten gyakorolt potenciális hatást.

(2) Az IKT-kockázatkezelési keretrendszerük részeként a 16. cikk (1) bekezdésének első albekezdésében említett szervezetektől eltérő és mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek – adott esetben a 6. cikk (9) bekezdésében említett, több beszállítóra épülő stratégia figyelembevételével – a harmadik féltől eredő IKT-kockázatra vonatkozó stratégiát kell elfogadniuk és rendszeresen felülvizsgálniuk. A harmadik féltől eredő IKT-kockázatra vonatkozó azon stratégiának, amelyet az egyedi szervezet szintjén, valamint adott esetben szubkonszolidált és konszolidált alapon is alkalmazni kell, magában kell foglalnia a harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételére vonatkozó szabályzatot. A vezető testületnek a pénzügyi szervezet általános kockázati profiljának, valamint az üzleti szolgáltatások nagyságrendjének és összetettségének értékelése alapján rendszeresen felül kell vizsgálnia a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokkal kapcsolatban azonosított kockázatokat.

(3) IKT-kockázatkezelési keretrendszerük részeként a pénzügyi szervezeteknek az egyedi szervezet szintjén, valamint szubkonszolidált és konszolidált szinten információ-nyilvántartást kell vezetniük és naprakészen tartaniuk a harmadik fél IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételéről szóló valamennyi szerződéses megállapodásról.

Az első albekezdésben említett szerződéses megállapodásokat megfelelően dokumentálni kell, megkülönböztetve azokat, amelyek kiterjednek a kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokra, és azokat, amelyek nem.

A pénzügyi szervezeteknek legalább évente jelentést kell tenniük az illetékes hatóságoknak az IKT-szolgáltatások igénybevételéről szóló új megállapodások számáról, a harmadik fél IKT-szolgáltatók kategóriáiról, a szerződéses megállapodások típusairól, valamint a nyújtott IKT-szolgáltatásokról és -funkciókról.

A pénzügyi szervezeteknek az illetékes hatóság kérésére annak rendelkezésére kell bocsátaniuk a teljes információ-nyilvántartást, vagy a kérésnek megfelelően annak meghatározott részeit, a pénzügyi szervezet eredményes felügyeletéhez szükségesnek ítélt bármely információval együtt.

A pénzügyi szervezeteknek időben tájékoztatniuk kell az illetékes hatóságot bármely, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló, tervezett szerződéses megállapodásról, valamint arról, ha egy funkció kritikussá vagy fontossá válik.

(4) Az IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodások megkötése előtt a pénzügyi szervezetek:

a) értékelik, hogy a szerződéses megállapodás érinti-e kritikus vagy fontos funkciót támogató IKT-szolgáltatások igénybevételét;

b) értékelik, hogy teljesülnek-e a szerződéskötés felügyeleti feltételei;

c) azonosítják és értékelik a szerződéses megállapodással összefüggő valamennyi releváns kockázatot, beleértve annak lehetőségét is, hogy a szerződéses megállapodás hozzájárulhat a 29. cikkben említett IKT-koncentrációs kockázat erősödéséhez;

d) elvégzik a leendő harmadik fél IKT-szolgáltató teljeskörű átvilágítását, továbbá a kiválasztási és értékelési folyamatok során meggyőződnek a harmadik fél IKT-szolgáltató alkalmasságáról;

e) azonosítják és értékelik a szerződéses megállapodással esetlegesen okozott összeférhetetlenséget.

(5) A pénzügyi szervezetek csak azon harmadik fél IKT-szolgáltatókkal köthetnek szerződéses megállapodást, amelyek megfelelnek a rájuk vonatkozó információbiztonsági szabványoknak. Amennyiben az említett szerződéses megállapodások kritikus vagy fontos funkciókat érintenek, a pénzügyi szervezeteknek a megállapodások megkötése előtt kellően figyelembe kell venniük a legfrissebb és legjobb minőségű információbiztonsági szabványok harmadik fél IKT-szolgáltatók általi alkalmazását.

(6) A harmadik fél IKT-szolgáltató kapcsán a hozzáférési, ellenőrzési és audit jogok gyakorlásakor a pénzügyi szervezetek kockázatalapú megközelítés alapján előzetesen megállapítják az auditok és ellenőrzések gyakoriságát, valamint azon területeket, amelyeket az általánosan elfogadott audit standardoknak és az ilyen audit standardok alkalmazására és beépítésére vonatkozó felügyeleti utasításnak megfelelően auditálni szükséges.

Amennyiben a harmadik fél IKT-szolgáltatókkal az IKT-szolgáltatások igénybevételéről kötött szerződéses megállapodások nagy fokú technikai összetettséggel járnak, a pénzügyi szervezetnek meg kell győződnie arról, hogy az ellenőrök – attól függetlenül, hogy belső vagy külső ellenőrről, vagy ellenőrök csoportjáról van szó – rendelkeznek-e a releváns auditok és értékelések eredményes elvégzéséhez szükséges készségekkel és ismeretekkel.

(7) A pénzügyi szervezetek biztosítják, hogy az IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokat meg lehessen szüntetni a következő körülmények bármelyikének fennállása esetén:

a) a harmadik fél IKT-szolgáltató jelentősen megsérti az alkalmazandó jogszabályi, hatósági és szerződéses rendelkezéseket;

b) a harmadik féltől eredő IKT-kockázat monitorozása olyan körülményeket tár fel, amelyek alkalmasnak tekinthetők arra, hogy befolyásolják a szerződéses megállapodás keretében ellátott funkciók teljesítményét, ideértve a megállapodást vagy a harmadik fél IKT-szolgáltató helyzetét érintő lényeges módosításokat is;

c) a harmadik fél IKT-szolgáltatónál az általános IKT-kockázatkezelését érintő, bizonyítható gyengeségek tapasztalhatók és különösen azon mód, ahogyan biztosítja az adatok akár személyes, akár egyébként érzékeny adatok, vagy nem személyes adatok rendelkezésre állását, hitelességét, integritását és bizalmas jellegét;

d) amennyiben a vonatkozó szerződéses megállapodással kapcsolatos feltételek vagy körülmények eredményeként az illetékes hatóság már nem tudja eredményesen felügyelni a pénzügyi szervezetet.

(8) A kritikus vagy fontos funkciókat támogató IKT-szolgáltatások esetében a pénzügyi szervezeteknek kilépési stratégiákat kell bevezetniük. A kilépési stratégiáknak figyelembe kell venniük a harmadik fél IKT-szolgáltatók szintjén esetlegesen felmerülő kockázatokat, így különösen a részükről bekövetkező lehetséges mulasztást, a nyújtott IKT-szolgáltatások minőségének romlását, a szolgáltatások nem megfelelő nyújtása vagy meghiúsulása miatt az üzletmenetben okozott súlyos zavart, vagy a vonatkozó IKT-szolgáltatás megfelelő és folyamatos ellátásával kapcsolatban felmerülő bármely lényeges kockázatot, vagy a harmadik fél IKT-szolgáltatókkal kötött szerződéses megállapodások felmondását a (7) bekezdésben felsorolt körülmények bármelyikének esetében.

A pénzügyi szervezetek biztosítják, hogy képesek kilépni a szerződéses megállapodásokból anélkül, hogy:

a) zavar keletkezne üzleti tevékenységükben;

b) korlátozottá válna a szabályozási követelményeknek való megfelelésük;

c) sérülne az ügyfeleknek nyújtott szolgáltatások folytonossága és minősége.

A kilépési terveknek átfogóaknak kell lenniük, azokat dokumentálni kell, valamint – a 4. cikk (2) bekezdésében foglalt kritériumokkal összhangban – megfelelően tesztelni és időszakonként felülvizsgálni.

A pénzügyi szervezeteknek alternatív megoldásokat kell azonosítaniuk és átállási terveket kidolgozniuk, amelyek lehetővé teszik számukra, hogy a szerződéses megbízásba adott IKT-szolgáltatásokat és a releváns adatokat leválasszák a harmadik fél IKT-szolgáltatóról, és azokat biztonságosan és teljeskörűen alternatív szolgáltatókhoz telepítsék, vagy visszaszervezzék a saját működésükbe.

A pénzügyi szervezeteknek az üzletmenet folytonosságát biztosító, megfelelő rendkívüli intézkedésekkel kell rendelkezniük az első albekezdésben említett körülmények esetén.

(9) Az EFH-knak a vegyes bizottság keretében olyan végrehajtás-technikai standardtervezeteket kell kidolgozniuk, amelyek meghatározzák a (3) bekezdésben említett információ-nyilvántartás céljából a mintadokumentumokat, ideértve az IKT-szolgáltatások igénybevételéről szóló valamennyi szerződéses megállapodás esetében közös információkat. Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. január 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 15. cikkével összhangban elfogadja az első albekezdésben említett végrehajtás-technikai standardokat.

(10) Az EFH-knak a vegyes bizottság keretében szabályozástechnikai standardtervezeteket kell kidolgozniuk, amelyek részletesen meghatározzák a (2) bekezdésben említett szabályzat tartalmi elemeit a harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodások tekintetében.

Az említett szabályozástechnikai standardtervezetek kidolgozása során az EFH-knak figyelembe kell venniük a pénzügyi szervezet méretét és általános kockázati profilját, valamint szolgáltatásai, tevékenységei és műveletei jellegét, nagyságrendjét és összetettségét. Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. január 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban az első albekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

29. cikk

Az IKT-koncentrációs kockázat szervezetszintű előzetes értékelése

(1) A kockázatoknak a 28. cikk (4) bekezdésének c) pontjában említett azonosítása és értékelése során a pénzügyi szervezeteknek figyelembe kell venniük azt is, hogy a kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokkal kapcsolatos szerződéses megállapodás tervezett megkötése a következők valamelyikét eredményezné-e:

a) olyan harmadik fél IKT-szolgáltatóval történő szerződéskötés, amely nem helyettesíthető könnyen; vagy

b) kritikus vagy fontos funkciókat támogató IKT-szolgáltatások nyújtásával kapcsolatban többszörös szerződéses megállapodás megléte ugyanazzal a harmadik fél IKT-szolgáltatóval, vagy egymással szoros kapcsolatban álló harmadik fél IKT-szolgáltatókkal.

A pénzügyi szervezeteknek mérlegelniük kell az alternatív megoldások így például a különböző harmadik fél IKT-szolgáltatók igénybevételének előnyeit és költségeit, figyelembe véve, hogy az előirányzott megoldások illeszkednek-e és hogyan a szervezetek digitális rezilienciára vonatkozó stratégiájában meghatározott üzleti igényekhez és célkitűzésekhez.

(2) Amennyiben a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokban szerepel az a lehetőség, hogy egy harmadik fél IKT-szolgáltató egy kritikus vagy fontos funkciót támogató IKT-szolgáltatást más harmadik fél IKT-szolgáltatóknak ad alvállalkozásba, a pénzügyi szervezeteknek mérlegelniük kell az alvállalkozó ezen igénybevételéből esetlegesen származó előnyöket és kockázatokat, különösen egy harmadik országban letelepedett IKT-alvállalkozó esetén.

Amennyiben a szerződéses megállapodások kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételére vonatkoznak, a pénzügyi szervezeteknek kellő figyelmet kell fordítaniuk a harmadik fél IKT-szolgáltató csődje esetén alkalmazandó fizetésképtelenségi jogi rendelkezésekre, valamint a pénzügyi szervezet adatainak haladéktalan visszaszerzése kapcsán esetlegesen felmerülő akadályokra.

Amennyiben egy harmadik országban letelepedett, harmadik fél IKT-szolgáltatóval jön létre kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodás, a pénzügyi szervezeteknek – a második albekezdésben említett megfontolásokon túlmenően – figyelembe kell venniük az uniós adatvédelmi szabályoknak való megfelelést és a jog hatékony érvényesítését az említett harmadik országban.

Amennyiben a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodások alvállalkozó igénybevételéről rendelkeznek, a pénzügyi szervezeteknek értékelniük kell, hogy a potenciálisan hosszú vagy összetett alvállalkozói láncok érinthetik-e – és ha igen, hogyan – a szervezet képességét a szerződéses megbízásba adott funkciók teljeskörű nyomon követésére, valamint az illetékes hatóság képességét arra, hogy e tekintetben eredményesen ellássa a pénzügyi szervezet felügyeletét.

30. cikk

Főbb szerződéses rendelkezések

(1) A pénzügyi szervezet és a harmadik fél IKT-szolgáltató jogait és kötelezettségeit egyértelműen meg kell határozni, és írásban kell rögzíteni. A teljes szerződésnek magában kell foglalnia a szolgáltatási szintekre vonatkozó megállapodást is, és azt egyetlen, írásba foglalt dokumentumban kell rögzíteni, amelynek nyomtatott vagy egyéb, letölthető, tartós és hozzáférhető formátumú dokumentumban kell a felek rendelkezésére állnia.

(2) Az IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásoknak legalább a következő elemeket kell magukban foglalniuk:

a) a harmadik fél IKT-szolgáltató által biztosítandó funkciók és IKT-szolgáltatások egyértelmű és teljeskörű leírása annak feltüntetésével, hogy valamely kritikus vagy fontos funkciót támogató IKT-szolgáltatásnak vagy annak érdemi részeinek alvállalkozásba adása megengedett-e, és ha igen, milyen feltételek alkalmazandók az ilyen alvállalkozásba adásra;

b) azon helyszínek – nevezetesen azon régiók és országok –, ahol a szerződéses megbízásba vagy alvállalkozásba adott funkciók vagy IKT-szolgáltatások nyújtása és az adatkezelés történik, ideértve a tárolás helyét is, továbbá annak előírása, hogy a harmadik fél IKT-szolgáltatónak előzetesen értesítenie kell a pénzügyi szervezetet, ha tervezi az ilyen helyszínek megváltoztatását;

c) az adatok – köztük a személyes adatok – védelmével kapcsolatban a rendelkezésre állásra, hitelességre, integritásra és bizalmas jellegre vonatkozó rendelkezések;

d) az olyan személyes és nem személyes adatok – könnyen hozzáférhető formátumban történő – hozzáférésének, helyreállításának és visszaszolgáltatásának biztosítására vonatkozó rendelkezések, amelyeket a pénzügyi szervezet a harmadik fél IKT-szolgáltató fizetésképtelensége, szanálása vagy üzleti tevékenységének megszüntetése, vagy a szerződéses megállapodások megszűnése esetén kezel;

e) a szolgáltatási szintek leírása, ideértve annak frissítéseit és módosításait is;

f) a harmadik fél IKT-szolgáltató azon kötelezettsége, hogy valamely, a pénzügyi szervezetnek nyújtott IKT-szolgáltatással kapcsolatos, IKT-biztonsági esemény bekövetkezésekor többletköltség nélkül vagy előzetesen megállapított költség mellett támogatást nyújtson a pénzügyi szervezetnek;

g) a harmadik fél IKT-szolgáltató azon kötelezettsége, hogy teljes mértékben együttműködjön az illetékes hatóságokkal és a pénzügyi szervezet szanálási hatóságaival, beleértve az általuk kinevezett személyeket is;

h) a szerződéses megállapodások megszüntetésére vonatkozó felmondási jogok és az azokhoz kapcsolódó minimális felmondási idő az illetékes hatóságok és a szanálási hatóságok elvárásainak megfelelően;

i) a harmadik fél IKT-szolgáltatóknak a pénzügyi szervezetek 13. cikk (6) bekezdése szerinti IKT-biztonsági tudatosságot elősegítő programjain és a digitális működési rezilienciával kapcsolatos képzésein való részvételére vonatkozó feltételek.

(3) A kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásoknak a (2) bekezdésben említett elemeken felül tartalmazniuk kell legalább a következőket:

a) a szolgáltatási szintek teljeskörű leírása, beleértve annak frissítéseit és felülvizsgálatait is, a megállapodás szerinti szolgáltatási szinteken belüli pontos mennyiségi és minőségi teljesítménycélokkal együtt, hogy lehetővé váljon az IKT-szolgáltatásoknak a pénzügyi szervezet általi eredményes nyomon követése, és lehetővé váljon megfelelő korrekciós intézkedések indokolatlan késedelem nélküli meghozatala, amikor a megállapodás szerinti szolgáltatási szintek nem teljesülnek;

b) a harmadik fél IKT-szolgáltatóra vonatkozó felmondási idők és a pénzügyi szervezettel szembeni bejelentési kötelezettségei, ideértve bármely olyan fejlemény bejelentését, amely lényeges hatást gyakorolhat a harmadik fél IKT-szolgáltató azon képességére, hogy a megállapodás szerinti szolgáltatási szinteknek megfelelően eredményesen biztosítsa a kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokat;

c) arra vonatkozó követelmények, hogy a harmadik fél IKT-szolgáltató vezessen be és teszteljen vészhelyzeti terveket, továbbá rendelkezzen olyan IKT-biztonsági intézkedésekkel, eszközökkel és szabályzatokkal, amelyek biztosítják a megfelelő biztonsági szintet ahhoz, hogy a pénzügyi szervezet a szabályozási keretével összhangban nyújtson szolgáltatásokat;

d) a harmadik fél IKT-szolgáltató azon kötelezettsége, hogy – a 26. és a 27. cikkben említettek szerint – részt vegyen és teljes mértékben együttműködjön a pénzügyi szervezet által végzett TLPT-ben;

e) a pénzügyi szervezet azon joga, hogy folyamatosan monitorozza a harmadik fél IKT-szolgáltató teljesítményét, ami a következőkkel jár:

i. a pénzügyi szervezet vagy egy kinevezett harmadik fél, valamint az illetékes hatóság korlátlan hozzáférési, ellenőrzési és audit joga és a releváns dokumentumokról a helyszínen való másolatkészítés joga – amennyiben azok kritikusak a harmadik fél IKT-szolgáltató műveletei szempontjából –, amelynek tényleges gyakorlását nem akadályozza vagy korlátozza más szerződéses megállapodás vagy végrehajtási szabályzat;

ii. az alternatív bizonyossági szintekről való megállapodás joga, ha más ügyfelek jogai érintettek;

iii. a harmadik fél IKT-szolgáltató azon kötelezettsége, hogy maradéktalanul együttműködjön az illetékes hatóságok, a vezető felvigyázó, a pénzügyi szervezet vagy egy kinevezett harmadik fél által végzett helyszíni ellenőrzések és auditok során; és

iv. az ilyen ellenőrzések és auditok terjedelmével, követendő eljárásaival és gyakoriságával kapcsolatos részletek megadásának kötelezettsége;

f) kilépési stratégiák, különösen egy kötelező megfelelő átmeneti időszak meghatározása:

i. amelynek során a harmadik fél IKT-szolgáltató folytatja a vonatkozó funkciók és IKT-szolgáltatások nyújtását annak érdekében, hogy csökkentse a pénzügyi szervezetnél keletkező zavar kockázatát, vagy biztosítsa annak eredményes szanálását és szerkezetátalakítását;

ii. amely lehetővé teszi a pénzügyi szervezet számára, hogy valamely egyéb harmadik fél IKT-szolgáltatóhoz migráljon, vagy házon belüli megoldásokra állhasson át a nyújtott szolgáltatás összetettségének megfelelően.

Az e) ponttól eltérve, a harmadik fél IKT-szolgáltató és a mikrovállalkozásként működő pénzügyi szervezet megállapodhat arról, hogy a pénzügyi szervezet hozzáférési, ellenőrzési és audit jogai átruházhatók a harmadik fél IKT-szolgáltató által kinevezett független harmadik félre, valamint hogy a pénzügyi szervezet bármikor tájékoztatást és biztosítékot kérhet a független harmadik féltől a harmadik fél IKT-szolgáltató teljesítése tekintetében.

(4) A szerződéses megállapodásokat előkészítő tárgyalások során a pénzügyi szervezeteknek és a harmadik fél IKT-szolgáltatóknak mérlegelniük kell az egyes szolgáltatásokra a hatóságok által kidolgozott általános szerződéses rendelkezések alkalmazását.

(5) Az EFH-knak a vegyes bizottságon keresztül szabályozástechnikai standardtervezeteket kell kidolgozniuk a (2) bekezdés a) pontjában említett azon elemek további pontosítása céljából, amelyeket a pénzügyi szervezetnek meg kell határoznia és értékelnie kell a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások alvállalkozásba adásakor.

A szabályozástechnikai standardtervezetek kidolgozása során az EFH-knak figyelembe kell venniük a pénzügyi szervezet méretét és általános kockázati profilját, valamint szolgáltatásai, tevékenységei és műveletei jellegét, nagyságrendjét és összetettségét.

Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. július 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban az első albekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

II. szakasz

A kritikus harmadik fél IKT-szolgáltatókra vonatkozó felvigyázási keretrendszer

31. cikk

A kritikus harmadik fél IKT-szolgáltatók kijelölése

(1) Az EFH-k a vegyes bizottság keretében, a 32. cikk (1) bekezdése alapján létrehozott felvigyázási fórum ajánlása alapján:

a) kijelölik azon harmadik fél IKT-szolgáltatókat, amelyek – a (2) bekezdésben meghatározott kritériumok figyelembevételével végzett értékelés nyomán – a pénzügyi szervezetek számára kritikusak;

b) a kritikus harmadik fél IKT-szolgáltatók mindegyikére vonatkozóan azon EFH-t nevezik ki vezető felvigyázóként, amely – az 1093/2010/EU, az 1094/2010/EU vagy az 1095/2010/EU rendeletnek megfelelően – azon pénzügyi szervezetekért felelős, amelyek teljes eszközértéke együttesen – amint azt az említett pénzügyi szervezetek egyedi mérlegeinek összesítése tanúsítja – a legnagyobb részt teszi ki a releváns kritikus harmadik fél IKT-szolgáltató szolgáltatásait igénybe vevő valamennyi pénzügyi szervezet teljes eszközértékén belül.

(2) Az (1) bekezdés a) pontjában említett kijelölésnek a harmadik fél IKT-szolgáltató által nyújtott IKT-szolgáltatásokkal kapcsolatban a következő kritériumokon kell alapulnia:

a) azon rendszerszintű hatás, amely a pénzügyi szolgáltatások nyújtásának stabilitását, folytonosságát vagy minőségét érné akkor, ha a releváns harmadik fél IKT-szolgáltató kiterjedt működési hiányosság miatt nem képes a szolgáltatásait nyújtani, figyelembe véve azon pénzügyi szervezetek számát, valamint azon pénzügyi szervezetek eszközeinek összértékét, amelyek részére a harmadik fél IKT-szolgáltató szolgáltatásokat nyújt;

b) a releváns harmadik fél IKT-szolgáltató szolgáltatásait igénybe vevő pénzügyi szervezetek rendszerszintű jellege vagy fontossága, a következő paraméterekkel összhangban értékelve:

   i. a vonatkozó harmadik fél IKT-szolgáltató szolgáltatásait igénybe vevő, globális rendszerszinten jelentős intézmények vagy egyéb rendszerszinten jelentős intézmények száma;

   ii. az i. alpontban említett globális rendszerszinten jelentős intézmények és egyéb rendszerszinten jelentős intézmények kölcsönös függése, beleértve azon helyzeteket is, amikor a globális rendszerszinten jelentős intézmények és egyéb rendszerszinten jelentős intézmények más pénzügyi szervezetek részére nyújtanak pénzügyi infrastrukturális szolgáltatásokat;

c) a releváns harmadik fél IKT-szolgáltató által nyújtott szolgáltatások igénybevétele a pénzügyi szervezetek olyan kritikus vagy fontos funkciói kapcsán, amelyek ellátására végső soron ugyanezen harmadik fél IKT-szolgáltató közreműködésével kerül sor függetlenül attól, hogy a pénzügyi szervezetek az említett szolgáltatásokat közvetlenül vagy közvetetten, alvállalkozási megállapodások útján veszik-e igénybe;

d) a harmadik fél IKT-szolgáltató helyettesíthetőségének mértéke, a következő paraméterek figyelembevételével:

   i. valós – legalább részleges – alternatívák hiánya, amely egy konkrét piacon működő harmadik fél IKT-szolgáltatók korlátozott számának, a releváns harmadik fél IKT-szolgáltató piaci részesedésének, vagy a megoldás technikai összetettségének vagy fejlettségének tulajdonítható, többek között bármely szabadalmaztatott technológia, vagy a harmadik fél IKT-szolgáltató szervezeti felépítésének vagy tevékenységének egyedi jellemzői kapcsán;

   ii. a releváns adatoknak és munkamennyiségnek a releváns harmadik fél IKT-szolgáltatótól egy másik harmadik fél IKT-szolgáltatóhoz történő részleges vagy teljes migrálásával járó nehézségek, amelyek okai lehetnek vagy a migrálási folyamattal esetleg együttjáró jelentős pénzügyi költségek, idő- vagy egyéb erőforrásigény, vagy azon megnövekedett IKT-kockázat vagy egyéb működési kockázatok, amelyeknek a pénzügyi szervezet ki lehet téve az ilyen migráció révén.

(3) Amennyiben a harmadik fél IKT-szolgáltató egy csoporthoz tartozik, a (2) bekezdésben említett kritériumokat a csoport egésze által nyújtott IKT-szolgáltatások tekintetében kell figyelembe venni.

(4) A csoport részét képező harmadik fél IKT-szolgáltatóknak koordinációs pontként ki kell jelölniük egy jogi személyt a megfelelő képviselet és a vezető felvigyázóval való kommunikáció biztosítása érdekében.

(5) A vezető felvigyázónak értesítenie kell a harmadik fél IKT-szolgáltatót az (1) bekezdés a) pontjában említett kijelöléshez vezető értékelés eredményéről. Az értesítés időpontjától számított 6 héten belül a harmadik fél IKT-szolgáltató indokolással ellátott nyilatkozatot nyújthat be a vezető felvigyázónak, amely tartalmazza az értékelés céljából releváns információkat. A vezető felvigyázónak meg kell vizsgálnia az indokolással ellátott nyilatkozatot, és az ilyen nyilatkozat kézhezvételétől számított 30 naptári napon belül további információk benyújtását kérheti.

Miután egy harmadik fél IKT-szolgáltatót kritikusnak jelöltek ki, az EFH-knak a vegyes bizottságon keresztül értesíteniük kell a harmadik fél IKT-szolgáltatót az ilyen kijelölésről és azon kezdőidőpontról, amelytől ténylegesen felvigyázási tevékenységek alá fog esni. Az említett kezdő időpontot az értesítéstől számított egy hónapon belül kell meghatározni. A harmadik fél IKT-szolgáltatónak értesítenie kell azon pénzügyi szervezeteket, amelyeknek szolgáltatásokat nyújt, a kritikusnak való kijelöléséről.

(6) A Bizottság felhatalmazást kap arra, hogy – az 57. cikkel összhangban – 2024. július 17-ig felhatalmazáson alapuló jogi aktust fogadjon el, amely az e cikk (2) bekezdésében említett kritériumok részletesebb meghatározásával egészíti ki ezt a rendeletet.

(7) Az (1) bekezdés a) pontjában említett kijelölés csak azt követően alkalmazható, hogy a Bizottság a (6) bekezdésnek megfelelően felhatalmazáson alapuló jogi aktust fogadott el.

(8) Az (1) bekezdés a) pontjában említett kijelölés nem alkalmazható a következők tekintetében:

i. azon pénzügyi intézmények, amelyek más pénzügyi intézményeknek nyújtanak IKT-szolgáltatásokat;

ii. azon harmadik fél IKT-szolgáltatók, amelyek az Európai Unió működéséről szóló szerződés 127. cikkének (2) bekezdésében említett feladatok támogatásának céljából létrehozott felvigyázási keretrendszerek hatálya alá tartoznak;

iii. a vállalatcsoporton belüli IKT-szolgáltatók;

iv. olyan harmadik fél IKT-szolgáltatók, amelyek kizárólag egy tagállamban nyújtanak IKT-szolgáltatásokat olyan pénzügyi szervezetek számára, amelyek csak az említett tagállamban tevékenykednek.

(9) Az EFH-knak a vegyes bizottság keretében össze kell állítaniuk, közzé kell tenniük és évente frissíteniük kell a kritikus harmadik fél IKT-szolgáltatók uniós szintű jegyzékét.

(10) Az (1) bekezdés a) pontjának alkalmazásában az illetékes hatóságok összesített formában évente átadják a 32. cikk alapján létrehozott felvigyázási fórumnak a 28. cikk (3) bekezdésének harmadik albekezdésében említett jelentéseket. A felvigyázási fórum az illetékes hatóságoktól kapott információk alapján értékeli a pénzügyi szervezetek harmadik féltől való IKT-függőségét.

(11) Azon harmadik fél IKT-szolgáltatók, amelyek nem szerepelnek a (9) bekezdésben említett jegyzékben, kérhetik, hogy az (1) bekezdés a) pontjának megfelelően kritikusnak legyenek kijelölve.

Az első albekezdés alkalmazásában a harmadik fél IKT-szolgáltatónak indokolással ellátott kérelmet kell benyújtania az EBH, az ESMA vagy az EIOPA részére, amely a vegyes bizottságon keresztül határoz arról, hogy az említett harmadik fél IKT-szolgáltatót az (1) bekezdés a) pontjának megfelelően kritikusnak jelöljék-e ki.

A kérelem beérkezésétől számított 6 hónapon belül kell elfogadni a második albekezdésben említett határozatot, és arról értesíteni a harmadik fél IKT-szolgáltatót.

(12) A pénzügyi szervezetek csak akkor vehetik igénybe egy harmadik országban letelepedett és az (1) bekezdés a) pontjával összhangban kritikusnak kijelölt harmadik fél IKT-szolgáltató szolgáltatásait, ha az utóbbi a kijelölést követő 12 hónapon belül leányvállalatot létesített az Unióban.

(13) A (12) bekezdésben említett kritikus harmadik fél IKT-szolgáltatónak értesítenie kell a vezető felvigyázót az Unióban letelepedett leányvállalat irányítási struktúráját érintő bármely változásról.

32. cikk

A felvigyázási keretrendszer felépítése

(1) Az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 57. cikkének (1) bekezdésével összhangban a vegyes bizottság albizottságként hozza létre a felvigyázási fórumot abból a célból, hogy támogassa a vegyes bizottság és a 31. cikk (1) bekezdésének b) pontjában említett vezető felvigyázó munkáját a pénzügyi ágazatokban fennálló, harmadik féltől eredő IKT-kockázat terén. A felvigyázási fórum előkészíti a vegyes bizottságnak az említett területet érintő közös álláspontokat és közös fellépéstervezeteit.

A felvigyázási fórum rendszeresen megvitatja az IKT-kockázattal és -sérülékenységgel kapcsolatos releváns fejleményeket, és következetes megközelítést szorgalmaz a harmadik féltől eredő IKT-kockázat uniós szintű nyomon követése terén.

(2) A felvigyázási fórum évente együttes értékelést végez a kritikus harmadik fél IKT-szolgáltatókra vonatkozó felvigyázási tevékenységek eredményeiről és megállapításairól, és koordinációs intézkedéseket mozdít elő, amelyek célja a pénzügyi szervezetek digitális működési rezilienciájának növelése, az IKT-koncentrációs kockázat kezelése terén elérhető legjobb gyakorlatok támogatása, továbbá a kockázat ágazatok közötti átterjedését mérséklő eszközök vizsgálata.

(3) A felvigyázási fórum a kritikus harmadik fél IKT-szolgáltatókra vonatkozó átfogó referenciamutatókat terjeszt elő, amelyeket a vegyes bizottság az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 56. cikkének (1) bekezdésével összhangban az EFH-k közös álláspontjaként fogad el.

(4) A felvigyázási fórum a következőkből áll:

a) az EFH-k elnökei;

b) az egyes tagállamoknak a 46. cikkben említett releváns illetékes hatósága mindenkori személyzetének egy-egy magas rangú képviselője;

c) megfigyelőként az egyes EFH-k ügyvezető igazgatója, valamint a Bizottság, az ERKT, az EKB és az ENISA egy-egy képviselője;

d) adott esetben megfigyelőként az egyes tagállamok valamely, a 46. cikkben említett illetékes hatóságának egy-egy további képviselője;

e) megfigyelőként adott esetben az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott – valamely kritikus harmadik fél IKT-szolgáltatónak kijelölt, az említett irányelv hatálya alá tartozó alapvető vagy fontos szervezet felügyeletéért felelős – illetékes hatóságok képviselője.

A felvigyázási fórum adott esetben kikérheti a (6) bekezdéssel összhangban kinevezett független szakértők tanácsát.

(5) Minden egyes tagállam kijelöli azon releváns illetékes hatóságot, amely személyzetének egyik tagja a (4) bekezdés első albekezdésének b) pontjában említett magas rangú képviselő, és erről tájékoztatja a vezető felvigyázót.

Az EFH-k a honlapjukon közzéteszik a releváns illetékes hatóság jelenlegi személyzetéből a tagállamok által kijelölt magas rangú képviselők jegyzékét.

(6) A (4) bekezdés második albekezdésében említett független szakértőket a felvigyázási fórum nevezi ki egy nyilvános és átlátható pályázati eljárást követően kiválasztott szakértői állományból.

A független szakértőket a pénzügyi stabilitással, a digitális működési rezilienciával és az IKT-biztonsággal kapcsolatos szakértelmük alapján kell kinevezni. Függetlenül és objektíven járnak el, kizárólag az Unió egészének érdekében, nem kérhetnek és nem fogadhatnak el utasítást sem uniós intézménytől vagy szervtől, sem tagállami kormánytól, sem más közjogi vagy magánjogi szervtől.

(7) Az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 16. cikkével összhangban az EFH-k 2024. július 17-ig – e szakasz alkalmazásában – iránymutatásokat adnak ki az EFH-k és az illetékes hatóságok között folytatandó együttműködésről, amely iránymutatások kiterjednek az illetékes hatóságok és az EFH-k közötti feladatok elosztására és végrehajtására vonatkozó részletes eljárásokra és feltételekre, valamint az ahhoz szükséges információcserék részleteire, hogy az illetékes hatóságok biztosítsák a 35. cikk (1) bekezdésének d) pontja alapján a kritikus harmadik fél IKT-szolgáltatóknak címzett ajánlások utókövetését.

(8) Az e szakaszban meghatározott követelmények nem érintik az (EU) 2022/2555 irányelv és a felhőszolgáltatókra alkalmazandó, felvigyázásra vonatkozó egyéb uniós szabályok alkalmazását.

(9) Az EFH-k a vegyes bizottságon keresztül és a felvigyázási fórum által végzett előkészítő munka alapján évente jelentést nyújtanak be e szakasz alkalmazásáról az Európai Parlamentnek, a Tanácsnak és a Bizottságnak.

33. cikk

A vezető felvigyázó feladatai

(1) A 31. cikk (1) bekezdésének b) pontjával összhangban kijelölt vezető felvigyázó elvégzi a kijelölt, kritikus harmadik fél IKT-szolgáltatók felvigyázását, és a felvigyázással kapcsolatos valamennyi kérdés céljából elsődleges kapcsolattartóként áll az említett kritikus harmadik fél IKT-szolgáltatók rendelkezésére.

(2) Az (1) bekezdés alkalmazásában a vezető felvigyázónak értékelnie kell, hogy a kritikus harmadik fél IKT-szolgáltatók mindegyike rendelkezik-e átfogó, megbízható és hatékony szabályokkal, eljárásokkal, mechanizmusokkal és intézkedésekkel azon tőle eredő IKT-kockázat kezeléséhez, amellyel a pénzügyi szervezetek szembesülhetnek.

Az első albekezdésben említett értékelésnek a kritikus harmadik fél IKT-szolgáltató által nyújtott IKT-szolgáltatások közül elsősorban a pénzügyi szervezetek kritikus vagy fontos funkcióit támogató szolgáltatásokra kell összpontosítania. Amennyiben az valamennyi releváns kockázat kezeléséhez szükséges, az említett értékelésnek ki kell terjednie a kritikus vagy fontos funkcióktól eltérő funkciókat támogató IKT-szolgáltatásokra is.

(3) A (2) bekezdésben említett értékelésnek ki kell terjednie a következőkre:

a) IKT-vonatkozású követelmények, hogy biztosítsák különösen azon szolgáltatások biztonságát, rendelkezésre állását, folytonosságát, skálázhatóságát és minőségét, amelyeket a kritikus harmadik fél IKT-szolgáltató nyújt pénzügyi szervezeteknek, valamint az adatok rendelkezésre állására, hitelességére, integritására vagy bizalmas jellegére vonatkozó magas szintű normák mindenkori fenntartásának képességét;

b) az IKT-biztonság biztosítását elősegítő fizikai biztonság, ezen belül a telephelyek, létesítmények, adatközpontok biztonsága;

c) a kockázatkezelési folyamatok, ezen belül az IKT-kockázatkezelési szabályzatok, az IKT-üzletmenetfolytonossági politika, valamint az IKT-reagálási és -helyreállítási tervek;

d) az irányítási rendszer, ezen belül az olyan szervezeti felépítés, amelyben az egyértelmű, átlátható és következetes felelősségi körök és elszámoltathatósági szabályok lehetővé teszik az eredményes IKT-kockázatkezelést;

e) a pénzügyi szervezeteket érő lényeges IKT-vonatkozású események azonosítása, nyomon követése és haladéktalan bejelentése, valamint az ilyen események, különösen a kiberbiztonsági események kezelése és elhárítása;

f) az adathordozhatóságot, valamint az alkalmazások hordozhatóságát és kölcsönös átjárhatóságát biztosító mechanizmusok, amelyek biztosítják a pénzügyi szervezetek számára a felmondási jogok tényleges gyakorlását;

g) az IKT-rendszerek, -infrastruktúrák és -kontrollok tesztelése;

h) az IKT-auditok;

i) a pénzügyi szervezetek részére nyújtott IKT-szolgáltatásokra alkalmazandó releváns nemzeti és nemzetközi szabványok használata.

(4) A (2) bekezdésben említett értékelés alapján és a 34. cikk (1) bekezdésében említett közös felvigyázási hálózattal (KFH) koordinálva, a vezető felvigyázónak egyértelmű, részletes és indokolással ellátott egyéni felvigyázási tervet kell elfogadnia, amelyben az egyes kritikus harmadik fél IKT-szolgáltatók számára kitűzött éves felvigyázási célok és tervezett főbb felvigyázási intézkedések szerepelnek. A tervről évente értesíteni kell a kritikus harmadik fél IKT-szolgáltatót.

A felvigyázási terv elfogadása előtt a vezető felvigyázónak ismertetnie kell a felvigyázásiterv-javaslatot a kritikus harmadik fél IKT-szolgáltatóval.

A felvigyázásiterv-javaslat kézhezvételét követően a kritikus harmadik fél IKT-szolgáltató 15 naptári napon belül indokolással ellátott nyilatkozatot nyújthat be, amelyben igazolja az e rendelet hatályán kívül eső ügyfelekre gyakorolt várható hatást, és adott esetben kockázatcsökkentő megoldásokat mutat be.

(5) A (4) bekezdésben említett éves felvigyázási tervek elfogadását és arról a kritikus harmadik fél IKT-szolgáltatók értesítését követően az illetékes hatóságok csak a vezető felvigyázó egyetértésével hozhatnak az ilyen kritikus harmadik fél IKT-szolgáltatókra vonatkozó intézkedéseket.

34. cikk

A vezető felvigyázók közötti operatív koordináció

(1) A felvigyázási tevékenységek következetes megközelítésének biztosítása céljából, valamint a koordinált általános felvigyázási stratégiák és a koherens operatív megközelítések és módszertanok lehetővé tétele érdekében a 31. cikk (1) bekezdésének b) pontjával összhangban kinevezett három vezető felvigyázónak KFH-t kell létrehozniuk, hogy egymás között koordináljanak az előkészítő szakaszokban, és koordinálják az általuk felvigyázott, kritikus harmadik fél IKT-szolgáltatók feletti felvigyázási tevékenységek végzését, valamint koordináljanak a 42. cikk alapján esetlegesen szükségessé váló bármely intézkedés során.

(2) Az (1) bekezdés alkalmazásában a vezető felvigyázóknak közös felvigyázási protokollt kell kidolgozniuk, amely meghatározza a napi koordinációs feladatok végzése, valamint a gyors információcsere és reagálás biztosítása érdekében követendő részletes eljárásokat. A protokollt időszakonként felül kell vizsgálni, hogy tükrözze az operatív igényeket, különösen a gyakorlati felvigyázási intézkedések alakulását.

(3) A vezető felvigyázók eseti alapon felkérhetik az EKB-t és az ENISA-t szakvélemény kiadására, gyakorlati tapasztalataik megosztására vagy a KFH bizonyos koordinációs ülésein való részvételre.

35. cikk

A vezető felvigyázó hatáskörei

(1) Az e szakaszban meghatározott feladatok elvégzése céljából a vezető felvigyázó a következő hatáskörökkel rendelkezik a kritikus harmadik fél IKT-szolgáltatók tekintetében:

a) a 37. cikknek megfelelően bekérhet minden releváns információt és dokumentumot;

b) a 38., illetve a 39. cikknek megfelelően általános vizsgálatokat, illetve ellenőrzéseket tarthat;

c) a felvigyázási tevékenységek elvégzését követően jelentést kérhet arról, hogy a kritikus harmadik fél IKT-szolgáltatók milyen intézkedéseket tettek vagy korrekciókat hajtottak végre az e bekezdés d) pontjában említett ajánlásokkal kapcsolatban;

d) ajánlásokat adhat ki a 33. cikk (3) bekezdésében említett területekre, különösen a következőkre vonatkozóan:

   i. specifikus IKT-biztonsági és -minőségi követelmények vagy folyamatok alkalmazása, különösen a javítócsomagok, a frissítések, a titkosítás és azon egyéb biztonsági intézkedések bevezetése kapcsán, amelyek a vezető felvigyázó megítélése szerint relevánsak a pénzügyi szervezeteknek nyújtott szolgáltatások IKT-biztonsága szempontjából;

   ii. a technikai megvalósításra is kiterjedően a kritikus harmadik fél IKT-szolgáltatók által a pénzügyi szervezetek részére nyújtott IKT-szolgáltatásokra vonatkozó feltételek közül azoknak az alkalmazása, amelyek a vezető felvigyázó megítélése szerint relevánsak az egyedi meghibásodási pontok kialakulása, az ezzel kapcsolatos kockázat felerősödése, vagy az IKT-koncentrációs kockázat esetében az uniós pénzügyi ágazat egészére kiterjedő esetleges rendszerszintű hatás csökkentése szempontjából;

   iii. olyan tervezett alvállalkozói tevékenységek, amelyek esetében a vezető felvigyázó megítélése szerint a további alvállalkozásba adás – ideértve a kritikus harmadik fél IKT-szolgáltatók által más kritikus harmadik fél IKT-szolgáltatókkal vagy harmadik országban letelepedett IKT-alvállalkozókkal megkötni tervezett alvállalkozói megállapodásokat is – a 37. és a 38. cikkel összhangban gyűjtött információ vizsgálata alapján kockázatokat eredményezhet a pénzügyi szervezet általi szolgáltatásnyújtásra vagy a pénzügyi stabilitására nézve;

   iv. a további alvállalkozási megállapodástól való tartózkodás, amennyiben a következő kumulatív feltételek teljesülnek:

      – a bevonni tervezett alvállalkozó harmadik fél IKT-szolgáltató vagy harmadik országban letelepedett IKT-alvállalkozó;

      – az alvállalkozó bevonása a pénzügyi szervezet kritikus vagy fontos funkcióinak ellátására irányul; és

– a vezető felvigyázó megítélése szerint az ilyen alvállalkozói szerződés alkalmazása egyértelmű és súlyos kockázatot jelent az Unió pénzügyi stabilitására vagy a pénzügyi szervezetekre nézve, ideértve a pénzügyi szervezetek azon képességét is, hogy megfeleljenek a felügyeleti követelményeknek.

E pont iv. alpontjának alkalmazásában a harmadik fél IKT-szolgáltatóknak a 41. cikk (1) bekezdésének b) pontjában említett sablon használatával továbbítaniuk kell az alvállalkozásba adásra vonatkozó információkat a vezető felvigyázónak.

(2) Az e cikkben említett hatáskörök gyakorlása során a vezető felvigyázó:

a) biztosítja a KFH-n belüli rendszeres koordinációt, és adott esetben következetes megközelítésekre törekszik a kritikus harmadik fél IKT-szolgáltatók felvigyázása tekintetében;

b) megfelelően figyelembe veszi az (EU) 2022/2555 irányelv által létrehozott keretet, és szükség esetén konzultál az említett irányelvvel összhangban kijelölt vagy létrehozott releváns illetékes hatóságokkal, hogy elkerüljék az egymást átfedő technikai és szervezeti intézkedéseket, amelyek az említett irányelv értelmében a kritikus harmadik fél IKT-szolgáltatókra vonatkozhatnak;

c) minimalizálni törekszik a kritikus harmadik fél IKT-szolgáltatók által az e rendelet hatályán kívül eső ügyfeleknek nyújtott szolgáltatások megszakadásának kockázatát.

(3) A vezető felvigyázónak az (1) bekezdésben említett hatáskörök gyakorlását megelőzően egyeztetnie kell a felvigyázási fórummal.

Mielőtt az (1) bekezdés d) pontjával összhangban ajánlásokat adna ki, a vezető felvigyázónak lehetőséget kell biztosítania a harmadik fél IKT-szolgáltató számára, hogy 30 naptári napon belül releváns információkat nyújtson be, amelyek igazolják az e rendelet hatályán kívül eső ügyfelekre gyakorolt várható hatást, és adott esetben kockázatcsökkentő megoldásokat körvonalaznak.

(4) A vezető felvigyázónak tájékoztatnia kell a KFH-t az (1) bekezdés a) és b) pontjában említett hatáskörök gyakorlásának eredményéről. A vezető felvigyázónak az (1) bekezdés c) pontjában említett jelentéseket indokolatlan késedelem nélkül továbbítania kell a KFH-nak és a kritikus harmadik fél IKT-szolgáltató IKT-szolgáltatásait igénybe vevő pénzügyi szervezetek illetékes hatóságainak.

(5) A kritikus harmadik fél IKT-szolgáltatóknak jóhiszeműen együtt kell működniük a vezető felvigyázóval, és segíteniük kell a feladatai ellátásában.

(6) Az (1) bekezdés a), b) és c) pontja szerinti hatáskörök gyakorlása alapján meghozandó intézkedéseknek való teljes vagy részleges meg nem felelés esetén és azon naptól számított legalább 30 naptári nap elteltével, amelyen a kritikus harmadik fél IKT-szolgáltató megkapta a vonatkozó intézkedésekről szóló értesítést, a vezető felvigyázónak határozatot kell elfogadnia, amelyben időszaki büntető bírság kiszabásával kényszeríti a kritikus harmadik fél IKT-szolgáltatót az említett intézkedéseknek való megfelelésre.

(7) A (6) bekezdésben említett időszaki büntető bírságot naponta ki kell szabni a megfelelés eléréséig, a kritikus harmadik fél IKT-szolgáltatónak az időszaki büntető bírság kiszabásáról szóló határozatról való értesítését követő legfeljebb hathónapos időszakban.

(8) Az időszaki büntető bírság összege az időszaki büntető bírság kiszabásáról szóló határozatban megjelölt naptól számítandó, mértéke a kritikus harmadik fél IKT-szolgáltató előző üzleti évben elért átlagos napi világpiaci forgalmának legfeljebb 1 %-a. A büntető bírság összegének meghatározásakor a vezető felvigyázónak a (6) bekezdésben említett intézkedések be nem tartása tekintetében a következő kritériumokat kell figyelembe vennie:

a) a meg nem felelés súlyossága és időtartama;

b) a meg nem felelés szándékos cselekmény vagy gondatlanság eredménye-e;

c) a harmadik fél IKT-szolgáltató és a vezető felvigyázó közötti együttműködés szintje.

Az első albekezdés alkalmazásában – a következetes megközelítés biztosítása érdekében – a vezető felvigyázónak konzultációt kell folytatnia a KFH-n belül.

(9) A büntető bírság közigazgatási jellegű és behajtható. A behajtásra azon tagállam hatályos polgári eljárásjogi szabályai vonatkoznak, amelynek területén az ellenőrzésre és a hozzáférésre sor kerül. A behajtás szabálytalanságára vonatkozó panaszok tekintetében az érintett tagállam bíróságai rendelkeznek joghatósággal. A büntető bírság összege az Európai Unió általános költségvetését illeti.

(10) A vezető felvigyázónak nyilvánosságra kell hoznia minden kiszabott időszaki büntető bírságot, kivéve, ha az ilyen nyilvánosságra hozatal súlyosan veszélyeztetné a pénzügyi piacokat, vagy aránytalan károkat okozna az érintett feleknek.

(11) Az időszaki büntető bírságnak a (6) bekezdés alapján történő kiszabása előtt a vezető felvigyázónak a megállapítások kapcsán meghallgatási lehetőséget kell biztosítania az eljárás alá vont kritikus harmadik fél IKT-szolgáltató képviselői számára, és a határozathozatal során kizárólag azon megállapításokat veheti figyelembe, amelyek kapcsán a kritikus harmadik fél IKT-szolgáltató lehetőséget kapott észrevételei megtételére.

Az eljárás alá vont személyek védelemhez való jogát az eljárás során teljes mértékben tiszteletben kell tartani. Az eljárás alá vont, kritikus harmadik fél IKT-szolgáltatónak jogában áll betekinteni az ügyiratba, amennyiben ez nem sérti más személyeknek az üzleti titkok védelméhez fűződő jogos érdekét. Az ügyiratba való betekintés joga nem terjed ki a bizalmas információkra és a vezető felvigyázó belső előkészítő dokumentumaira.

36. cikk

A vezető felvigyázó hatásköreinek gyakorlása az Unión kívül

(1) Amennyiben a felvigyázási célok nem érhetők el a 31. cikk (12) bekezdésének alkalmazásában létrehozott leányvállalattal való interakcióval vagy a felvigyázási tevékenységeknek az Unióban található telephelyeken történő gyakorlásával, a vezető felvigyázó a következő rendelkezésekben említett hatásköröket bármely olyan, harmadik országban található telephelyen gyakorolhatja, amely egy kritikus harmadik fél IKT-szolgáltató tulajdonában van, vagy amelyet egy kritikus harmadik fél IKT-szolgáltató uniós pénzügyi szervezetek részére történő szolgáltatásnyújtás céljából bármely módon használ az üzleti műveleteivel, funkcióival vagy szolgáltatásaival kapcsolatban – ideértve az adminisztratív, üzleti és üzemeltetési irodákat, telephelyeket, földterületeket, épületeket vagy egyéb ingatlanokat is:

a) a 35. cikk (1) bekezdésének a) pontja; és

b) a 35. cikk (1) bekezdésének b) pontja, összhangban a 38. cikk (2) bekezdésének a), b) és d) pontjával, valamint a 39. cikk (1) bekezdésével és (2) bekezdésének a) pontjával.

Az első albekezdésben említett hatáskörök valamennyi következő feltétel fennállása esetén gyakorolhatók:

i. a vezető felvigyázó szükségesnek tartja egy harmadik országbeli ellenőrzés lefolytatását ahhoz, hogy teljes mértékben és eredményesen el tudja látni az e rendelet szerinti feladatait;

ii. a harmadik országbeli ellenőrzés közvetlenül kapcsolódik az Unióban működő pénzügyi szervezetek számára nyújtott IKT-szolgáltatásokhoz;

iii. az érintett kritikus harmadik fél IKT-szolgáltató hozzájárul egy harmadik országbeli ellenőrzés lefolytatásához; és

iv. a vezető felvigyázó hivatalosan értesítette az érintett harmadik ország releváns hatóságát, és az nem emelt kifogást.

(2) Az uniós intézmények és a tagállamok vonatkozó hatásköreinek sérelme nélkül, az (1) bekezdés alkalmazásában az EBH, az ESMA vagy az EIOPA igazgatási együttműködési megállapodásokat köt a harmadik ország releváns hatóságával annak érdekében, hogy a vezető felvigyázó és az említett harmadik országbeli kiküldetésre kijelölt csoportja az érintett harmadik országban zökkenőmentesen lefolytathassa az ellenőrzéseket. Az említett együttműködési megállapodások nem keletkeztethetnek jogi kötelezettségeket az Unióval és tagállamaival szemben, és nem akadályozhatják meg a tagállamokat és illetékes hatóságaikat abban, hogy két- vagy többoldalú megállapodásokat kössenek az említett harmadik országokkal és azok releváns hatóságaival.

Az említett együttműködési megállapodásoknak tartalmazniuk kell legalább a következő elemeket:

a) az e rendelet alapján végzett felvigyázási tevékenységek és bármely hasonló, az érintett harmadik ország releváns hatósága által folytatott, a harmadik féltől eredő IKT-kockázatnak a pénzügyi ágazatban való nyomon követését célzó tevékenység koordinálására vonatkozó eljárások, beleértve a harmadik ország releváns hatósága által ahhoz adott hozzájárulás továbbításának részletes szabályait, hogy a joghatósága alá tartozó területen a vezető felvigyázó és az általa kijelölt csoport lefolytathassa az (1) bekezdés első albekezdésében említett általános vizsgálatokat és helyszíni ellenőrzéseket;

b) a releváns információknak az EBH, az ESMA vagy az EIOPA, valamint az érintett harmadik ország releváns hatósága közötti továbbításának mechanizmusa, különösen a vezető felvigyázó által a 37. cikk alapján kérhető információkkal kapcsolatban;

c) azon mechanizmusok, amelyek révén az érintett harmadik ország releváns hatósága haladéktalanul értesíti az EBH-t, az ESMA-t vagy az EIOPA-t azon esetekről, amikor úgy tekinthető, hogy egy harmadik országban letelepedett és a 31. cikk (1) bekezdésének a) pontjával összhangban kritikusnak kijelölt IKT-szolgáltató megsértette azon követelményeket, amelyeket az érintett harmadik ország alkalmazandó joga értelmében köteles betartani, amikor az említett harmadik országban pénzügyi intézményeknek nyújt szolgáltatásokat, továbbá az alkalmazott jogorvoslatok és szankciók;

d) az érintett harmadik országban lévő pénzügyi intézmények harmadik féltől eredő IKT-kockázatának nyomon követésével kapcsolatos szabályozási vagy felügyeleti fejleményekkel kapcsolatos naprakész információk rendszeres továbbítása;

e) az annak engedélyezésével kapcsolatos részletek, hogy szükség esetén a harmadik országbeli illetékes hatóság egy képviselője részt vegyen a vezető felvigyázó és a kijelölt csoport által végzett ellenőrzéseken.

(3) Amennyiben a vezető felvigyázó nem képes az (1) és (2) bekezdésben említett, Unión kívüli felvigyázási tevékenységeket végezni, a vezető felvigyázónak:

a) a 35. cikk szerinti hatáskörét a rendelkezésére álló valamennyi tény és dokumentum alapján kell gyakorolnia;

b) dokumentálnia kell és ki kell fejtenie az e cikkben említett tervezett felvigyázási tevékenységek végzésére való képtelenségének lehetséges következményeit.

Az e bekezdés b) pontjában említett lehetséges következményeket figyelembe kell venni a vezető felvigyázónak a 35. cikk (1) bekezdésének d) pontja alapján kiadott ajánlásaiban.

37. cikk

Információkérés

(1) A vezető felvigyázó egyszerű kérés vagy határozat útján előírhatja a kritikus harmadik fél IKT-szolgáltatók számára, hogy adják át a részére az e rendelet szerinti feladatainak elvégzéséhez szükséges információkat, ideértve a releváns üzleti vagy működési dokumentumokat, szerződéseket, szabályzatokat, dokumentációkat, az IKT-biztonsági auditjelentéseket, az IKT-vonatkozású eseményekről készült jelentéseket, valamint az olyan felekkel kapcsolatos információkat, akikhez a kritikus harmadik fél IKT-szolgáltató operatív funkciókat vagy tevékenységeket szervezett ki.

(2) Az (1) bekezdés szerinti egyszerű információkérés megküldésekor a vezető felvigyázónak:

a) a kérés jogalapjaként e cikkre kell hivatkoznia;

b) meg kell jelölnie a kérés célját;

c) pontosan meg kell határoznia a kért információt;

d) meg kell határoznia az információnyújtás határidejét;

e) tájékoztatnia kell a kritikus harmadik fél IKT-szolgáltató azon képviselőjét, akitől az információt kérik, hogy nem köteles megadni az információt, de amennyiben önkéntesen válaszol a kérésre, a nyújtott információ nem lehet helytelen vagy félrevezető.

(3) Az (1) bekezdés szerinti, határozat útján történő információkérés esetén a vezető felvigyázónak:

a) a kérés jogalapjaként e cikkre kell hivatkoznia;

b) meg kell jelölnie a kérés célját;

c) pontosan meg kell határoznia a kért információt;

d) meg kell határoznia az információnyújtás határidejét;

e) meg kell jelölnie a 35. cikk (6) bekezdésében azon esetre előírt időszaki büntető bírságot, amennyiben a kért információk nyújtása hiányos, vagy amikor az ilyen információkat az e bekezdés d) pontjában említett határidőn belül nem biztosítják;

f) meg kell jelölnie azon jogot, hogy – az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 60. és 61. cikkével összhangban – a határozat ellen fellebbezni lehet az EFH fellebbezési tanácsa előtt, és a határozat felülvizsgáltatható az Európai Unió Bíróságával (Bíróság).

(4) A kritikus harmadik fél IKT-szolgáltatók képviselői benyújtják a kért információkat. Megfelelően meghatalmazott ügyvédek az ügyfelük nevében nyújthatják be az információkat. A harmadik fél IKT-szolgáltatók teljes felelősséggel tartoznak, ha a szolgáltatott információ hiányos, helytelen vagy félrevezető.

(5) A vezető felvigyázó a határozat példányának haladéktalan továbbításával tájékoztatja a releváns kritikus harmadik fél IKT-szolgáltatók szolgáltatásait igénybe vevő pénzügyi szervezetek illetékes hatóságait és a KFH-t.

38. cikk

Általános vizsgálatok

(1) Az e rendelet szerinti feladatainak elvégzése érdekében a vezető felvigyázó a 40. cikk 1) bekezdésében említett közös vizsgálócsoport támogatásával – szükség esetén – lefolytathatja a kritikus harmadik fél IKT-szolgáltatók vizsgálatait.

(2) A vezető felvigyázó a következő hatáskörökkel rendelkezik:

a) a feladatainak végrehajtása szempontjából releváns nyilvántartások, adatok, eljárások és egyéb anyagok megvizsgálása, az adathordozótól függetlenül;

b) az ilyen nyilvántartásokból, adatokból, dokumentált eljárásokból és bármely egyéb anyagból hiteles másolatok vagy kivonatok készítése vagy bekérése;

c) a kritikus harmadik fél IKT-szolgáltató képviselőinek felszólítása a személyes megjelenésre, és szóbeli vagy írásbeli magyarázat kérése a vizsgálat tárgyával és céljával összefüggő tényekkel és dokumentumokkal kapcsolatban, valamint a válaszok rögzítése;

d) bármely egyéb olyan természetes vagy jogi személy meghallgatása, aki vagy amely hozzájárul ahhoz, hogy a vizsgálat tárgyával kapcsolatos információgyűjtés céljából meghallgassák;

e) a telefon- és adatforgalmi nyilvántartások kikérése.

(3) Az (1) bekezdésben említett vizsgálat céljából a vezető felvigyázó által felhatalmazott tisztviselőknek és más személyeknek hatáskörük gyakorlásához fel kell mutatniuk a vizsgálat tárgyát és célját feltüntető írásbeli felhatalmazást.

Az említett felhatalmazásban szintén fel kell tüntetni a 35. cikk (6) bekezdésében azon esetre előírt időszaki büntető bírságokat, amennyiben a kért nyilvántartásokat, adatokat, dokumentált eljárásokat vagy egyéb anyagokat nem vagy hiányosan nyújtják be, vagy ha a harmadik fél IKT-szolgáltató képviselői a feltett kérdésekre nem vagy hiányosan válaszolnak.

(4) A kritikus harmadik fél IKT-szolgáltatók képviselői kötelesek alávetni magukat a vezető felvigyázó határozata alapján elrendelt vizsgálatoknak. A határozatban fel kell tüntetni a vizsgálat tárgyát és célját, a 35. cikk (6) bekezdésében előírt időszaki büntető bírságokat, az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet alapján igénybe vehető jogorvoslatokat, valamint azon jogot, hogy a határozat az Európai Unió Bíróságával felülvizsgáltatható.

(5) A vezető felvigyázónak a vizsgálat kezdete előtt kellő időben tájékoztatnia kell a tervezett vizsgálatról és a felhatalmazott személyek személyazonosságáról az említett kritikus harmadik fél IKT-szolgáltató IKT-szolgáltatásait igénybe vevő pénzügyi szervezetek illetékes hatóságait.

A vezető felvigyázónak az első albekezdés alapján átadott valamennyi információt közölnie kell a KFH-val.

39. cikk

Ellenőrzések

(1) Az e rendelet szerinti feladatainak elvégzése érdekében a vezető felvigyázó a 40. cikk (1) bekezdésében említett közös vizsgálócsoportok támogatásával beléphet a harmadik fél IKT-szolgáltatók bármely telephelyére, területére vagy ingatlanára, beleértve a szolgáltató székhelyét, üzemeltetési központjait, egyéb telephelyeit is, és elvégezhet minden szükséges helyszíni ellenőrzést, valamint helyszínen kívüli ellenőrzést végezhet.

Az első albekezdésben említett hatáskörök gyakorlása céljából a vezető felvigyázónak konzultálnia kell a KFH-val.

(2) A vezető felvigyázó által a helyszíni ellenőrzés lefolytatására felhatalmazott tisztviselők és egyéb személyek jogosultak arra, hogy:

a) belépjenek bármely ilyen telephelyre, területre vagy ingatlanra; és

b) az ellenőrzéshez szükséges időre és mértékben zár alá vegyenek bármely ilyen telephelyet, könyvet vagy feljegyzést.

A vezető felvigyázó által felhatalmazott tisztviselőknek és egyéb személyeknek hatáskörük gyakorlásához fel kell mutatniuk az ellenőrzés tárgyát és célját feltüntető írásbeli felhatalmazást, amely megjelöli a 35. cikk (6) bekezdésében azon esetre előírt időszaki büntető bírságokat, amennyiben az érintett kritikus harmadik fél IKT-szolgáltatók képviselői nem vetik alá magukat az ellenőrzésnek.

(3) A vezető felvigyázónak az ellenőrzés kezdete előtt kellő időben értesítést kell küldenie az említett harmadik fél IKT-szolgáltatót igénybe vevő pénzügyi szervezetek illetékes hatóságainak.

(4) Az ellenőrzéseknek ki kell terjedniük a pénzügyi szervezeteknek nyújtott IKT-szolgáltatások teljesítéséhez felhasznált vagy ahhoz hozzájáruló releváns IKT-rendszerek, -hálózatok, -eszközök, -információk és -adatok teljes körére.

(5) A tervezett helyszíni ellenőrzést megelőzően a vezető felvigyázónak észszerű értesítést kell adnia a kritikus harmadik fél IKT-szolgáltatóknak, kivéve, ha az ilyen értesítés veszélyhelyzet vagy válsághelyzet miatt nem lehetséges, vagy ha az meghiúsítaná az eredményes ellenőrzést vagy auditot.

(6) A kritikus harmadik fél IKT-szolgáltatónak alá kell vetnie magát a vezető felvigyázó határozata alapján elrendelt helyszíni ellenőrzéseknek. A határozatban fel kell tüntetni az ellenőrzés tárgyát és célját, rögzíteni kell az ellenőrzés megkezdésének időpontját, valamint meg kell jelölni a 35. cikk (6) bekezdésében előírt időszaki büntető bírságokat, az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet alapján igénybe vehető jogorvoslatokat, valamint azon jogot, hogy a határozat az Európai Unió Bíróságával felülvizsgáltatható.

(7) Amennyiben a vezető felvigyázó által felhatalmazott tisztviselők és más személyek azt állapítják meg, hogy a kritikus harmadik fél IKT-szolgáltató ellenzi az e cikk alapján elrendelt ellenőrzést, a vezető felvigyázónak tájékoztatnia kell a kritikus harmadik fél IKT-szolgáltatót az ilyen ellenkezés következményeiről, beleértve annak lehetőségét, hogy a releváns pénzügyi szervezetek illetékes hatóságai előírják a pénzügyi szervezetek számára, hogy szüntessék meg az említett kritikus harmadik fél IKT-szolgáltatóval kötött szerződéses megállapodásokat.

40. cikk

Folyamatos felvigyázás

(1) A vezető felvigyázót a felvigyázási tevékenységek folytatása során, különösen általános vizsgálatok vagy ellenőrzések lefolytatásakor az egyes kritikus harmadik fél IKT-szolgáltatók tekintetében létrehozott közös vizsgálócsoport támogatja.

(2) Az (1) bekezdésben említett közös vizsgálócsoport a következő intézmények személyzetének tagjaiból áll:

a) az EFH-k;

b) azon releváns illetékes hatóságok, amelyek a kritikus harmadik fél IKT-szolgáltató IKT-szolgáltatásait igénybe vevő pénzügyi szervezeteket felügyelik;

c) a 32. cikk (4) bekezdésének e) pontjában említett illetékes nemzeti hatóság, önkéntes alapon;

d) a kritikus harmadik fél IKT-szolgáltató letelepedésének helye szerinti tagállam egy illetékes nemzeti hatósága, önkéntes alapon.

A közös vizsgálócsoport tagjainak tapasztalattal kell rendelkezniük az IKT-vel kapcsolatos kérdések és a működési kockázatok terén. A közös vizsgálócsoport munkáját a vezető felvigyázó személyzete egy kijelölt tagjának (a továbbiakban: a vezető felvigyázó koordinátora) kell koordinálnia.

(3) A vizsgálat vagy ellenőrzés befejezését követő 3 hónapon belül a vezető felvigyázónak a felvigyázási fórummal történt egyeztetés után a 35. cikkben említett hatáskörében ajánlásokat kell megfogalmaznia a harmadik fél IKT-szolgáltató számára.

(4) A vezető felvigyázónak haladéktalanul közölnie kell a (3) bekezdésben említett ajánlásokat a kritikus harmadik fél IKT-szolgáltatóval és az annak IKT-szolgáltatásait igénybe vevő pénzügyi szervezetek illetékes hatóságaival.

A felvigyázási tevékenységek céljából a vezető felvigyázó figyelembe veheti a kritikus harmadik fél IKT-szolgáltató által rendelkezésére bocsátott, harmadik fél által kiállított tanúsítványokat, valamint harmadik fél által készített belső és külső IKT-audit jelentéseket.

41. cikk

A felvigyázási tevékenységek végzését lehetővé tevő előfeltételek harmonizálása

(1) Az EFH-knak a vegyes bizottság keretében szabályozástechnikai standardtervezeteket kell kidolgozniuk, amelyekben részletesen meghatározzák:

a) a 31. cikk (11) bekezdése szerinti kritikusként való kijelölés iránti saját kezdeményezésű kérelemben a harmadik fél IKT-szolgáltató által benyújtandó információkat;

b) a 35. cikk (1) bekezdése alapján a harmadik fél IKT-szolgáltató által benyújtandó, közzéteendő vagy jelentendő információk tartalmát, struktúráját és formátumát, beleértve az alvállalkozási megállapodásokról szóló információk benyújtására szolgáló sablont is;

c) a közös vizsgálócsoport összetételének meghatározására vonatkozó kritériumokat, amelyek biztosítják az EFH-k és a releváns illetékes hatóságok személyzete tagjainak kiegyensúlyozott részvételét, valamint kijelölésüket, feladataikat és munkafeltételeiket;

d) a kritikus harmadik fél IKT-szolgáltató által a vezető felvigyázó ajánlásai alapján végrehajtott intézkedések alapján a 42. cikk (3) bekezdése szerint végzendő illetékes hatósági értékelés részleteit.

(2) Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. július 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkében megállapított eljárással összhangban az (1) bekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

42. cikk

Az illetékes hatóságok által végzett utókövetés

(1) A vezető felvigyázó által a 35. cikk (1) bekezdésének d) pontja alapján kiadott ajánlások kézhezvételét követő 60 naptári napon belül a kritikus harmadik fél IKT-szolgáltatónak vagy értesítenie kell a vezető felvigyázót arról, hogy végre kívánja hajtani az ajánlásokat, vagy indokolással ellátott magyarázatot kell adnia a vezető felvigyázónak arról, hogy miért nem kívánja végrehajtani az ajánlásokat. A vezető felvigyázónak a kapott tájékoztatást haladéktalanul továbbítania kell az érintett pénzügyi szervezetek illetékes hatóságainak.

(2) A vezető felvigyázónak nyilvánosságra kell hoznia, ha a kritikus harmadik fél IKT-szolgáltató nem értesíti a vezető felvigyázót az (1) bekezdésnek megfelelően, vagy ha a kritikus harmadik fél IKT-szolgáltató által nyújtott magyarázat nem tekinthető elégségesnek. A közzétett információknak tartalmazniuk kell a kritikus harmadik fél IKT-szolgáltató kilétét, valamint a meg nem felelés típusára és jellegére vonatkozó információkat. Az ilyen információknak a nyilvánosság tájékoztatásának biztosítása céljából releváns és arányos mértékre kell korlátozódniuk, kivéve, ha az ilyen közzététel aránytalan kárt okozna az érintett feleknek, vagy súlyosan veszélyeztethetné a pénzügyi piacok szabályos működését és integritását vagy az Unió pénzügyi rendszere egészének vagy egy részének stabilitását.

A vezető felvigyázónak értesítenie kell a harmadik fél IKT-szolgáltatót a nyilvánosságra hozatalról.

(3) Az illetékes hatóságoknak tájékoztatniuk kell a releváns pénzügyi szervezeteket a 35. cikk (1) bekezdésének d) pontjával összhangban megfogalmazott, a kritikus harmadik fél IKT-szolgáltatók számára tett ajánlásokban azonosított kockázatokról.

A harmadik féltől eredő IKT-kockázat kezelése során a pénzügyi szervezeteknek figyelembe kell venniük az első albekezdésben említett kockázatokat.

(4) Amennyiben az illetékes hatóság úgy ítéli meg, hogy a pénzügyi szervezet nem veszi figyelembe vagy nem kezeli megfelelően a harmadik féltől eredő IKT-kockázat saját kezelésén belül az ajánlásokban azonosított konkrét kockázatokat, értesítenie kell a pénzügyi szervezetet annak lehetőségéről, hogy az ilyen kockázatok kezelését célzó megfelelő szerződéses megállapodások hiányában a (6) bekezdés alapján az ilyen értesítés kézhezvételétől számított 60 naptári napon belül határozatot hozzon.

(5) A 35. cikk (1) bekezdésének c) pontjában említett jelentések kézhezvételét követően és az e cikk (6) bekezdésében említett határozat meghozatala előtt az illetékes hatóságok önkéntes alapon konzultálhatnak az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságokkal, amelyek felelősek valamely, kritikus harmadik fél IKT-szolgáltatóként kijelölt, az említett irányelv hatálya alá tartozó alapvető vagy fontos szervezet felügyeletéért.

(6) Az illetékes hatóságok végső eszközként – az értesítést és adott esetben az e cikk (4) és (5) bekezdésében meghatározottak szerinti konzultációt követően – az 50. cikkel összhangban határozhatnak úgy, hogy előírják a pénzügyi szervezetek számára a kritikus harmadik fél IKT-szolgáltató által nyújtott szolgáltatás igénybevételének vagy bevezetésének átmeneti – részleges vagy teljes – felfüggesztését a kritikus harmadik fél IKT-szolgáltató részére megfogalmazott ajánlásokban azonosított kockázatok kezeléséig. Az illetékes hatóságok szükség esetén előírhatják a kritikus harmadik fél IKT-szolgáltatóval kötött, releváns szerződéses megállapodások részleges vagy teljes megszüntetését.

(7) Amennyiben egy kritikus harmadik fél IKT-szolgáltató a vezető felvigyázó által javasolttól eltérő megközelítés alapján elutasítja az ajánlások jóváhagyását, és az ilyen eltérő megközelítés hátrányosan érintheti a pénzügyi szervezetek nagy számát, vagy a pénzügyi ágazat jelentős részét, és az illetékes hatóságok által kiadott egyedi figyelmeztetések nem vezettek a pénzügyi stabilitást fenyegető potenciális kockázatot csökkentő következetes megközelítésekhez, a vezető felvigyázó a felvigyázási fórummal folytatott konzultációt követően adott esetben nem kötelező erejű és nem nyilvános véleményeket fogalmazhat meg az illetékes hatóságok számára a következetes és konvergens felügyeleti utókövetési intézkedések előmozdítása érdekében.

(8) A 35. cikk (1) bekezdésének c) pontjában említett jelentések kézhezvételét követően az illetékes hatóságoknak az e cikk (6) bekezdésében említett határozat meghozatala során figyelembe kell venniük a kritikus harmadik fél IKT-szolgáltató által nem kezelt kockázat jellegét és nagyságát, továbbá a meg nem felelés jelentőségét, szem előtt tartva a következő kritériumokat:

a) a meg nem felelés súlyossága és időtartama;

b) a meg nem felelés súlyos gyengeségeket tárt-e fel a kritikus harmadik fél IKT-szolgáltató eljárásaiban, irányítási rendszereiben, kockázatkezelésében és belső kontrolljaiban;

c) a meg nem felelés megkönnyítette-e pénzügyi bűncselekmény elkövetését, előidézte-e azt, vagy egyébként annak tulajdonítható-e;

d) a meg nem felelés szándékos volt-e, vagy gondatlanság eredménye;

e) a szerződéses megállapodások felfüggesztése vagy megszüntetése kockázatot jelent-e a pénzügyi szervezet üzleti tevékenységeinek folytonosságára nézve, a pénzügyi szervezet arra irányuló erőfeszítéseinek ellenére, hogy elkerülje a szolgáltatásnyújtás zavarát;

f) adott esetben az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott azon illetékes hatóságok – önkéntes alapon, az e cikk (5) bekezdésével összhangban kikért – véleménye, amelyek felelősek valamely, kritikus harmadik fél IKT-szolgáltatóként kijelölt, az említett irányelv hatálya alá tartozó alapvető vagy fontos szervezet felügyeletéért.

Az illetékes hatóságoknak biztosítaniuk kell a pénzügyi szervezetek számára a szükséges időt ahhoz, hogy módosíthassák a kritikus harmadik fél IKT-szolgáltatókkal kötött szerződéses megállapodásaikat a digitális működési rezilienciájukra gyakorolt káros hatások elkerülése érdekében, valamint hogy lehetővé tegyék számukra a kilépési stratégiák és átállási tervek bevezetését, a 28. cikkben említetteknek megfelelően.

(9) Az e cikk (6) bekezdésében említett határozatról értesíteni kell a 32. cikk (4) bekezdésének a), b) és c) pontjában említett felvigyázási fórum tagjait és a KFH-t.

A (6) bekezdésben előírt határozatok által érintett, kritikus harmadik fél IKT-szolgáltatóknak teljes mértékben együtt kell működniük az érintett pénzügyi szervezetekkel, különösen szerződéses megállapodásaik felfüggesztésének vagy felmondásának folyamatával összefüggésben.

(10) Az illetékes hatóságoknak rendszeresen tájékoztatniuk kell a vezető felvigyázót a pénzügyi szervezetekkel kapcsolatos felügyeleti feladataik ellátása során alkalmazott megközelítésekről és intézkedésekről, valamint a pénzügyi szervezetek által azon esetekben alkalmazott szerződéses intézkedésekről, amikor a kritikus harmadik fél IKT-szolgáltatók részben vagy teljes egészében nem hagyták jóvá a vezető felvigyázó nekik szóló ajánlásait.

(11) A vezető felvigyázó kérésre további pontosításokat adhat a kiadott ajánlásokkal kapcsolatban, hogy iránymutatást nyújtson az illetékes hatóságoknak az utókövetési intézkedésekkel kapcsolatban.

43. cikk

Felvigyázási díjak

(1) A vezető felvigyázónak – az e cikk (2) bekezdésében említett, felhatalmazáson alapuló jogi aktussal összhangban – díjakat kell felszámítania a kritikus harmadik fél IKT-szolgáltatókkal szemben, amelyek teljes mértékben fedezik a vezető felvigyázónál az e rendelet alapján végzett felvigyázási feladatokkal kapcsolatban felmerült szükséges kiadásokat, beleértve azon költségek megtérítését, amelyek a 40. cikkben említett közös vizsgálócsoport által végzett munka eredményeként merülhetnek fel, valamint a 32. cikk (4) bekezdésének második albekezdésében említett független szakértők által a közvetlen felvigyázási tevékenységek hatóköre alá tartozó kérdésekkel kapcsolatos tanácsadás költségeinek megtérítését is.

A kritikus harmadik fél IKT-szolgáltatónak felszámított díj összegének fedeznie kell az e szakaszban előírt feladatok ellátásából eredő valamennyi költséget, és arányosnak kell lennie annak forgalmával.

(2) A Bizottság felhatalmazást kap arra, hogy az 57. cikkel összhangban felhatalmazáson alapuló jogi aktust fogadjon el, amely a díj összegének és a díjfizetés 2024. július 17-ig történő megfizetése módjának meghatározásával kiegészíti ezt a rendeletet.

44. cikk

Nemzetközi együttműködés

(1) A 36. cikk sérelme nélkül az EBH, az ESMA és az EIOPA az 1093/2010/EU, az 1095/2010/EU és az 1094/2010/EU rendelet 33. cikkével összhangban igazgatási megállapodásokat köthet harmadik országbeli szabályozó és felügyeleti hatóságokkal annak érdekében, hogy előmozdítsa a különböző pénzügyi ágazatokra kiterjedő, harmadik féltől eredő IKT-kockázattal kapcsolatos nemzetközi együttműködést, különösen legjobb gyakorlatok kidolgozásával az IKT-kockázatkezelési gyakorlatok és kontroll, a kockázatcsökkentő intézkedések és az IKT-biztonsági eseményekre való reagálásra irányuló intézkedések területén.

(2) Az EFH-knak a vegyes bizottság keretében ötévenként közös, bizalmas jelentést kell benyújtaniuk be az Európai Parlamentnek, a Tanácsnak és a Bizottságnak, amelyben összefoglalják az (1) bekezdésben említett harmadik országbeli hatóságokkal folytatott releváns egyeztetések megállapításait, kiemelt figyelmet fordítva a harmadik féltől eredő IKT-kockázat alakulására, valamint a pénzügyi stabilitással, a piaci integritással, a befektetővédelemmel és a belső piac működésével kapcsolatos vonatkozásokra.

VI. FEJEZET

Információmegosztásra vonatkozó megállapodások

45. cikk

A kiberfenyegetéssel kapcsolatos információk és hírszerzés megosztására vonatkozó megállapodások

(1) A pénzügyi szervezetek kiberfenyegetésekkel kapcsolatban többek között az illetéktelen hozzáférésre utaló körülményekre, taktikákra, módszerekre, eljárásokra, kiberbiztonsági riasztásokra és konfigurációs eszközökre is kiterjedő információkat és hírszerzést oszthatnak meg egymással, amennyiben az ilyen információ- és hírszerzés-megosztás:

a) arra irányul, hogy a pénzügyi szervezetek javíthassák digitális működési rezilienciájukat, különösen a kiberfenyegetésekkel kapcsolatos tudatosság növelésével, a kiberfenyegetések terjedési képességének korlátozásával vagy megakadályozásával, a védelmi képességek, a fenyegetésészlelési módszerek, a mérséklési stratégiák vagy a reagálási és helyreállítási megoldások támogatásával;

b) pénzügyi szervezetek megbízható közösségein belül történik;

c) olyan információmegosztási megállapodások keretében történik, amelyek védik a megosztott információk esetlegesen érzékeny jellegét, és amelyek irányadó magatartási szabályai biztosítják az üzleti titoktartás, a személyes adatoknak az (EU) 2016/679 rendelettel összhangban történő védelme, valamint a versenypolitikára vonatkozó iránymutatások maradéktalan betartását.

(2) Az (1) bekezdés c) pontjának alkalmazásában az információmegosztási megállapodásoknak meg kell határozniuk a részvétel feltételeit, valamint adott esetben rögzíteniük kell a hatóságok bevonásának részleteit és azt, hogy azok milyen minőségben kapcsolódhatnak az információmegosztási megállapodásokhoz, a harmadik fél IKT-szolgáltatók bevonásának részleteit és a működési elemeket, ideértve a célzott informatikai platformok alkalmazását.

(3) A pénzügyi szervezeteknek értesíteniük kell az illetékes hatóságokat az (1) bekezdésben említett információmegosztási megállapodásban való részvételükről a tagságuk érvényesítésekor, vagy adott esetben a tagságuk megszűnéséről annak hatálybalépésekor.

VII. FEJEZET

Illetékes hatóságok

46. cikk

Illetékes hatóságok

A harmadik fél IKT-szolgáltatókra vonatkozó, e rendelet V. fejezetének II. szakaszában említett felvigyázási keretrendszer rendelkezéseinek sérelme nélkül az e rendeletnek való megfelelést a vonatkozó jogi aktusokban rájuk ruházott hatásköröknek megfelelően a következő illetékes hatóságok biztosítják:

a) hitelintézetek és a 2013/36/EU irányelv alapján mentesített intézmények esetében az említett irányelv 4. cikkével összhangban kijelölt illetékes hatóság, valamint az 1024/2013/EU rendelet 6. cikke (4) bekezdésével összhangban jelentősnek minősített hitelintézetek esetében az EKB, az említett rendeletben rá ruházott hatáskörökkel és feladatokkal összhangban;

b) pénzforgalmi intézmények, többek között az (EU) 2015/2366 irányelv alapján mentesített pénzforgalmi intézmények, elektronikuspénz-kibocsátó intézmények, többek között a 2009/110/EK irányelv alapján mentesített elektronikuspénz-kibocsátó intézmények és az (EU) 2015/2366 irányelv 33. cikkének (1) bekezdésében említett, számlainformációkat összesítő szolgáltatók esetében az (EU) 2015/2366 irányelv 22. cikkével összhangban kijelölt illetékes hatóság;

c) befektetési vállalkozások esetében az (EU) 2019/2034 európai parlamenti és tanácsi irányelv ([38]) 4. cikkével összhangban kijelölt illetékes hatóság;

d) a kriptoeszközök piacairól szóló rendelet alapján engedélyezett kriptoeszköz-szolgáltatók és az eszközalapú tokenek kibocsátói esetében az említett rendelet releváns rendelkezésével összhangban kijelölt illetékes hatóság;

e) központi értéktárak esetében a 909/2014/EU rendelet 11. cikkével összhangban kijelölt illetékes hatóság;

f) központi szerződő felek esetében a 648/2012/EU rendelet 22. cikkével összhangban kijelölt illetékes hatóság;

g) kereskedési helyszínek és adatszolgáltatók esetében a 2014/65/EU irányelv 67. cikkével összhangban kijelölt illetékes hatóság és a 600/2014/EU rendelet 2. cikke (1) bekezdésének 18. pontjában meghatározott illetékes hatóság;

h) kereskedési adattárak esetében a 648/2012/EU rendelet 22. cikkével összhangban kijelölt illetékes hatóság;

i) alternatívbefektetésialap-kezelők esetében a 2011/61/EU irányelv 44. cikkével összhangban kijelölt illetékes hatóság;

j) alapkezelő társaságok esetében a 2009/65/EK irányelv 97. cikkével összhangban kijelölt illetékes hatóság;

k) biztosítók és viszontbiztosítók esetében a 2009/138/EK irányelv 30. cikkével összhangban kijelölt illetékes hatóság;

l) biztosításközvetítők, viszontbiztosítás-közvetítők és kiegészítő biztosításközvetítői tevékenységet végző személyek esetében az (EU) 2016/97 irányelv 12. cikkével összhangban kijelölt illetékes hatóság;

m) foglalkoztatói nyugellátást szolgáltató intézmények esetében az (EU) 2016/2341 irányelv 47. cikkével összhangban kijelölt illetékes hatóság;

n) hitelminősítő intézetek esetében az 1060/2009/EK rendelet 21. cikkével összhangban kijelölt illetékes hatóság;

o) kritikus referenciamutatók kezelői esetében az (EU) 2016/1011 rendelet 40. és 41. cikkével összhangban kijelölt illetékes hatóság;

([38]) Az Európai Parlament és a Tanács (EU) 2019/2034 irányelve (2019. november 27.) a befektetési vállalkozások prudenciális felügyeletéről, valamint a 2002/87/EK, a 2009/65/EK, a 2011/61/EU, a 2013/36/EU, a 2014/59/EU és a 2014/65/EU irányelv módosításáról (HL L 314., 2019.12.5., 64. o.).

p) közösségi finanszírozási szolgáltatók esetében az (EU) 2020/1503 rendelet 29. cikkével összhangban kijelölt illetékes hatóság;

q) értékpapírosítási adattárak esetében az (EU) 2017/2402 rendelet 10. cikkével és 14. cikkének (1) bekezdésével összhangban kijelölt illetékes hatóság.

47. cikk

Együttműködés az (EU) 2022/2555 irányelvvel létrehozott struktúrákkal és hatóságokkal

(1) Az együttműködés elősegítése, valamint az e rendelet alapján kijelölt illetékes hatóságok és az (EU) 2022/2555 irányelv 14. cikkével létrehozott együttműködési csoport közötti felügyeleti kapcsolattartás lehetővé tétele érdekében az EFH-k és az illetékes hatóságok részt vehetnek az együttműködési csoport tevékenységeiben a pénzügyi szervezetekhez kapcsolódó felügyeleti tevékenységeiket illető kérdésekben. Az EFH-k és az illetékes hatóságok kérhetik, hogy felkérjék őket az együttműködési csoport tevékenységeiben való részvételre az (EU) 2022/2555 irányelv hatálya alá tartozó, azon alapvető vagy fontos szervezetekhez kapcsolódó kérdések tekintetében, amelyeket harmadik fél IKT-szolgáltatóként is kijelöltek e rendelet 31. cikkének értelmében.

(2) Adott esetben az illetékes hatóságok konzultálhatnak, és megoszthatnak információkat az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott egyedüli kapcsolattartó pontokkal és a CSIRT-ekkel.

(3) Az illetékes hatóságok adott esetben releváns szakvéleményt és technikai segítségnyújtást kérhetnek az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságoktól, és együttműködési megállapodásokat köthetnek a hatékony és gyors reagálásra képes koordinációs mechanizmusok létrehozása érdekében.

(4) Az e cikk (3) bekezdésében említett megállapodások meghatározhatják többek között az (EU) 2022/2555 irányelv hatálya alá tartozó, azon alapvető vagy fontos szervezetekkel kapcsolatos felügyeleti és felvigyázási tevékenységek koordinációjára vonatkozó eljárásokat, amelyeket e rendelet 31. cikke alapján harmadik fél IKT-szolgáltatókként jelöltek ki, beleértve a vizsgálatok és helyszíni ellenőrzések nemzeti joggal összhangban történő lefolytatása, továbbá az e rendelet szerinti illetékes hatóságok és az említett irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságok közötti, olyan információcserére vonatkozó mechanizmusok tekintetében, amely magában foglalja az utóbbi hatóságok által kért információkhoz való hozzáférést is.

48. cikk

A hatóságok közötti együttműködés

(1) Az illetékes hatóságoknak szorosan együtt kell működniük egymással és adott esetben a vezető felvigyázóval.

(2) Az illetékes hatóságoknak és a vezető felvigyázónak megfelelő időben kölcsönösen ki kell cserélniük egymással a harmadik fél IKT-szolgáltatókra vonatkozó minden olyan releváns információt, amely az e rendelet szerinti feladataik ellátásához szükséges, különösen a vezető felvigyázó felvigyázási feladatainak részeként azonosított kockázatokkal, megközelítésekkel és intézkedésekkel kapcsolatban.

49. cikk

Több pénzügyi ágazatra kiterjedő műveletek, kommunikáció és együttműködés

(1) Az EFH-k a vegyes bizottságon keresztül és együttműködve adott esetben az illetékes hatóságokkal, a 2014/59/EU irányelv 3. cikkében említett szanálási hatóságokkal, az EKB-val, a 806/2014/EU rendelet hatálya alá tartozó szervezetekre vonatkozó információk tekintetében az Egységes Szanálási Testülettel, az ERKT-val, valamint az ENISA-val mechanizmusokat alakíthatnak ki, amelyek lehetővé teszik az eredményes módszerek pénzügyi ágazatok közötti megosztását a helyzetismeret javítása, valamint az egyes ágazatok tekintetében közös kiber-sérülékenységek és -kockázatok azonosítása céljából.

Válságkezelési és vészhelyzeti műveleteket dolgozhatnak ki kibertámadási forgatókönyvek felhasználásával kommunikációs csatornák kialakítása, valamint az eredményes, koordinált uniós szintű reagálás fokozatos lehetővé tétele érdekében, hogy kezelhessék a jelentős, határokon átnyúló IKT-vonatkozású eseményeket vagy az azokhoz kapcsolódó fenyegetéseket, amelyek rendszerszintű hatással lehetnek az uniós pénzügyi ágazat egészére.

Az említett műveletek adott esetben tesztelhetik a pénzügyi ágazat más gazdasági ágazatoktól való függőségeit is.

(2) Az illetékes hatóságoknak, az EFH-knak és az EKB-nek szorosan együtt kell működniük és információcserét kell folytatniuk a 47–54. cikk szerinti feladataik ellátása céljából. Felügyeleti tevékenységüket szorosan összehangolva kell végezniük annak érdekében, hogy azonosítsák és orvosolják e rendelet megsértésének eseteit, kidolgozzák és terjesszék a bevált módszereket, megkönnyítsék az együttműködést, előmozdítsák az egységes értelmezést, továbbá vitás esetekben joghatóságokon átívelő értékelést készítsenek.

50. cikk

Közigazgatási szankciók és korrekciós intézkedések

(1) Az illetékes hatóságoknak rendelkezniük kell minden olyan felügyeleti, vizsgálati és szankcionálási hatáskörrel, amely az e rendelet szerinti feladataik ellátásához szükséges.

(2) Az (1) bekezdésben említett hatásköröknek legalább a következő hatásköröket kell magukban foglalniuk:

a) bármilyen formájú betekintés bármilyen iratba vagy adatba, amelyet az illetékes hatóság feladatainak teljesítése szempontjából relevánsnak ítél, valamint másolat beszerzése vagy készítése azokról;

b) helyszíni ellenőrzések vagy vizsgálatok elvégzése, amelyek magukban foglalják többek között a következőket, ugyanakkor nem korlátozódnak azokra:

   i. a pénzügyi szervezetek képviselőinek felszólítása szóbeli vagy írásbeli magyarázatok szolgáltatására a vizsgálat tárgyával és céljával összefüggő tényekkel és dokumentumokkal kapcsolatban, valamint a válaszok rögzítése;

   ii. bármely egyéb olyan természetes vagy jogi személy meghallgatása, aki vagy amely hozzájárul ahhoz, hogy a vizsgálat tárgyával kapcsolatos információgyűjtés céljából meghallgassák;

c) az e rendeletben meghatározott követelmények megsértésével kapcsolatos korrekciós intézkedések előírása.

(3) A tagállamok azon jogának sérelme nélkül, hogy az 52. cikkel összhangban büntetőjogi szankciókat szabjanak ki, a tagállamok meghatározzák az e rendelet megsértése esetén alkalmazandó megfelelő közigazgatási szankciók és korrekciós intézkedések megállapításának szabályait, és biztosítják azok eredményes végrehajtását.

A szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük.

(4) A tagállamok hatáskörrel ruházzák fel az illetékes hatóságokat arra, hogy e rendelet megsértése esetén legalább a következő közigazgatási szankciókat vagy korrekciós intézkedéseket alkalmazzák:

a) végzés kibocsátása, amely előírja a természetes vagy jogi személy számára, hogy hagyjon fel az ezen rendeletet sértő magatartással, és tartózkodjon a magatartás megismétlésétől;

b) az illetékes hatóság által e rendelet rendelkezéseivel ellentétesnek ítélt gyakorlat vagy magatartás ideiglenes vagy tartós beszüntetésének az előírása, és az ilyen gyakorlat vagy magatartás ismételt előfordulásának a megakadályozása;

c) bármilyen típusú, akár pénzügyi jellegű intézkedés meghozatala, amely biztosítja, hogy a pénzügyi szervezetek folyamatosan betartsák a jogszabályi követelményeket;

d) amilyen mértékig ezt a nemzeti jog megengedi, a meglévő, valamely távközlési üzemeltető birtokában lévő adatforgalmi nyilvántartások bekérése, amennyiben észszerűen feltételezhető e rendelet megsértése, és amennyiben ezen nyilvántartások relevánsak lehetnek e rendelet megsértésének kivizsgálása szempontjából; és

e) nyilvános közlemény kiadása, ideértve a rendeletet megsértő természetes vagy jogi személy személyazonosságának és a jogsértés jellegének nyilvános közzétételét is.

(5) Amennyiben a (2) bekezdés c) pontjában és a (4) bekezdésben említett rendelkezések jogi személyekre alkalmazandók, a tagállamok arra vonatkozó hatáskört ruháznak az illetékes hatóságokra, hogy a közigazgatási szankciókat és korrekciós intézkedéseket – a nemzeti jogban megállapított feltételek mellett – a vezető testület azon tagjaira és más olyan egyénekre is alkalmazzák, akik a nemzeti jog szerint felelősséggel tartoznak a rendelet megsértéséért.

(6) A tagállamok biztosítják, hogy a (2) bekezdés c) pontjában meghatározott közigazgatási szankciókat vagy korrekciós intézkedéseket kiszabó bármely határozatot kellően megindokolják, és azzal szemben jogorvoslattal lehessen élni.

51. cikk

A közigazgatási szankciók és korrekciós intézkedések kiszabására vonatkozó hatáskörök gyakorlása

(1) Az illetékes hatóságoknak az 50. cikkben említett közigazgatási szankciók és korrekciós intézkedések kiszabására vonatkozó hatáskörüket adott esetben a nemzeti jogi kereteikkel összhangban kell gyakorolniuk a következők szerint:

a) közvetlenül;

b) más hatóságokkal együttműködve;

c) saját felelősségi körükön belül, más hatóságokra történő hatáskör-átruházás útján; vagy

d) az illetékes igazságügyi hatóságok megkeresése útján.

(2) Az illetékes hatóságoknak az e rendelet 50. cikke alapján kiszabandó közigazgatási szankció vagy korrekciós intézkedés típusának és szintjének meghatározása során figyelembe kell venniük, hogy a jogsértés mennyiben szándékos, vagy mennyiben származik gondatlanságból, valamint minden egyéb releváns körülményt, többek között – adott esetben – a következőket:

a) a jogsértés lényegessége, súlyossága és időtartama;

b) a jogsértésért felelős természetes vagy jogi személy felelősségének mértéke;

c) a felelős természetes vagy jogi személy pénzügyi stabilitása;

d) a felelős természetes vagy jogi személy által elért nyereség vagy elkerült veszteség fontossága, amennyiben azok meghatározhatók;

e) a jogsértés által harmadik feleknek okozott veszteség, amennyiben az meghatározható;

f) a felelős természetes vagy jogi személynek az illetékes hatósággal való együttműködésének szintje, nem érintve annak szükségességét, hogy biztosítani kell az említett természetes vagy jogi személy által – nyereség elérésével vagy veszteség elkerülésével – szerzett haszon visszaszolgáltatását;

g) a felelős természetes vagy jogi személy által elkövetett korábbi jogsértések.

52. cikk

Büntetőjogi szankciók

(1) A tagállamok dönthetnek úgy, hogy a nemzeti joguk alapján büntetőjogi szankciók hatálya alá tartozó jogsértésekre vonatkozóan nem állapítanak meg közigazgatási szankciókat vagy korrekciós intézkedéseket előíró szabályokat.

(2) Amennyiben a tagállamok úgy döntöttek, hogy büntetőjogi szankciókat írnak elő e rendelet megsértésére vonatkozóan, megfelelő intézkedésekkel biztosítják, hogy az illetékes hatóságok rendelkezzenek az ahhoz szükséges hatáskörökkel, hogy a joghatóságukon belül kapcsolatba lépjenek az igazságügyi, bűnüldöző vagy egyéb bűnügyi igazságszolgáltatási hatóságokkal annak érdekében, hogy az e rendelet megsértése miatt indított bűnügyi nyomozásokhoz vagy eljárásokhoz kapcsolódó konkrét információkat szerezzenek be, és azokat továbbítsák más illetékes hatóságoknak és az EBH-nak, az ESMA-nak vagy az EIOPA-nak, hogy e rendelet céljából teljesítsék együttműködési kötelezettségeiket.

53. cikk

Értesítési kötelezettség

A tagállamok 2025. január 17-ig értesítik a Bizottságot, az ESMA-t, az EBH-t és az EIOPA-t az e fejezetet végrehajtó törvényi, rendeleti és közigazgatási rendelkezésekről, ideértve bármely releváns büntetőjogi rendelkezést is. A tagállamok indokolatlan késedelem nélkül értesítik a Bizottságot, az ESMA-t, az EBH-t és az EIOPA-t az e rendelkezéseket érintő későbbi módosításokról is.

54. cikk

A közigazgatási szankciók nyilvánosságra hozatala

(1) Az illetékes hatóságoknak a hivatalos honlapjukon haladéktalanul közzé kell tenniük bármely, közigazgatási szankciót kiszabó határozatot, amellyel szemben nincs helye fellebbezésnek azt követően, hogy a szankció címzettjét értesítették az említett határozatról.

(2) Az (1) bekezdésben említett közzétételnek ki kell kiterjednie a jogsértés típusára és jellegére vonatkozó információkra, valamint a felelős személyek személyazonosságára és a kiszabott szankciókra.

(3) Amennyiben az illetékes hatóság eseti értékelés alapján úgy ítéli meg, hogy a jogi személyek kilétének vagy a természetes személyek személyazonosságának és személyes adatainak a közzététele aránytalan lenne, többek között a személyes adatok védelméhez kapcsolódó kockázatok miatt, vagy a közzététel veszélyeztetné a pénzügyi piacok stabilitását vagy egy folyamatban lévő nyomozást, vagy – amennyiben annak mértéke megállapítható – az érintett személynek aránytalan kárt okozna, az illetékes hatóságnak a közigazgatási szankciót kiszabó határozat tekintetében a következő megoldások egyikét kell alkalmaznia:

a) elhalasztja a közzétételt addig, amíg a közzététel ellen szóló indokok meg nem szűnnek;

b) a határozatot a nemzeti jogszabályokkal összhangban anonim jelleggel teszi közzé; vagy

c) mellőzi a közzétételt akkor, ha úgy ítéli meg, hogy az a) és b) pont szerinti megoldások elégtelenek, vagy nem garantálják, hogy a pénzügyi piacok stabilitása nem kerül veszélybe, vagy ha az ilyen közzététel nem állna arányban a kiszabott szankció engedékenységével.

(4) A közigazgatási szankció anonim közzétételéről szóló, a (3) bekezdés b) pontja szerinti határozat meghozatala esetén a releváns adatok közzététele elhalasztható.

(5) Amennyiben az illetékes hatóság olyan közigazgatási szankciót elrendelő határozatot tesz közzé, amely ellen az illetékes igazságügyi hatóságnál fellebbezés van folyamatban, az illetékes hatóságnak a hivatalos honlapján haladéktalanul közzé kell tennie az említett információt és bármely későbbi, az ilyen fellebbezés eredményével kapcsolatos információkat is. A közigazgatási szankciót elrendelő határozatot megsemmisítő bírósági határozatokat szintén közzé kell tenni.

(6) Az illetékes hatóságoknak biztosítaniuk kell, hogy az (1)–(4) bekezdésben említett bármely közzététel csak azon időszakra maradjon hivatalos honlapjukon, amely szükséges e cikk érvényesítéséhez. Ezen időszak nem haladhatja meg a közzétételtől számított öt évet.

55. cikk

Szakmai titoktartás

(1) A szakmai titoktartásnak a (2) bekezdésben meghatározott feltételeit az e rendelet alapján megkapott, kicserélt vagy továbbított minden bizalmas információra alkalmazni kell.

(2) Szakmai titoktartási kötelezettség alkalmazandó minden olyan személyre, aki az e rendelet szerint kijelölt illetékes hatóságnak vagy olyan hatóságnak vagy piaci vállalkozásnak vagy természetes vagy jogi személynek dolgozik vagy dolgozott, akire vagy amelyre az illetékes hatóság hatásköröket ruházott át, beleértve az illetékes hatóság által megbízott ellenőröket és szakértőket is.

(3) A szakmai titoktartás hatálya alá tartozó információk – többek között az e rendelet szerinti illetékes hatóságok és az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságok közötti információcsere – semmilyen más személlyel vagy hatósággal nem közölhetők, kivéve, ha ezt uniós vagy nemzeti joggal megállapított rendelkezések írják elő.

(4) Az e rendelet alapján az illetékes hatóságok között folytatott bármilyen, üzleti vagy működési feltételekkel, valamint más gazdasági vagy személyes jellegű ügyekkel kapcsolatos információcsere bizalmas adatközlésnek minősül, és a szakmai titoktartás követelményeinek hatálya alá tartozik, kivéve, ha az illetékes hatóság az információközléssel egyidejűleg megállapítja, hogy az ilyen információ nyilvánosságra hozható, vagy ha az ilyen nyilvánosságra hozatalt bírósági eljárás teszi szükségessé.

56. cikk

Adatvédelem

(1) Az EFH-k és az illetékes hatóságok csak akkor kezelhetnek személyes adatokat, ha az az e rendelet szerinti kötelezettségeik és feladataik teljesítéséhez szükséges, különösen vizsgálat, ellenőrzés, információkérés, kommunikáció, közzététel, értékelés, ellenőrzés, felmérés és felvigyázási tervek kidolgozása céljából. A személyes adatokat az (EU) 2016/679 vagy az (EU) 2018/1725 rendelettel összhangban kell kezelni, attól függően, hogy a két rendelet közül melyik alkalmazandó.

(2) Amennyiben más ágazati jogi aktusok másként nem rendelkeznek, az (1) bekezdésben említett személyes adatok az alkalmazandó felügyeleti feladatok teljesítéséig, de legfeljebb 15 évig őrizhetők meg, kivéve, ha az ilyen adatok további megőrzését igénylő bírósági eljárás van folyamatban.

VIII. FEJEZET

Felhatalmazáson alapuló jogi aktusok

57. cikk

A felhatalmazás gyakorlása

(1) A felhatalmazáson alapuló jogi aktusok elfogadására vonatkozóan a Bizottság részére adott felhatalmazás gyakorlásának feltételeit ez a cikk határozza meg.

(2) A Bizottságnak a 31. cikk (6) bekezdésében és a 43. cikk (2) bekezdésében említett, felhatalmazáson alapuló jogi aktus elfogadására vonatkozó felhatalmazása ötéves időtartamra szól 2024. január 17-én kezdődő hatállyal. A Bizottság legkésőbb kilenc hónappal az ötéves időtartam letelte előtt jelentést készít a felhatalmazásról. Amennyiben az Európai Parlament vagy a Tanács nem ellenzi a meghosszabbítást legkésőbb három hónappal az egyes időtartamok letelte előtt, a felhatalmazás hallgatólagosan meghosszabbodik a korábbival megegyező időtartamra.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 31. cikk (6) bekezdésében és a 43. cikk (2) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon, vagy a benne megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

(4) A felhatalmazáson alapuló jogi aktus elfogadása előtt a Bizottság a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban megállapított elvekkel összhangban konzultál az egyes tagállamok által kijelölt szakértőkkel.

(5) A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul és egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.

(6) A 31. cikk (6) bekezdése és a 43. cikk (2) bekezdése értelmében elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha az Európai Parlamentnek és a Tanácsnak a jogi aktusról való értesítését követő három hónapon belül sem az Európai Parlament, sem a Tanács nem emelt ellene kifogást, illetve ha az említett időtartam lejártát megelőzően mind az Európai Parlament, mind a Tanács arról tájékoztatta a Bizottságot, hogy nem fog kifogást emelni. Az Európai Parlament vagy a Tanács kezdeményezésére ez az időtartam három hónappal meghosszabbodik.

IX. FEJEZET

Átmeneti és záró rendelkezések

I. szakasz

58. cikk

Felülvizsgálati záradék

(1) A Bizottság 2028. január 17-ig – adott esetben az EFH-kkal és az ERKT-val folytatott konzultációt követően – felülvizsgálatot végez, és – adott esetben jogalkotási javaslattal együtt – jelentést nyújt be az Európai Parlamentnek és a Tanácsnak. A felülvizsgálatnak ki kell terjednie legalább a következőkre:

a) a harmadik fél IKT-szolgáltatóknak a 31. cikk (2) bekezdése szerinti kijelölésére vonatkozó kritériumok;

b) a 19. cikkben említett, jelentős kiberfenyegetésekről szóló értesítés önkéntes jellege;

c) a 31. cikk (12) bekezdésében említett rendszer és a vezető felvigyázónak a 35. cikk (1) bekezdése d) pontja iv. alpontjának első francia bekezdésében meghatározott hatásköre, annak értékelése céljából, hogy az említett rendelkezések mennyire hatékonyak a harmadik országban letelepedett, harmadik fél IKT-szolgáltatók hatékony felvigyázásának biztosítása tekintetében, valamint hogy szükség van-e leányvállalat létrehozására az Unióban.

   E pont első albekezdésének alkalmazásában a felülvizsgálatnak ki kell terjednie a 31. cikk (12) bekezdésében említett rendszer elemzésére, többek között az uniós pénzügyi szervezetek harmadik országokból származó szolgáltatásokhoz való hozzáférését és az ilyen szolgáltatásoknak az uniós piacon való rendelkezésre állását illetően, és figyelembe kell vennie az e rendelet hatálya alá tartozó szolgáltatások piacán bekövetkező további fejleményeket, a pénzügyi szervezeteknek, illetve a pénzügyi felügyeleteknek az említett rendszer alkalmazása, illetve felügyelete tekintetében szerzett gyakorlati tapasztalatait, valamint a nemzetközi szinten bekövetkező releváns szabályozási és felügyeleti fejleményeket;

d) arra, hogy helyénvaló-e e rendelet hatálya alá vonni a 2. cikk (3) bekezdésének e) pontjában említett, automatizált értékesítési rendszereket alkalmazó pénzügyi szervezeteket az ilyen rendszerek használatával kapcsolatos jövőbeli piaci fejlemények fényében;

e) a KFH működése és hatékonysága a felvigyázás következetességének és a felvigyázási keretrendszeren belüli információcsere hatékonyságának támogatása terén.

(2) Az (EU) 2015/2366 irányelv felülvizsgálatával összefüggésben a Bizottság értékeli, hogy szükség van-e a fizetési rendszerek és a fizetésfeldolgozási tevékenységek kiber-rezilienciájának növelésére, valamint azt, hogy helyénvaló-e e rendelet hatályát kiterjeszteni a fizetési rendszerek üzemeltetőire és a fizetésfeldolgozási tevékenységekben részt vevő szervezetekre. Ezen értékelés fényében a Bizottság az (EU) 2015/2366 irányelv felülvizsgálatának részeként legkésőbb 2023. július 17-ig jelentést nyújt be az Európai Parlamentnek és a Tanácsnak.

Az említett felülvizsgálati jelentés alapján, valamint az EFH-kal, az EKB-val és az ERKT-val folytatott konzultációt követően a Bizottság – adott esetben és azon jogalkotási javaslat részeként, amelyet az (EU) 2015/2366 irányelv 108. cikkének második bekezdése alapján fogadhat el – javaslatot nyújthat be annak biztosítására, hogy valamennyi fizetésirendszer-üzemeltető és valamennyi fizetésfeldolgozási tevékenységekben részt vevő szervezet megfelelő felvigyázás alatt álljon, figyelembe véve ugyanakkor a központi bank általi meglévő felügyeletet.

(3) A Bizottság 2026. január 17-ig – az EFH-kkal és a Európai Könyvvizsgálat-felügyeleti Szervek Bizottságával való konzultációt követően – felülvizsgálatot végez és indokolt esetben jogalkotási javaslattal együtt jelentést nyújt be az Európai Parlamentnek és a Tanácsnak a jogszabály szerint engedélyezett könyvvizsgálókra és könyvvizsgáló cégekre vonatkozó megerősített követelményeknek a digitális működési reziliencia tekintetében való megfelelőségéről a jogszabály szerint engedélyezett könyvvizsgálóknak és könyvvizsgáló cégeknek e rendelet hatálya alá vonása vagy a 2006/43/EK európai parlamenti és tanácsi irányelv ([39]) módosítása révén.

II. szakasz

Módosítások

59. cikk

Az 1060/2009/EK rendelet módosításai

Az 1060/2009/EK rendelet a következőképpen módosul:

1. Az I. melléklet A. szakasza 4. pontja első albekezdésének helyébe a következő szöveg lép:

„A hitelminősítő intézetnek megbízható adminisztratív és számviteli eljárásokkal, belső ellenőrzési mechanizmusokkal, hatékony kockázatértékelési eljárásokkal, valamint az IKT-rendszerek kezelésére vonatkozó hatékony ellenőrzési és biztonsági szabályozással kell rendelkeznie az (EU) 2022/2554 európai parlamenti és tanácsi rendelettel (*) összhangban.

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27., 1. o.).”

2. A III. melléklet 12. pontjának helyébe a következő szöveg lép:

„12. A hitelminősítő intézet megsérti a 6. cikk (2) bekezdését az I. melléklet A. szakasza 4. pontjával összefüggésben azáltal, ha nem rendelkezik megbízható adminisztratív vagy számviteli eljárásokkal, belső ellenőrzési mechanizmusokkal, hatékony kockázatértékelési eljárásokkal, vagy az IKT-rendszerek kezelésére vonatkozó hatékony ellenőrzési és biztonsági szabályozással az (EU) 2022/2554 rendelettel összhangban; vagy nem vezet be vagy nem tart fenn az említett pont által előírt határozathozatali eljárásokat vagy szervezeti felépítéseket.”

60. cikk

A 648/2012/EU rendelet módosításai

A 648/2012/EU rendelet a következőképpen módosul:

1. A 26. cikk a következőképpen módosul:

a) a (3) bekezdés helyébe a következő szöveg lép:

„(3) A központi szerződő félnek olyan szervezeti struktúrát kell fenntartania és üzemeltetnie, amely biztosítja a szolgáltatásnyújtás és a tevékenységvégzés folyamatosságát és rendes működését. Megfelelő és arányos rendszereket, erőforrásokat és eljárásokat, többek között az (EU) 2022/2554 európai parlamenti és tanácsi rendelettel (*) összhangban kezelt IKT-rendszereket kell alkalmaznia.

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27., 1. o.).”;

([39]) Az Európai Parlament és a Tanács 2006/43/EK irányelve (2006. május 17.) az éves és összevont (konszolidált) éves beszámolók jog szerinti könyvvizsgálatáról, a 78/660/EGK és a 83/349/EGK tanácsi irányelv módosításáról, valamint a 84/253/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 157., 2006.6.9., 87. o.).

b) a (6) bekezdést el kell hagyni.

2. A 34. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) A központi szerződő fél megfelelő üzletmenet-folytonossági politikát és vészhelyzeti helyreállítási tervet – beleértve az (EU) 2022/2554 rendelettel összhangban bevezetett és végrehajtott IKT-vonatkozású üzletmenet-folytonossági politikát, valamint IKT-reagálási és helyreállítási tervet – hoz létre, hajt végre és tart fenn annak céljából, hogy biztosítsa a központi szerződő fél funkcióinak megőrzését, a műveletek időben történő helyreállítását és a kötelezettségeinek teljesítését.”;

b) a (3) bekezdés első albekezdésének helyébe a következő szöveg lép:

„(3) E cikk következetes alkalmazása érdekében az EÉPH a KBER tagjaival folytatott konzultációt követően kidolgozza az üzletmenet-folytonossági politika, valamint a vészhelyzeti helyreállítási terv minimális tartalmát és követelményeit meghatározó szabályozástechnikai standardok tervezetét, kivéve az IKT-vonatkozású üzletmenet-folytonossági politikát és a vészhelyzeti helyreállítási terveket.”.

3. Az 56. cikk (3) bekezdése első albekezdésének helyébe a következő szöveg lép:

„(3) E cikk következetes alkalmazása érdekében az ESMA kidolgozza – az IKT-kockázatkezelésre vonatkozó követelmények kivételével – az (1) bekezdésben említett, nyilvántartásba vétel iránti kérelem részleteit meghatározó szabályozástechnikai standardok tervezetét.”

4. A 79. cikk (1) és (2) bekezdésének helyébe a következő szöveg lép:

„(1) A kereskedési adattár azonosítja a működési kockázat forrásait, és minimalizálja azokat többek között a megfelelő rendszerek, ellenőrzések és eljárások kidolgozása révén, beleértve az (EU) 2022/2554 rendelettel összhangban kezelt IKT-rendszereket is.

(2) A kereskedési adattár megfelelő üzletmenet-folytonossági politikát és vészhelyzeti helyreállítási tervet – beleértve az (EU) 2022/2554 rendelettel összhangban létrehozott IKT-vonatkozású üzletmenet-folytonossági politikát, valamint IKT-reagálási és helyreállítási tervet – hoz létre, hajt végre és tart fenn annak céljából, hogy biztosítsa a kereskedési adattár funkcióinak fenntartását, a műveletek időben történő helyreállítását és a kötelezettségeinek teljesítését.”

5. A 80. cikk (1) bekezdését el kell hagyni.

6. Az I. melléklet II. szakasza a következőképpen módosul:

a) az a) és a b) pont helyébe a következő szöveg lép:

„a) a kereskedési adattár megsérti a 79. cikk (1) bekezdését azáltal, hogy nem azonosítja a működési kockázat forrásait, és nem minimalizálja azokat a megfelelő rendszerek, ellenőrzések és eljárások kidolgozása révén, beleértve az (EU) 2022/2554 rendelettel összhangban kezelt IKT-rendszereket is;

b) a kereskedési adattár megsérti a 79. cikk (2) bekezdését azáltal, hogy nem hoz létre, nem hajt végre és nem tart fenn az (EU) 2022/2554 rendelettel összhangban bevezetett megfelelő üzletmenet-folytonossági politikát és vészhelyzeti helyreállítási tervet annak céljából, hogy biztosítsa a kereskedési adattár funkcióinak fenntartását, a műveletek időben történő helyreállítását és a kötelezettségeinek teljesítését;”

b) a c) pontot el kell hagyni.

7. A III. melléklet a következőképpen módosul:

a) a II. szakasz a következőképpen módosul:

i. a c) pont helyébe a következő szöveg lép:

„c) a 2. szintű központi szerződő fél megsérti a 26. cikk (3) bekezdését, azáltal, hogy nem tart fenn vagy nem működtet olyan szervezeti struktúrát, amely biztosítja szolgáltatásainak és tevékenységeinek folyamatosságát és szabályos működését, vagy nem alkalmaz megfelelő és arányos rendszereket, erőforrásokat vagy eljárásokat, beleértve az (EU) 2022/2554 rendelettel összhangban kezelt IKT-rendszereket is;”

ii. az f) pontot el kell hagyni.

b) a III. szakasz a) pontjának helyébe a következő szöveg lép:

„a) a 2. szintű központi szerződő fél megsérti a 34. cikk (1) bekezdését azáltal, hogy nem hoz létre, hajt végre vagy tart fenn az (EU) 2022/2554 rendelettel összhangban bevezetett megfelelő üzletmenet-folytonossági politikát és vészhelyzeti helyreállítási tervet annak céljából, hogy biztosítsa a központi szerződő fél működőképességének fenntartását, a műveletek időben történő helyreállítását és a kötelezettségeinek teljesítését, ami lehetővé teszi legalább a zavar bekövetkezésekor folyamatban lévő valamennyi tranzakció helyreállítását, hogy a központi szerződő fél biztonsággal folytatni tudja működését, és a tervezett időpontban le tudja zárni az ügyleteket;”.

61. cikk

A 909/2014/EU rendelet módosításai

A 909/2014/EU rendelet 45. cikke a következőképpen módosul:

1. Az (1) bekezdés helyébe a következő szöveg lép:

„(1) A központi értéktárnak meg kell határoznia a működési kockázatok külső és belső forrásait, és mérsékelnie kell azok hatását az (EU) 2022/2554 európai parlamenti és tanácsi rendelettel (*) összhangban létrehozott és kezelt megfelelő IKT-eszközök, -eljárások és -politikák bevezetése révén, valamint a működési kockázat más típusai – többek között az általa üzemeltetett valamennyi értékpapír-kiegyenlítési rendszer – esetében bármely egyéb releváns megfelelő eszközök, ellenőrzések és eljárások révén.

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27., 1. o.).”

2. A (2) bekezdést el kell hagyni.

3. A (3) és a (4) bekezdés helyébe a következő szöveg lép:

„(3) A központi értéktárnak valamennyi nyújtott szolgáltatás és minden egyes üzemeltetett értékpapír-kiegyenlítési rendszer tekintetében megfelelő üzletmenet-folytonossági politikát és vészhelyzeti helyreállítási tervet – beleértve az (EU) 2022/2554 rendelettel összhangban kidolgozott IKT-vonatkozású üzletmenet-folytonossági politikát, valamint IKT-reagálási és helyreállítási tervet – kell kidolgoznia, bevezetnie és fenntartania, hogy biztosítsa a szolgáltatásnyújtása megőrzését, a működése mielőbbi helyreállítását és a kötelezettségei teljesítését olyan események bekövetkeztekor, amelyek komoly kockázatot jelentenek a működés megszakítására nézve.

(4) A (3) bekezdésben említett tervnek – többek közt annak biztosításával, hogy az (EU) 2022/2554 rendelet 12. cikkének (5) és (7) bekezdésében foglaltak szerint a kritikus informatikai rendszerek a leállás időpontjától kezdődően folytassák a működésüket – lehetővé kell tennie az üzemzavar bekövetkeztekor folyamatban lévő valamennyi tranzakciónak és a résztvevők pozícióinak a helyreállítását, hogy a központi értéktár résztvevői biztonsággal folytatni tudják működésüket, és az ütemezésnek megfelelően el tudják végezni a kiegyenlítést.”

4. A (6) bekezdés helyébe a következő szöveg lép:

„(6) A központi értéktárnak azonosítania, nyomon követnie és kezelnie kell azon kockázatokat, amelyeket az általa üzemeltetett értékpapír-kiegyenlítési rendszerek fő résztvevői, valamint a szolgáltatók és közműszolgáltatók vagy más központi értéktárak és piaci infrastruktúrák jelenthetnek a működésére. Kérésre az illetékes és releváns hatóságok rendelkezésére kell bocsátania a feltárt kockázatokkal kapcsolatos információkat. Haladéktalanul tájékoztatnia kell az illetékes hatóságot és a releváns hatóságokat az ilyen kockázatokból eredő működési zavarokról is, kivéve azokat, amelyek IKT-kockázattal összefüggésben következnek be.”

5. A (7) bekezdés első albekezdésének helyébe a következő szöveg lép:

„(7) Az ESMA – a KBER tagjaival szorosan együttműködve – szabályozástechnikai standardtervezeteket dolgoz ki, hogy meghatározza az (1) és a (6) bekezdésben említett, IKT-kockázattól eltérő működési kockázatokat és az e kockázatok tesztelésének, kezelésének vagy minimalizálásának módszereit, ideértve a (3) és a (4) bekezdésben említett üzletmenet-folytonossági politikát és vészhelyzeti helyreállítási tervet, valamint azok értékelési módszereit.”

62. cikk

A 600/2014/EU rendelet módosításai

A 600/2014/EU rendelet a következőképpen módosul:

1. A 27 g. cikk a következőképpen módosul:

   a) a (4) bekezdés helyébe a következő szöveg lép:

   „(4) Az APA-nak meg kell felelnie a hálózati és információs rendszerek biztonságára vonatkozó, az (EU) 2022/2554 európai parlamenti és tanácsi rendeletben (*) meghatározott követelményeknek.

   _____

   (*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27., 1. o.).";

   b) a (8) bekezdés c) pontjának helyébe a következő szöveg lép:

   „c) a (3) és az (5) bekezdésben megállapított konkrét szervezeti követelményeket.".

2. A 27h. cikk a következőképpen módosul:

   a) az (5) bekezdés helyébe a következő szöveg lép:

   „(5) A CTP-nek meg kell felelnie a hálózati és információs rendszerek biztonságára vonatkozó, az (EU) 2022/2554 rendeletben meghatározott követelményeknek.";

   b) a (8) bekezdés e) pontjának helyébe a következő szöveg lép:

   „e) a (4) bekezdésben megállapított konkrét szervezeti követelményeket."

3. A 27i. cikk a következőképpen módosul:

   a) az (3) bekezdés helyébe a következő szöveg lép:

   „(3) Az ARM-nek meg kell felelnie a hálózati és információs rendszerek biztonságára vonatkozó, az (EU) 2022/2554 rendeletben meghatározott követelményeknek.";

   b) az (5) bekezdés b) pontjának helyébe a következő szöveg lép:

   „b) a (2) és a (4) bekezdésben megállapított konkrét szervezeti követelményeket."

63. cikk

Az (EU) 2016/1011 rendelet módosításai

Az (EU) 2016/1011 rendelet 6. cikke a következő bekezdéssel egészül ki:

„(6) A kritikus referenciamutatók tekintetében a referenciamutató-kezelőnek megbízható adminisztratív és számviteli eljárásokkal, belső kontrollmechanizmusokkal, hatékony kockázatértékelési eljárásokkal, valamint az IKT-rendszerek kezelésére vonatkozó hatékony kontroll- és biztonsági szabályozással kell rendelkeznie az (EU) 2022/2554 európai parlamenti és tanácsi rendelettel (*) összhangban.

_____

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27., 1. o.)."

64. cikk

Hatálybalépés és alkalmazás

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ezt a rendeletet 2025. január 17-től kell alkalmazni.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Strasbourgban, 2022. december 14-én.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*
R. METSOLA	M. BEK

IRÁNYELVEK

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE

(2022. december 14.)

az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

(EGT-vonatkozású szöveg)

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 114. cikkére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Központi Bank véleményére ([1]),

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére ([2]),

a Régiók Bizottságával folytatott konzultációt követően,

rendes jogalkotási eljárás keretében ([3]),

mivel:

(1) Az (EU) 2016/1148 európai parlamenti és tanácsi irányelv ([4]) célja a kiberbiztonsági képességek egész Unióban történő kiépítése, a kulcsfontosságú ágazatokban az alapvető szolgáltatások nyújtására használt hálózati és információs rendszerek fenyegetéseinek mérséklése és az említett szolgáltatások folyamatosságának biztosítása az események során, hozzájárulva ezzel az Unió biztonságához, valamint gazdaságának és társadalmának hatékony működéséhez.

(2) Az (EU) 2016/1148 irányelv hatálybalépése óta jelentős előrelépés történt az Unió kiberrezilienciájának növelése terén. Az említett irányelv felülvizsgálata megmutatta, hogy az katalizátorként szolgált az uniós kiberbiztonság intézményi és szabályozási megközelítésében, utat nyitva a gondolkodásmód jelentős változásának. Az említett irányelv a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiák létrehozásával, a nemzeti képességek kialakításával és az egyes tagállamok által azonosított alapvető infrastruktúrákra és szervezetekre vonatkozó szabályozási intézkedések végrehajtásával biztosította a hálózati és információs rendszerek biztonságára vonatkozó nemzeti keretek teljessé tételét. Az (EU) 2016/1148 irányelv az együttműködési csoport, valamint a nemzeti számítógép-biztonsági eseményekre reagáló csoportok hálózata létrehozásával hozzájárult az uniós szintű együttműködéshez is. Ezen eredmények ellenére az (EU) 2016/1148 irányelv felülvizsgálata olyan benne rejlő hiányosságokat tárt fel, amelyek megakadályozzák, hogy eredményesen kezelje a jelenlegi és a jövőben felmerülő kiberbiztonsági kihívásokat.

(3) A hálózati és információs rendszerek a mindennapi élet központi jellemzőjévé fejlődtek a társadalom gyors digitális átalakulásával és összekapcsolódásával, beleértve a határokon átnyúló információmegosztást is. Ez a fejlődés a kiberfenyegetettség bővüléséhez vezetett, új kihívások támasztásával, amelyek minden tagállamban kiigazított, összehangolt és innovatív reagálást igényelnek. Az események száma, nagysága, kifinomultsága, gyakorisága és hatása növekszik, és komoly veszélyt jelentenek a hálózati és információs rendszerek működésére. Ennek következtében az események akadályozhatják gazdasági tevékenységek folytatását a belső piacon, pénzügyi veszteséget okozhatnak, aláásható a felhasználók bizalmát, és jelentős károkat okozhatnak az Unió gazdaságában

([1]) HL C 233., 2022.6.16., 22. o.
([2]) HL C 286., 2021.7.16., 170. o.
([3]) Az Európai Parlament 2022. november 10-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2022. november 28-i határozata.
([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.).

és a társadalmában. A kiberbiztonsági felkészültség és hatásosság ezért minden eddiginél elengedhetetlenebb a belső piac megfelelő működéséhez. Emellett a kiberbiztonság számos kritikus ágazat szempontjából kulcsfontosságú tényező a digitális átalakulás sikeres megvalósításában és a digitalizáció gazdasági, társadalmi és fenntartható előnyeinek teljes körű kiaknázásában.

(4) Az (EU) 2016/1148 irányelv jogalapja az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikke volt, amelynek célja a belső piac megteremtése és működése a nemzeti szabályok közelítésére irányuló intézkedések fokozásával. A szolgáltatásokat nyújtó vagy gazdaságilag jelentős tevékenységeket végző szervezetekre előírt kiberbiztonsági követelmények jelentősen eltérnek az egyes tagállamokban a követelmények típusa, részletességi szintje és a felügyelet módja tekintetében. Ezek az eltérések többletköltségekkel járnak és nehézségeket okoznak a határokon átnyúló viszonylatban árukat vagy szolgáltatásokat kínáló szervezetek számára. Az egyik tagállam által előírt, a másik tagállam által előírtaktól eltérő vagy akár azoknak ellentmondó követelmények jelentősen befolyásolhatják az ilyen határokon átnyúló tevékenységeket. Ezenkívül egy tagállamban a kiberbiztonsági követelmények nem megfelelő kialakításának vagy végrehajtásának lehetősége valószínűleg károsan hat más tagállamok kiberbiztonsági szintjére, tekintve különösen a határokon átnyúló információmegosztás intenzitását. Az (EU) 2016/1148 irányelv felülvizsgálata jelentős eltéréseket mutatott az irányelv tagállamok általi végrehajtása terén, beleértve a hatály tekintetében, amelynek lehatárolása nagyrészt a tagállamok mérlegelési jogkörében maradt. Az (EU) 2016/1148 irányelv szintén nagyon tág mérlegelési jogkört biztosított a tagállamoknak az abban megállapított biztonsági és eseményjelentési kötelezettségek végrehajtása tekintetében. Ezeket a kötelezettségeket tehát nemzeti szinten jelentősen eltérő módon hajtották végre. Hasonló eltérések vannak az (EU) 2016/1148 irányelv felügyeletre és végrehajtásra vonatkozó rendelkezéseinek végrehajtásában is.

(5) Mindezek az eltérések a belső piac széttöredezettségével járnak, és káros hatással lehetnek annak működésére, különösen a határokon átnyúló szolgáltatások nyújtására és a kiberbiztonsági ellenállóképesség szintjére, az eltérő intézkedések alkalmazása miatt. Ezek az eltérések végső soron azt eredményezhetik, hogy egyes tagállamok jobban ki vannak téve a kiberfenyegetéseknek, aminek az egész Unióra kiterjedő, tovagyűrűző hatásai lehetnek. Ennek az irányelvnek az a célja, hogy kiküszöbölje a tagállamok közötti ilyen nagy eltéréseket, különösen egy összehangolt szabályozási keret működésével kapcsolatos minimumszabályok megállapításával, az egyes tagállamok felelős hatóságai közötti hatékony együttműködés mechanizmusainak meghatározásával, a kiberbiztonsági kötelezettségek hatálya alá tartozó ágazatok és tevékenységek listájának frissítésével, valamint olyan hatékony jogorvoslatok és végrehajtási intézkedések biztosításával, amelyek kulcsfontosságúak az említett kötelezettségek tényleges érvényesítéséhez. Ezért az (EU) 2016/1148 irányelvet hatályon kívül kell helyezni, és azt ezen irányelvvel kell felváltani.

(6) Az (EU) 2016/1148 irányelv hatályon kívül helyezésével az ágazatokon alapuló alkalmazási kört ki kell terjeszteni a gazdaság nagyobb részére, hogy átfogóan lefedjék azokat az ágazatokat és szolgáltatásokat, amelyek létfontosságúak a belső piacon kulcsfontosságú társadalmi és gazdasági tevékenységek szempontjából. Ezen irányelv célja különösen az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók közötti különbségtétel hiányosságainak kiküszöbölése, amely különbségtétel elavultnak bizonyult, mivel nem tükrözi az ágazatok vagy szolgáltatások jelentőségét a belső piaci társadalmi és gazdasági tevékenységek szempontjából.

(7) Az (EU) 2016/1148 irányelv értelmében a tagállamok voltak felelősek azon szervezetek meghatározásáért, amelyek megfelelnek az ahhoz szükséges kritériumoknak, hogy alapvető szolgáltatásokat nyújtó szereplőknek minősüljenek. A tagállamok között e tekintetben mutatkozó nagy eltérések kiküszöbölése, valamint az összes érintett szervezet vonatkozásában a kiberbiztonsági kockázatkezelési intézkedések és a jelentéstételi kötelezettségek tekintetében a jogbiztonság biztosítása érdekében egy olyan egységes kritériumot kell megállapítani, amely meghatározza az ezen irányelv hatálya alá tartozó szervezeteket. Ennek a kritériumnak tartalmaznia kell a méretküszöb-szabály alkalmazását, amely szerint ezen irányelv hatálya alá tartozik minden olyan szervezet, amely a 2003/361/EK bizottsági ajánlás ([5]) mellékletének 2. cikke szerint középvállalkozásnak minősül, vagy meghaladja az említett cikk (1) bekezdésében a középvállalkozásokra vonatkozóan előírt küszöbértékeket, és amely az ezen irányelv hatálya alá

([5]) A Bizottság 2003/361/EK ajánlása (2003. május 6.) a mikro-, kis- és középvállalkozások meghatározásáról (HL L 124., 2003.5.20., 36. o.).

tartozó ágazatokban működik, és az irányelv hatálya alá tartozó típusú szolgáltatásokat nyújt vagy tevékenységeket végez. A tagállamoknak rendelkezniük kell arról is, hogy ezen irányelv hatálya alá tartozzanak bizonyos olyan, az említett melléklet 2. cikkének (2) és (3) bekezdésében meghatározott kisvállalkozások és mikrovállalkozások, amelyek megfelelnek az arra utaló bizonyos kritériumoknak, hogy kulcsfontosságú szerepet töltenek be a társadalom, a gazdaság, vagy bizonyos ágazatok vagy szolgáltatástípusok szempontjából.

(8) A közigazgatási szervek ezen irányelv hatálya alóli kizárását azokra a szervezetekre kell alkalmazni, amelyek tevékenységeiket elsősorban a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés – többek között a bűncselekmények megelőzése, kivizsgálása, felderítése és büntetőeljárás alá vonása – területén végzik. Azon közigazgatási szervek azonban, amelyek tevékenységei csak csekély mértékben kapcsolódnak az említett területekhez, nem zárhatók ki ezen irányelv hatálya alól. Ezen irányelv alkalmazásában a szabályozási hatáskörrel rendelkező szervezetek nem tekintendők a bűnüldözés területén tevékenységet folytató szervezetnek, ezért ezen az alapon nincsenek kizárva ezen irányelv hatálya alól. Nem tartoznak ezen irányelv hatálya alá azon közigazgatási szervek, amelyeket valamely nemzetközi megállapodással összhangban harmadik országgal közösen hoztak létre. Ez az irányelv nem alkalmazandó a tagállamok harmadik országokban működő diplomáciai és konzuli képviseleteire, illetve azok hálózati és információs rendszereire, amennyiben ezek a rendszerek a képviselet helyiségeiben találhatók, vagy harmadik országbeli felhasználók számára üzemelnek.

(9) A tagállamok számára lehetővé kell tenni, hogy megtegyék az alapvető nemzetbiztonsági érdekeik védelmének biztosításához, a közrend és a közbiztonság megóvásához, valamint a bűncselekmények megelőzésének, kivizsgálásának, felderítésének és büntetőeljárás alá vonásának lehetővé tételéhez szükséges intézkedéseket. E célból a tagállamok számára lehetővé kell tenni, hogy a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés – többek között a bűncselekmények megelőzése, kivizsgálása, felderítése és büntetőeljárás alá vonása – területén tevékenységet végző meghatározott szervezeteket mentesítsenek e tevékenységek tekintetében az ezen irányelvben megállapított egyes kötelezettségek alól. Amennyiben egy szervezet kizárólag olyan közigazgatási szerv részére nyújt szolgáltatásokat, amely nem tartozik ezen irányelv hatálya alá, a tagállamok számára lehetővé kell tenni, hogy az adott szervezetet az említett szolgáltatások tekintetében mentesítsék az ezen irányelvben megállapított egyes kötelezettségek alól. Ezenkívül egyetlen tagállamtól sem követelhető meg olyan információk szolgáltatása, amelyek nyilvánosságra hozatala ellentétes lenne nemzetbiztonságának, közbiztonságának vagy védelmének alapvető érdekeivel. Ebben az összefüggésben figyelembe kell venni a minősített információk védelmére vonatkozó uniós és nemzeti szabályokat, a titoktartási megállapodásokat és az informális titoktartási megállapodásokat, például a jelzőlámpa-protokollt (TLP). A jelzőlámpa-protokollt olyan eszközként kell értelmezni, amely arra szolgál, hogy tájékoztatást nyújtson az információk további terjesztésének korlátairól. Használják szinte valamennyi számítógép-biztonsági eseményekre reagáló csoportban (CSIRT-ek), valamint egyes információelemző és -megosztó központokban.

(10) Jóllehet ez az irányelv az atomerőművekből származó villamos energia előállításával kapcsolatos tevékenységeket végző szervezetekre is alkalmazandó, e tevékenységek némelyike nemzetbiztonsági vonatkozású lehet. Ha ez az eset áll fenn, a tagállamok számára lehetővé kell tenni, hogy a Szerződésekkel összhangban gyakorolhassák a nemzetbiztonság védelmével kapcsolatos felelősségüket e tevékenységek tekintetében, ideértve a nukleáris értékláncon belüli tevékenységeket is.

(11) Egyes szervezetek a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés – többek között a bűncselekmények megelőzése, kivizsgálása, felderítése és büntetőeljárás alá vonása – területén végzik tevékenységeiket, miközben bizalmi szolgáltatásokat is nyújtanak. A 910/2014/EU európai parlamenti és tanácsi rendelet ([6]) hatálya alá tartozó bizalmi szolgáltatóknak ezen irányelv hatálya alá kell tartozniuk az említett rendelet által a bizalmi szolgáltatók tekintetében korábban megállapított biztonsági követelményekével és felügyeletével azonos szint megőrzése érdekében. Egyes meghatározott szolgáltatásoknak a 910/2014/EU rendelet hatálya alóli kizárásával összhangban ez az irányelv nem alkalmazandó a nemzeti jogon vagy meghatározott résztvevők közötti megállapodásokon alapuló, kizárólag zárt rendszerekben használt bizalmi szolgáltatások nyújtására.

([6]) Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (HL L 257., 2014.8.28., 73. o.).

(12) A 97/67/EK európai parlamenti és tanácsi irányelvben ([7]) meghatározott postai szolgáltatóknak – beleértve a futárszolgáltatókat is – ezen irányelv hatálya alá kell tartozniuk, ha a postai kézbesítési lánc legalább egyik lépését biztosítják, különös tekintettel a postai küldemények felvételére, válogatására, szállítására vagy terjesztésére, ideértve az átvételi szolgáltatásokat is, figyelembe véve a hálózati és információs rendszerektől való függőségük mértékét. Azokat a szállítási szolgáltatásokat, amelyeket nem az említett lépések egyikével kapcsolatban végeznek, ki kell zárni a postai szolgáltatások köréből.

(13) Tekintettel az egyre intenzívebb és kifinomultabb kiberfenyegetésekre, a tagállamoknak törekedniük kell annak biztosítására, hogy az ezen irányelv hatálya alól kizárt szervezetek magas szintű kiberbiztonságot érjenek el, és támogatniuk kell olyan egyenértékű kiberbiztonsági kockázatkezelési intézkedések végrehajtását, amelyek tükrözik az említett szervezetek érzékeny jellegét.

(14) A személyes adatok ezen irányelv szerinti bármely kezelésére alkalmazni kell az adatvédelemre és a magánélet védelmére vonatkozó uniós jogot. Ez az irányelv nem érinti különösen az (EU) 2016/679 európai parlamenti és tanácsi rendeletet ([8]), valamint a 2002/58/EK európai parlamenti és tanácsi irányelvet ([9]). Ez az irányelv ezért nem érintheti többek között az adatvédelemre és a magánélet védelmére vonatkozó, alkalmazandó uniós jognak való megfelelés nyomon követésére hatáskörrel rendelkező hatóságok feladatait és hatásköreit.

(15) A kiberbiztonsági kockázatkezelési intézkedéseknek és jelentéstételi kötelezettségeknek való megfelelés céljából az ezen irányelv hatálya alá tartozó szervezeteket két kategóriába, az alapvető szervezetek és a fontos szervezetek közé kell sorolni, ami tükrözi annak mértékét, hogy az ágazatuk vagy az általuk nyújtott szolgáltatások típusa szempontjából mennyire kritikusak, valamint a méretüket. E tekintetben kellően figyelembe kell venni a vonatkozó ágazati kockázatértékeléseket vagy adott esetben az illetékes hatóságok által adott iránymutatást. A szervezetek e két kategóriája között a felügyeleti és a végrehajtási rendszer tekintetében különbséget kell tenni, hogy biztosítani lehessen a méltányos egyensúlyt a kockázatalapú követelmények és kötelezettségek, valamint a megfelelés felügyeletéből adódó adminisztratív terhek között.

(16) Annak elkerülése érdekében, hogy a partnervállalkozásokkal rendelkező vagy kapcsolt vállalkozásként működő szervezeteket alapvető vagy fontos szervezetnek tekintsék olyan esetben, amikor ez aránytalan lenne, a tagállamok a 2003/361/EK ajánlás melléklete 6. cikke (2) bekezdésének alkalmazásakor figyelembe vehetik a szervezetek partnereikkel vagy kapcsolt vállalkozásaikkal szembeni függetlenségének mértékét. A tagállamok különösen figyelembe vehetik azt, hogy egy szervezet partnerétől vagy kapcsolt vállalkozásaitól független a szervezet által a szolgáltatásai nyújtása során használt hálózati és információs rendszerek, valamint az általa nyújtott szolgáltatások tekintetében. Ennek alapján a tagállamok adott esetben úgy tekinthetik, hogy egy ilyen szervezet a 2003/361/EK ajánlás melléklete 2. cikke szerint nem minősül középvállalkozásnak vagy nem haladja meg az említett cikk (1) bekezdésében a középvállalkozásokra vonatkozóan előírt küszöbértékeket, ha a szervezet függetlenségének mértékét figyelembe véve a szervezetet – ha csak a saját adatait vették volna figyelembe – nem tekintették volna úgy, hogy középvállalkozásnak minősül vagy meghaladja az említett küszöbértékeket. Ez nem érinti az ezen irányelv hatálya alá tartozó partner- és kapcsolt vállalkozások ezen irányelvben megállapított kötelezettségeit.

(17) A tagállamok számára lehetőséget kell biztosítani annak eldöntésére, hogy az ezen irányelv hatálybalépése előtt az (EU) 2016/1148 irányelvvel összhangban alapvető szolgáltatásokat nyújtó szereplőként azonosított szervezetek alapvető szervezetnek tekintendők-e.

([7]) Az Európai Parlament és a Tanács 97/67/EK irányelve (1997. december 15.) a közösségi postai szolgáltatások belső piacának fejlesztésére és a szolgáltatások minőségének javítására vonatkozó közös szabályokról (HL L 15., 1998.1.21., 14. o.).

([8]) 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 említett adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

([9]) Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) (HL L 201., 2002.7.31., 37. o.).

(18) Az ezen irányelv hatálya alá tartozó szervezetek áttekinthetőségének biztosítása érdekében a tagállamoknak össze kell állítaniuk az alapvető és fontos szervezetek, valamint a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek jegyzékét. E célból a tagállamoknak elő kell írniuk a szervezetek számára, hogy legalább a következő információkat nyújtsák be az illetékes hatóságoknak, nevezetesen a szervezet nevét, címét és naprakész elérhetőségét, beleértve a szervezet e-mail-címeit, IP-tartományait és telefonszámait, és adott esetben a mellékletekben említett érintett ágazatot és alágazatot, valamint adott esetben azon tagállamok jegyzékét, amelyekben a szervezet az ezen irányelv hatálya alá tartozó szolgáltatásokat nyújt. E célból a Bizottságnak az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) segítségével indokolatlan késedelem nélkül iránymutatásokat kell nyújtania és sablonokat kell rendelkezésre bocsátania az információszolgáltatási kötelezettségre vonatkozóan. Az alapvető és fontos szervezetek, valamint a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek jegyzéke összeállításának és frissítésének megkönnyítése érdekében a tagállamok számára lehetővé kell tenni, hogy nemzeti mechanizmusokat hozzanak létre abból a célból, hogy a szervezetek bejegyeztessék magukat. Amennyiben nemzeti szinten léteznek nyilvántartások, a tagállamok dönthetnek az ezen irányelv hatálya alá tartozó szervezetek azonosítását lehetővé tevő megfelelő mechanizmusokról.

(19) A tagállamok feladata, hogy a mellékletekben említett minden egyes ágazat és alágazat tekintetében legalább az alapvető és fontos szervezetek számát, valamint az azonosított szervezetek számáról és az ezen irányelvben megállapítottak közül az azonosítás alapjául szolgáló rendelkezésről, valamint az általuk nyújtott szolgáltatás típusáról szóló releváns információkat megküldjék a Bizottságnak. A tagállamok ösztönzést kapnak arra, hogy a Bizottsággal cseréljék ki az alapvető és fontos szervezetekről szóló információkat, valamint nagyszabású kiberbiztonsági események esetén a releváns információkat, így például az érintett szervezet nevét.

(20) A Bizottságnak az együttműködési csoporttal együttműködve és az érintett érdekelt felekkel folytatott konzultációt követően iránymutatásokat kell nyújtania a mikro- és kisvállalkozásokra alkalmazandó azon kritériumok végrehajtásáról, amelyek célja annak értékelése, hogy a mikro- és kisvállalkozások ezen irányelv hatálya alá tartoznak-e. A Bizottságnak biztosítania kell továbbá, hogy az ezen irányelv hatálya alá tartozó valamennyi mikro- és kisvállalkozás megfelelő iránymutatást kapjon. A Bizottság a tagállamok segítségével e tekintetben információkat bocsát a mikro- és kisvállalkozások rendelkezésére.

(21) A Bizottság iránymutatást nyújthat annak érdekében, hogy segítse a tagállamokat ezen irányelv hatályra vonatkozó rendelkezéseinek végrehajtásában és az ezen irányelv alapján meghozandó intézkedések arányosságának értékelésében, különös tekintettel az olyan összetett üzleti modellel vagy működési környezettel rendelkező szervezetekre, amelyek révén egy szervezet egyszerre is megfelelhet mind az alapvető, mind a fontos szervezetekre vonatkozó kritériumoknak, vagy egyidejűleg végezhet olyan tevékenységeket, amelyek közül egyesek ezen irányelv hatálya alá tartoznak, mások pedig ki vannak zárva annak hatálya alól.

(22) Ez az irányelv a kiberbiztonsági kockázatkezelési intézkedések és jelentéstételi kötelezettségek alapjául szolgál a hatálya alá tartozó ágazatokban. Az uniós jogi aktusok kiberbiztonsági rendelkezései széttagoltságának elkerülése érdekében azokban az esetekben, amikor a kiberbiztonsági kockázatkezelési intézkedésekkel és jelentéstételi kötelezettségekkel kapcsolatos további ágazatspecifikus uniós jogi aktusokra van szükség a magas szintű kiberbiztonság Unió-szerte történő biztosításához, a Bizottságnak meg kell vizsgálnia, hogy egy ezen irányelv szerinti végrehajtási jogi aktusban elő lehetne-e írni ilyen további rendelkezéseket. Amennyiben az ilyen végrehajtási jogi aktus nem alkalmas erre a célra, az ágazatspecifikus uniós jogi aktusok járulhatnak hozzá a magas szintű kiberbiztonság biztosításához Unió-szerte, teljeskörűen figyelembe véve az érintett ágazatok sajátosságait és összetettségét. Ennek érdekében ez az irányelv nem zárja ki a kiberbiztonsági kockázatkezelési intézkedésekkel és a jelentéstételi kötelezettségekkel foglalkozó további olyan ágazatspecifikus uniós jogi aktusok elfogadását, amelyek kellően figyelembe veszik az átfogó és következetes kiberbiztonsági keret szükségességét. Ez az irányelv nem érinti a Bizottságra számos ágazatban – ideértve a közlekedést és az energiaágazatot is – átruházott, meglévő végrehajtási hatásköröket.

(23) Ha egy ágazatspecifikus uniós jogi aktus olyan rendelkezéseket tartalmaz, amelyek előírják az alapvető vagy fontos szervezetek számára, hogy kiberbiztonsági kockázatkezelési intézkedéseket fogadjanak el vagy bejelentsék a jelentős eseményeket, és ha ezek a követelmények hatásukban legalább egyenértékűek az ezen irányelvben meghatározott kötelezettségekkel, akkor az ilyen szervezetekre az említett rendelkezéseket – többek között a felügyeletre és a

végrehajtásra vonatkozó rendelkezéseket is – kell alkalmazni. Amennyiben az ágazatspecifikus uniós jogi aktus nem terjed ki az ezen irányelv hatálya alá tartozó adott ágazatban működő valamennyi szervezetre, ezen irányelv vonatkozó rendelkezései továbbra is alkalmazandók azokra a szervezetekre, amelyek nem tartoznak az említett jogi aktus hatálya alá.

(24) Amennyiben az ágazatspecifikus uniós jogi aktus rendelkezései előírják az alapvető vagy fontos szervezetek számára, hogy az ezen irányelvben megállapított jelentéstételi kötelezettségekkel legalább egyenértékű hatású jelentéstételi kötelezettségeknek feleljenek meg, biztosítani kell az események bejelentésének következetességét és kezelésének hatékonyságát. E célból az ágazatspecifikus uniós jogi aktus események bejelentésére vonatkozó rendelkezéseinek azonnali hozzáférést kell biztosítaniuk a CSIRT-ek, az illetékes hatóságok vagy az ezen irányelv szerinti, kiberbiztonsággal foglalkozó egyedüli kapcsolattartó pontok (a továbbiakban: egyedüli kapcsolattartó pontok) számára az ágazatspecifikus uniós jogi aktusnak megfelelően benyújtott eseménybejelentésekhez. Ilyen azonnali hozzáférés különösen akkor biztosítható, ha indokolatlan késedelem nélkül továbbítják az eseménybejelentéseket a CSIRT-nek, az illetékes hatóságnak vagy az ezen irányelv szerinti egyedüli kapcsolattartó pontnak. Adott esetben a tagállamoknak olyan automatikus és közvetlen jelentéstételi mechanizmust kell bevezetniük, amely biztosítja az információk szisztematikus és azonnali megosztását a CSIRT-ekkel, az illetékes hatóságokkal vagy az egyedüli kapcsolattartó pontokkal az eseménybejelentések kezelésével kapcsolatban. A jelentéstétel egyszerűsítése és az automatikus és közvetlen jelentéstételi mechanizmus végrehajtása céljából a tagállamok az ágazatspecifikus uniós jogi aktussal összhangban használhatnak egy egyedüli kapcsolattartó pontot.

(25) Az ezen irányelvben megállapítottakkal legalább egyenértékű hatású kiberbiztonsági kockázatkezelési intézkedéseket vagy jelentéstételi kötelezettségeket előíró ágazatspecifikus uniós jogi aktusok előírhatják, hogy az ilyen jogi aktusok szerinti illetékes hatóságok az ilyen intézkedésekkel vagy kötelezettségekkel kapcsolatos felügyeleti és végrehajtási hatásköreiket az ezen irányelv szerinti illetékes hatóságok támogatásával gyakorolják. Az érintett illetékes hatóságok e célból együttműködési megállapodásokat hozhatnak létre. Az ilyen együttműködési megállapodásokban meg lehet határozni többek között a felügyeleti tevékenységek koordinálásával kapcsolatos eljárásokat, ideértve a nemzeti joggal összhangban végzett vizsgálatokra és helyszíni ellenőrzésekre vonatkozó eljárásokat, valamint a felügyelettel és a végrehajtással kapcsolatos releváns információk illetékes hatóságok közötti cseréjére szolgáló mechanizmusokat, ideértve az ezen irányelv szerinti illetékes hatóságok által kért, kiberjellegű információkhoz való hozzáférést.

(26) Amennyiben az ágazatspecifikus uniós jogi aktusok előírják a szervezeteknek a jelentős kiberfenyegetések bejelentését, vagy ösztönzik azt, a tagállamoknak is ösztönözniük kell a jelentős kiberfenyegetéseknek a CSIRT-ekkel, az illetékes hatóságokkal vagy az ezen irányelv szerinti egyedüli kapcsolattartó pontokkal való megosztását is annak biztosítása érdekében, hogy e szervek jobban tisztában legyenek a kiberfenyegetettségi helyzettel, és hogy lehetővé tegyék számukra, hogy hatékonyan és kellő időben reagáljanak, amennyiben a jelentős kiberfenyegetések megvalósulnak.

(27) A jövőbeli ágazatspecifikus uniós jogi aktusoknak megfelelően figyelembe kell venniük az ezen irányelvben meghatározott fogalommeghatározásokat, valamint felügyeleti és végrehajtási keretet.

(28) Az (EU) 2022/2554 európai parlamenti és tanácsi rendeletet ([10]) ezen irányelv vonatkozásában ágazatspecifikus uniós jogi aktusnak kell tekinteni a pénzügyi szervezetek tekintetében. Az ezen irányelvben előírt rendelkezések helyett az (EU) 2022/2554 rendeletnek az információs és kommunikációs technológiai (IKT) kockázatkezelésre, az IKT-vel kapcsolatos események kezelésére és különösen a jelentős IKT-vonatkozású események bejelentésére, valamint a digitális működési rezilienciára vonatkozó tesztekre, az információmegosztási megállapodásokra és a harmadik féllel kapcsolatos IKT-kockázatokra vonatkozó rendelkezéseit kell alkalmazni. A tagállamok ezért nem alkalmazhatják ezen irányelv kiberbiztonsági kockázatkezelésre és jelentéstételi kötelezettségekre, valamint felügyeletre és végrehajtásra vonatkozó rendelkezéseit az (EU) 2022/2554 rendelet hatálya alá tartozó pénzügyi szervezetekre. Ugyanakkor fontos, hogy ezen irányelv alapján fennmaradjon a szoros kapcsolat és információmegosztás a pénzügyi ágazattal. Ennek érdekében az (EU) 2022/2554 rendelet lehetővé teszi, hogy az európai felügyeleti hatóságok (a továbbiakban: EFH-k) és az említett rendelet szerinti illetékes hatóságok részt vegyenek az együttműködési csoport tevékenységeiben, továbbá hogy információt cseréljenek és együttműködjenek az egyedüli kapcsolattartó pontokkal, valamint a CSIRT-ekkel és az ezen irányelv szerinti illetékes hatóságokkal. Az (EU) 2022/2554 rendelet szerint illetékes hatóságoknak továbbítaniuk kell az IKT-vel kapcsolatos jelentős események és adott esetben a jelentős kiberfenyegetések részleteit a CSIRT-eknek, az illetékes hatóságoknak vagy az ezen irányelv

([10]) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (lásd e Hivatalos Lap 1. oldalát).

szerinti egyedüli kapcsolattartó pontoknak is. Ez az eseménybejelentésekhez való azonnali hozzáférés és azok közvetlenül vagy egy egyedüli kapcsolattartó pont révén történő továbbítása biztosításával érhető el. Ezenkívül a tagállamoknak továbbra is be kell vonniuk a pénzügyi ágazatot kiberbiztonsági stratégiájukba, és a CSIRT-ek tevékenységei kiterjedhetnek a pénzügyi ágazatra.

(29) A légiközlekedési ágazatban működő szervezetekre vonatkozó kiberbiztonsági kötelezettségek közötti hiányosságok vagy átfedések elkerülése érdekében a 300/2008/EK ([11]), valamint az (EU) 2018/1139 ([12]) európai parlamenti és tanácsi rendelet szerinti nemzeti hatóságoknak és az ezen irányelv szerinti illetékes hatóságoknak együtt kell működniük egymással a kiberbiztonsági kockázatkezelési intézkedések végrehajtása és az ezen intézkedéseknek való megfelelés nemzeti szintű felügyelete terén. Valamely szervezetnek a 300/2008/EK és az (EU) 2018/1139 rendeletben, valamint az e rendeletek alapján elfogadott vonatkozó felhatalmazáson alapuló jogi aktusokban és végrehajtási jogi aktusokban meghatározott biztonsági követelményeknek való megfelelését az ezen irányelv szerinti illetékes hatóságok az ezen irányelvben meghatározott megfelelő követelményeknek való megfelelésnek tekinthetik.

(30) A kiberbiztonság és a szervezetek fizikai biztonsága közötti összefüggésekre tekintettel koherens megközelítést kell biztosítani az (EU) 2022/2557 európai parlamenti és tanácsi irányelv ([13]) és ezen irányelv között. Ennek elérése érdekében az (EU) 2022/2557 irányelv szerinti kritikus szervezetként azonosított szervezeteket ezen irányelv értelmében alapvető szervezeteknek kell tekinteni. Ezenkívül minden tagállamnak arról is gondoskodnia kell, hogy nemzeti kiberbiztonsági stratégiája biztosítson egy szakpolitikai keretet az adott tagállamon belül az ezen irányelv és az (EU) 2022/2557 irányelv szerinti illetékes hatóságai közötti fokozott koordinációhoz, a kockázatokra, a kiberfenyegetésekre és eseményekre, valamint a nem kiberjellegű kockázatokra, fenyegetésekre és eseményekre vonatkozó információk megosztásával és a felügyeleti feladatok ellátásával összefüggésben. Az ezen irányelv és az (EU) 2022/2557 irányelv szerinti illetékes hatóságoknak indokolatlan késedelem nélkül együtt kell működniük és információt kell cserélniük egymással, különösen a következőkkel kapcsolatban: a kritikus szervezetek azonosítása, a kritikus szervezeteket érintő kockázatok, kiberfenyegetések és események, valamint nem kiberjellegű kockázatok, fenyegetések és események, ideértve a kritikus szervezetek által végrehajtott kiberbiztonsági és fizikai intézkedéseket, valamint az ilyen szervezetek tekintetében végzett felügyeleti tevékenységek eredményei.

Ezenkívül az ezen irányelv és az (EU) 2022/2557 irányelv szerinti illetékes hatóságok közötti felügyeleti tevékenységek észszerűsítése, valamint az érintett szervezetek adminisztratív terheinek minimálisra csökkentése érdekében az említett illetékes hatóságoknak törekedniük kell az eseménybejelentésre szolgáló sablonok és a felügyeleti eljárások harmonizálására. Adott esetben az (EU) 2022/2557 irányelv szerinti illetékes hatóságok számára lehetővé kell tenni, hogy felkérjék az ezen irányelv szerinti illetékes hatóságokat, hogy gyakorolják felügyeleti és végrehajtási hatásköreiket az (EU) 2022/2557 irányelv értelmében kritikus szervezetként azonosított szervezetek tekintetében. E célból az ezen irányelv és az (EU) 2022/2557 irányelv szerinti illetékes hatóságoknak – lehetőség szerint valós időben – együtt kell működniük és információt kell cserélniük egymással.

(31) A digitálisinfrastruktúra-ágazathoz tartozó szervezetek lényegében a hálózati és információs rendszereken alapulnak, ezért az ezen irányelv alapján az ilyen szervezetekre vonatkozóan meghatározott kötelezettségeknek átfogó módon kell kezelniük az ilyen rendszerek fizikai biztonságát kiberbiztonsági kockázatkezelési intézkedéseik és jelentéstételi kötelezettségeik részeként. Mivel az említett területek ezen irányelv hatálya alá tartoznak, az (EU) 2022/2557 irányelv III., IV. és VI. fejezetében meghatározott kötelezettségek nem vonatkoznak az ilyen szervezetekre.

([11]) Az Európai Parlament és a Tanács 300/2008/EK rendelete (2008. március 11.) a polgári légi közlekedés védelmének közös szabályairól és a 2320/2002/EK rendelet hatályon kívül helyezéséről (HL L 97., 2008.4.9., 72. o.).

([12]) Az Európai Parlament és a Tanács (EU) 2018/1139 rendelete (2018. július 4.) a polgári légi közlekedés területén alkalmazandó közös szabályokról és az Európai Unió Repülésbiztonsági Ügynökségének létrehozásáról és a 2111/2005/EK, az 1008/2008/EK, a 996/2010/EU, a 376/2014/EU európai parlamenti és tanácsi rendelet és a 2014/30/EU és a 2014/53/EU európai parlamenti és tanácsi irányelv módosításáról, valamint az 552/2004/EK és a 216/2008/EK európai parlamenti és tanácsi rendelet és a 3922/91/EGK tanácsi rendelet hatályon kívül helyezéséről (HL L 212., 2018.8.22., 1. o.).

([13]) Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (lásd e Hivatalos Lap 164. oldalát).

(32) A megbízható, rugalmas és biztonságos doménnévrendszer (DNS) fenntartása és megőrzése kulcsfontosságú tényező az internet integritásának fenntartásában, és elengedhetetlen annak folyamatos és stabil működéséhez, amelytől a digitális gazdaság és a társadalom függ. Ezért ezen irányelvnek alkalmazandónak kell lennie a legfelső szintű doménnév-nyilvántartókra és a DNS-szolgáltatókra, amelyeket az internet végfelhasználói számára nyilvánosan hozzáférhető rekurzív doménnév-feloldási szolgáltatásokat vagy harmadik fél általi használatra szánt hiteles doménnév-feloldási szolgáltatásokat nyújtó szervezeteknek kell tekinteni. Ez az irányelv nem alkalmazandó a gyökérnévszerverekre.

(33) A felhőszolgáltatásoknak ki kell terjedniük azokra a digitális szolgáltatásokra, amelyek igény szerinti adminisztrációt és széles távoli hozzáférést tesznek lehetővé a megosztható számítástechnikai erőforrások méretezhető és rugalmas készletéhez, beleértve azt az esetet is, amikor az ilyen erőforrásokat több helyszínen osztják el. A számítástechnikai erőforrások részét képezik olyan erőforrások, mint a hálózatok, a szerverek vagy más infrastruktúra, az operációs rendszerek, a szoftverek, a tárhelyek, az alkalmazások és a szolgáltatások. A felhőalapú számítástechnika szolgáltatási modelljei magukban foglalják többek között az infrastruktúra-szolgáltatást (IaaS), a platformszolgáltatást (PaaS), a szoftverszolgáltatást (SaaS), valamint a hálózatszolgáltatást (NaaS). A felhőalapú számítástechnika telepítési modelljeinek ki kell terjedniük a magán-, a közösségi, a nyilvános és a hibrid felhőre. A felhőalapú számítástechnikai szolgáltatási és telepítési modelleknek ugyanaz a jelentése, mint az ISO/IEC 17788: 2014 szabványban meghatározott szolgáltatási és telepítési modelleknek. A felhőszolgáltatás felhasználójának azon képessége, hogy egyoldalúan számítástechnikai kapacitásokról, például kiszolgálói időről vagy hálózati tárhelyről gondoskodjon, a felhőszolgáltató emberi beavatkozása nélkül, igény szerinti adminisztrációként jellemezhető.

A „széles távoli hozzáférés” kifejezést annak leírására használják, hogy a felhőképességeket a hálózaton keresztül biztosítják, és heterogén vékony vagy vastag kliensplatformok – beleértve a mobiltelefonokat, táblagépeket, laptopokat és munkaállomásokat – használatát elősegítő mechanizmusok révén férnek hozzájuk. A „méretezhető” kifejezés olyan számítástechnikai erőforrásokra utal, amelyeket a felhőszolgáltató rugalmasan allokál, függetlenül az erőforrások földrajzi elhelyezkedésétől, a kereslet ingadozásainak kezelése érdekében. A „rugalmas készlet” kifejezés leírja azokat a számítástechnikai erőforrásokat, amelyeket az igényeknek megfelelően hoznak létre és bocsátanak ki a rendelkezésre álló erőforrások gyors növelése és csökkentése érdekében, a munkaterheléstől függően. A „megosztható” kifejezés azoknak a számítástechnikai erőforrásoknak a leírására szolgál, amelyeket több olyan felhasználónak biztosítanak, akiknek közös hozzáférése van a szolgáltatáshoz, de ahol a feldolgozást minden felhasználó számára külön végzik, bár a szolgáltatást ugyanazon elektronikus berendezések nyújtják. Az „elosztott” kifejezés azon számítástechnikai erőforrások leírására szolgál, amelyek különböző hálózatba kötött számítógépeken vagy eszközökön találhatók, és amelyek üzenetközvetítéssel kommunikálnak és koordinálnak egymás között.

(34) Tekintettel az innovatív technológiák és az új üzleti modellek megjelenésére, várhatóan új felhőalapú számítástechnikai szolgáltatási és telepítési modellek jelennek meg a belső piacon, a fejlődő vásárlói igényeknek megfelelően. Ebben az összefüggésben a felhőszolgáltatásokat rendkívül elosztott formában lehet nyújtani, még közelebb az adatok generálásának vagy összegyűjtésének helyéhez, ezáltal átállva a hagyományos modellről a nagymértékben elosztottra („pereminformatika”).

(35) Az adatközpont-szolgáltatók által kínált szolgáltatásokat nem mindig biztosíthatják felhőszolgáltatások formájában. Ennek megfelelően az adatközpontok nem mindig képezik a felhőalapú számítástechnikai infrastruktúra részét. A hálózati és információs rendszerek biztonsága tekintetében fennálló összes kockázat kezelése érdekében ennek az irányelvnek ezért ki kell terjednie az olyan adatközpont-szolgáltatások szolgáltatóira is, amelyek nem felhőszolgáltatások. Ezen irányelv alkalmazásában az „adatközpont-szolgáltatás” kifejezésnek magában kell foglalnia olyan szolgáltatások nyújtását, amelyeknek részét képezik olyan struktúrák vagy struktúracsoportok, amelyek az adattárolási, feldolgozási és továbbítási szolgáltatásokat nyújtó informatikai és hálózati berendezések központosított elhelyezésére, összekapcsolására és működtetésére szolgálnak, az energia-elosztás és a környezetvédelmi ellenőrzés összes létesítményével és infrastruktúrájával együtt. Az „adatközpont-szolgáltatás” kifejezés nem vonatkozik az érintett szervezet saját tulajdonában lévő és saját céljaira működtetett házon belüli, vállalati adatközpontokra.

(36) A kutatási tevékenységek kulcsszerepet játszanak az új termékek és folyamatok kifejlesztésében. Az említett tevékenységek nagy részét olyan szervezetek végzik, amelyek megosztják, terjesztik vagy kereskedelmi célokra hasznosítják kutatásaik eredményeit. Az említett szervezetek ezért az értékláncok fontos szereplői lehetnek, ami hálózati és információs rendszereik biztonságát a belső piac általános kiberbiztonságának szerves részévé teszi. Kutatóhelyek alatt olyan szervezetek értendők, amelyek a Gazdasági Együttműködési és Fejlesztési Szervezet 2015-ös, „Iránymutatás a kutatással és a kísérleti fejlesztéssel kapcsolatos adatgyűjtésről és adatszolgáltatásról” című

Frascati kézikönyve értelmében tevékenységük lényeges részét alkalmazott kutatásra vagy kísérleti fejlesztésre összpontosítják, eredményeik kereskedelmi célú hasznosítása céljából, például termékek vagy eljárások előállítása vagy fejlesztése, szolgáltatások nyújtása, vagy ezek forgalmazása céljából.

(37) Az egyre növekvő kölcsönös függőségek az egyre inkább nemzetközivé váló és egymástól függő olyan szolgáltatási hálózat következményei, amelyek az Unió egész területén kulcsfontosságú infrastruktúrákat használnak olyan ágazatokban, mint például az energia, a közlekedés, a digitális infrastruktúra, az ivóvíz- és szennyvíz-, az egészségügy, a közigazgatás bizonyos vonatkozásai, valamint az űrágazat, amennyiben bizonyos szolgáltatások nyújtása olyan földi infrastruktúráktól függ, amelyek tulajdonosai, kezelői és üzemeltetői tagállamok vagy magánszemélyek, tehát nem tartoznak ide az Unió űrprogramja részeként az Unió vagy annak megbízottja tulajdonában lévő, általuk kezelt vagy üzemeltetett infrastruktúrák. Ezek a kölcsönös függőségek azt jelentik, hogy bármilyen zavarnak – akkor is, ha eredetileg csak egy szervezetre vagy egy ágazatra korlátozódik – szélesebb körben lépcsőzetes hatásai lehetnek, ami messzemenő és hosszú távú negatív hatásokat eredményezhet a szolgáltatások belső piacon történő nyújtásában. A Covid19-járvány idején felerősödött kibertámadások megmutatták az egyre inkább egymásra utalt társadalmak sérülékenységét az alacsony valószínűségű kockázatokkal szemben.

(38) Figyelemmel a nemzeti irányítási struktúrák közötti különbségekre, és a már meglévő ágazati megállapodások vagy az uniós felügyeleti és szabályozó testületek védelme érdekében a tagállamok számára lehetővé kell tenni, hogy kijelöljenek vagy létrehozzanak egy vagy több, a kiberbiztonságért és az ezen irányelv szerinti felügyeleti feladatokért felelős illetékes hatóságot.

(39) A határokon átnyúló együttműködés és a hatóságok közötti kommunikáció megkönnyítése és ezen irányelv hatékony végrehajtásának lehetővé tétele érdekében minden tagállamnak ki kell jelölnie egy egyedüli kapcsolattartó pontot, amely felelős a hálózati és információs rendszerek biztonságával kapcsolatos kérdések koordinálásáért és az uniós szintű, határokon átnyúló együttműködésért.

(40) Az egyedüli kapcsolattartó pontoknak hatékony, határokon átnyúló együttműködést kell biztosítaniuk más tagállamok érintett hatóságaival, valamint adott esetben a Bizottsággal és az ENISA-val. Az egyedüli kapcsolattartó pontokat ezért meg kell bízni azzal, hogy a jelentős, határokon átnyúló hatású eseményekre vonatkozó bejelentéseket a CSIRT vagy az illetékes hatóság kérésére továbbítsák a többi érintett tagállam egyedüli kapcsolattartó pontjának. Nemzeti szinten az egyedüli kapcsolattartó pontnak lehetővé kell tennie a többi illetékes hatósággal való zökkenőmentes ágazatközi együttműködést. Az (EU) 2022/2554 rendelet szerinti illetékes hatóságok a pénzügyi szervezetekkel kapcsolatos eseményekkel kapcsolatos releváns információkat az egyedüli kapcsolattartó pontoknak is megküldhetik, amelyek adott esetben azokat a CSIRT-eknek vagy az ezen irányelv szerinti illetékes hatóságoknak is továbbíthatják.

(41) A tagállamoknak mind technikai, mind szervezeti képességek tekintetében megfelelő felszereléssel kell rendelkezniük az események és kockázatok megelőzésére, észlelésére, az azokra való reagálásra, valamint azok mérséklésére. A tagállamoknak ezért ezen irányelv alapján létre kell hozniuk vagy ki kell jelölniük egy vagy több CSIRT-et, és biztosítaniuk kell, hogy azok megfelelő erőforrásokkal és technikai képességekkel rendelkezzenek. A CSIRT-eknek meg kell felelniük az ezen irányelvben meghatározott követelményeknek annak érdekében, hogy garantálják az események és kockázatok kezeléséhez szükséges hatékony és kompatibilis képességeket, valamint hogy biztosítsák a hatékony uniós szintű együttműködést. A tagállamok számára lehetővé kell tenni, hogy meglévő, számítógépes vészhelyzeteket elhárító csoportokat (CERT-eket) is kijelölhessenek CSIRT-eknek. A szervezetek és a CSIRT-ek közötti bizalmi kapcsolat erősítése érdekében azokban az esetekben, amikor a CSIRT az illetékes hatóság része, a tagállamok számára lehetővé kell tenni, hogy fontolóra vegyék a CSIRT-ek által végzett operatív feladatok közötti funkcionális elkülönítést, különösen az információmegosztással és a szervezetek számára nyújtott támogatással, illetve az illetékes hatóságok felügyeleti tevékenységeivel kapcsolatban.

(42) A CSIRT-ek feladata az események kezelése. Ez magában foglalja nagy mennyiségű, olykor érzékeny adatok kezelését. A tagállamoknak biztosítaniuk kell, hogy a CSIRT-ek rendelkezzenek az információk megosztására és feldolgozására szolgáló infrastruktúrával, valamint jól felszerelt személyzettel, amely biztosítja műveleteik titkosságát és megbízhatóságát. A CSIRT-ek e tekintetben magatartási kódexeket is elfogadhatnak.

(43) A személyes adatok tekintetében a CSIRT-ek számára lehetővé kell tenni, hogy az (EU) 2016/679 rendelettel összhangban valamely alapvető vagy fontos szervezet kérésére proaktív módon átvizsgálhassák a szervezet szolgáltatásainak nyújtásához használt hálózati és információs rendszereket. Adott esetben a tagállamoknak törekedniük kell arra, hogy valamennyi ágazati CSIRT számára egyenlő szintű technikai képességeket biztosítsanak. A tagállamok számára biztosítani kell annak lehetőségét, hogy segítséget kérhessenek az ENISA-tól CSIRT-jeik fejlesztéséhez.

(44) A CSIRT-eknek képesnek kell lenniük arra, hogy valamely alapvető vagy fontos szervezet kérésére nyomon kövessék a szervezet internetre mutató eszközeit mind a helyszínen, mind azon kívül, annak érdekében, hogy azonosítsák, megértsék és kezeljék a szervezet általános szervezeti kockázatait az ellátási lánc újonnan azonosított veszélyeivel vagy kritikus sérülékenységeivel kapcsolatban. A szervezetet ösztönözni kell arra, hogy tájékoztassa a CSIRT-et arról, hogy működtet-e kiváltságos irányítási interfészt, mivel ez befolyásolhatja a kockázatmérséklő intézkedések végrehajtásának sebességét.

(45) Tekintettel a kiberbiztonság terén folytatott nemzetközi együttműködés fontosságára, a CSIRT-ek részt vehetnek az ezen irányelv által létrehozott CSIRT-hálózat mellett nemzetközi együttműködési hálózatokban is. Ezért feladataik ellátása céljából a CSIRT-ek és az illetékes hatóságok számára lehetővé kell tenni, hogy információkat – többek között személyes adatokat – cseréljenek harmadik országok nemzeti számítógép-biztonsági eseményekre reagáló csoportjaival vagy illetékes hatóságaival, feltéve, hogy teljesülnek az uniós adatvédelmi jog személyes adatok harmadik országokba történő továbbítására vonatkozó feltételei, többek között az (EU) 2016/679 rendelet 49. cikkében foglaltak.

(46) Alapvető fontosságú, hogy megfelelő forrásokat biztosítsanak ezen irányelv célkitűzéseinek eléréséhez, valamint az illetékes hatóságok és a CSIRT-ek számára ezen irányelvben megállapított feladatok végrehajtásának lehetővé tételéhez. A tagállamok nemzeti szinten finanszírozási mechanizmust vezethetnek be az ezen irányelv értelmében a kiberbiztonságért felelős tagállami közigazgatási szervek feladatainak ellátásához szükséges kiadások fedezésére. E mechanizmusnak meg kell felelnie az uniós jognak, arányosnak és megkülönböztetéstől mentesnek kell lennie, és figyelembe kell vennie a biztonságos szolgáltatások nyújtására vonatkozó különböző megközelítéseket.

(47) A CSIRT-hálózatnak továbbra is hozzá kell járulnia a bizalom erősítéséhez és továbbra is elő kell mozdítania a tagállamok közötti gyors és hatékony operatív együttműködést. Az uniós szintű operatív együttműködés fokozása érdekében a CSIRT-hálózatnak fontolóra kell vennie, hogy felkérje a kiberbiztonsági szakpolitikában részt vevő uniós szerveket és ügynökségeket – például az Europolt – arra, hogy vegyenek részt a hálózat munkájában.

(48) A kiberbiztonság magas szintjének elérése és fenntartása érdekében az ezen irányelvben előírt nemzeti kiberbiztonsági stratégiáknak olyan koherens keretekből kell állniuk, amelyek stratégiai célkitűzéseket és prioritásokat határoznak meg a kiberbiztonság területén, valamint az ezek eléréséhez szükséges irányítást. Ezek a stratégiák egy vagy több jogalkotási vagy nem jogalkotási eszközből állhatnak.

(49) A kiberhigiéniai szakpolitikák biztosítják a hálózati és információs rendszerek infrastruktúrája, hardver-, szoftver- és online alkalmazásbiztonsága, valamint a szervezetek által felhasznált üzleti vagy végfelhasználói adatok védelmének alapjait. A kiberhigiéniai szakpolitikák közös alapvető gyakorlatokat foglalnak magukban, beleértve a szoftver- és hardverfrissítéseket, a jelszó megváltoztatását, az új telepítések kezelését, a rendszergazda-szintű hozzáférési fiókok korlátozását és az adatmentést, lehetővé teszik a proaktív felkészültségi keretet, valamint az általános biztonságot és védelmet események vagy kiberfenyegetések esetén. Az ENISA-nak nyomon kell követnie és elemeznie kell a tagállamok kiberhigiéniai szakpolitikáit.

(50) A kiberbiztonsággal kapcsolatos tudatosság és a kiberhigiénia elengedhetetlen az Unión belüli kiberbiztonság szintjének növeléséhez, különös tekintettel a kibertámadások során egyre gyakrabban használt csatlakoztatott eszközök növekvő számára. Törekedni kell az ilyen eszközökkel kapcsolatos kockázatokra vonatkozó általános tudatosság növelésére, míg az uniós szintű értékelések segíthetnek biztosítani az ilyen kockázatok egységes értelmezését a belső piacon.

(51) A tagállamoknak ösztönözniük kell minden olyan innovatív technológia alkalmazását, ideértve a mesterséges intelligenciát is, amelynek használata javíthatná a kibertámadások észlelését és megelőzését, lehetővé téve, hogy az erőforrásokat hatékonyabban lehessen a kibertámadásokra fordítani. A tagállamoknak ezért nemzeti kiberbiztonsági stratégiájukban ösztönözniük kell az ilyen technológiák – különösen a kiberbiztonság automatizált vagy félautomatizált eszközeivel kapcsolatos technológiák – használatát elősegítő kutatási és fejlesztési tevékenységeket, valamint adott esetben az ilyen technológiák felhasználóinak képzéséhez és e technológiák fejlesztéséhez szükséges adatok megosztását. Az innovatív technológiák, köztük a mesterséges intelligencia használatának teljes mértékben meg kell felelnie az uniós adatvédelmi jognak, ideértve az adatok pontosságára, az adatminimalizálásra, a méltányosságra és az átláthatóságra, valamint az adatbiztonságra vonatkozó adatvédelmi elveket, például a legkorszerűbb titkosítást. Teljes mértékben ki kell használni az (EU) 2016/679 rendeletben meghatározott beépített és alapértelmezett adatvédelemre vonatkozóan meghatározott követelményeket.

(52) A nyílt forráskódú kiberbiztonsági eszközök és alkalmazások nagyobb fokú nyitottságot biztosíthatnak, és pozitív hatást gyakorolhatnak az ipari innováció hatékonyságára. A nyílt szabványok elősegítik a biztonsági eszközök közötti interoperabilitást, ami az ipari szereplők biztonságát is szolgálja. A nyílt forráskódú kiberbiztonsági eszközök és alkalmazások ösztönözhetik a szélesebb fejlesztői közösséget, lehetővé téve a beszállítók diverzifikálását. A nyílt forráskód a kiberbiztonsággal kapcsolatos eszközök átláthatóbb ellenőrzési folyamatához és a sérülékenységek közösségi alapú felderítéséhez vezethet. A tagállamoknak ezért képesnek kell lenniük arra, hogy előmozdítsák a nyílt forráskódú szoftverek és nyílt szabványok használatát a nyílt hozzáférésű adatok és a nyílt forráskódok – az átláthatóságon alapuló biztonság részeként történő – felhasználásával kapcsolatos szakpolitikák folytatása révén. A nyílt forráskódú kiberbiztonsági eszközök bevezetését és fenntartható használatát előmozdító szakpolitikák különösen fontosak a jelentős végrehajtási költségekkel szembesülő kis- és középvállalkozások számára, mivel a költségek a konkrét alkalmazások vagy eszközök iránti igény csökkentésével minimalizálhatók.

(53) A városi közlekedési hálózatok fejlesztése, a vízellátás és a hulladékártalmatlanító létesítmények korszerűsítése, valamint a világítás és az épületek fűtése hatékonyságának növelése érdekében a városokban a közművek egyre inkább kapcsolódnak a digitális hálózatokhoz. Ezek a digitalizált közművek ki vannak téve a kibertámadásoknak, és sikeres kibertámadások esetén fennáll annak a kockázata, hogy összekapcsoltságuk miatt nagymértékben ártanak a polgároknak. A tagállamoknak nemzeti kiberbiztonsági stratégiájuk részeként olyan szakpolitikát kell kidolgozniuk, amely foglalkozik az ilyen összekapcsolt vagy intelligens városok fejlődésével és azok társadalomra gyakorolt lehetséges hatásaival.

(54) Az elmúlt években az Unióban exponenciálisan nőtt a zsarolóvírus-támadások száma, amelyek során a rosszindulatú szoftverek titkosítják az adatokat és rendszereket, és váltságdíjat követelnek felszabadításukért. A zsarolóvírus-támadások gyakoriságának és súlyosságának növekedése több tényezőre vezethető vissza, például a különböző támadási mintákra, a „szolgáltatásként nyújtott zsarolóvírus” és a kriptovaluták köré épülő bűnözői üzleti modellekre, a váltságdíjkövetelésekre és az ellátási láncot érintő támadások terjedésére. A tagállamoknak nemzeti kiberbiztonsági stratégiájuk részeként ki kell dolgozniuk egy olyan szakpolitikát, amely kezeli a zsarolóvírus-támadások növekedését.

(55) A kiberbiztonság területén működő köz-magán társulások (a továbbiakban: PPP-k) megfelelő keretet biztosíthatnak a tudáscseréhez, a bevált gyakorlatok megosztásához és az érdekelt felek közötti közös megértési szint kialakításához. A tagállamoknak olyan szakpolitikákat kell előmozdítaniuk, amelyek támogatják a kiberbiztonsági PPP-k létrehozását. E szakpolitikáknak egyértelművé kell tenniük többek között a hatályt és a részt vevő érdekelt feleket, az irányítási modellt, a rendelkezésre álló finanszírozási lehetőségeket, valamint a részt vevő érdekelt felek közötti interakciót a PPP-k tekintetében. A PPP-k kihasználhatják a magánszektorbeli szervezetek szakértelmét annak érdekében, hogy segítsék az illetékes hatóságokat a legkorszerűbb szolgáltatások és folyamatok kifejlesztésében, ideértve az információcserét, a korai figyelmeztetéseket, a kiberfenyegetés- és kiberesemény-gyakorlatokat, a válságkezelést és a rezilienciatervezést.

(56) A tagállamoknak nemzeti kiberbiztonsági stratégiáikban foglalkozniuk kell a kis- és középvállalkozások sajátos kiberbiztonsági igényeivel. A kis- és középvállalkozások Unió-szerte az ipari és üzleti piac jelentős hányadát képviselik, és gyakran nehezen tudnak alkalmazkodni az összekapcsoltabb világban az új üzleti gyakorlatokhoz és a digitális környezethez, amelyben az alkalmazottak egyre inkább otthonról dolgoznak és az üzleti tevékenységet egyre inkább online folytatják. Egyes kis- és középvállalkozások olyan sajátos kiberbiztonsági kihívásokkal néznek szembe, mint például az alacsony kibertudatosság, a távoli informatikai biztonság hiánya, a kiberbiztonsági megoldások magas költsége és a fokozott fenyegetettségi szint, például a zsarolóvírusok, amelyekkel kapcsolatban iránymutatást és segítséget kell kapniuk. A kis- és középvállalkozások egyre inkább az ellátási lánccal szembeni támadások célpontjává válnak, mivel kevésbé szigorú kiberbiztonsági kockázatkezelési intézkedésekkel és támadáskezeléssel rendelkeznek, és korlátozott biztonsági erőforrásaik vannak. Az ilyen ellátási láncot érintő támadások nem csak elszigetelten hatnak a kis- és középvállalkozásokra és azok működésére, hanem lépcsőzetes hatást gyakorolhatnak az azon szervezetek elleni nagyobb támadásokra is, amelyek számára a kis- és

középvállalkozások ellátást biztosítottak. A tagállamoknak nemzeti kiberbiztonsági stratégiáik révén segíteniük kell a kis- és középvállalkozásokat az ellátási láncaikban felmerülő kihívások kezelésében. A tagállamoknak nemzeti vagy regionális szinten kapcsolattartó pontot kell létrehozniuk a kis- és középvállalkozások számára, amely vagy iránymutatást és segítséget nyújt a kis- és középvállalkozások számára, vagy a megfelelő szervekhez irányítja őket a kiberbiztonsággal kapcsolatos kérdésekre vonatkozó iránymutatást és segítséget illetően. Arra is ösztönzik a tagállamokat, hogy kínáljanak olyan szolgáltatásokat, mint a honlapok konfigurációja és naplózás lehetővé tétele, az ilyen képességekkel nem rendelkező mikrovállalkozások és kisvállalkozások számára.

(57) Nemzeti kiberbiztonsági stratégiáik részeként a tagállamoknak egy szélesebb körű védelmi stratégia részeként az aktív kiberbiztonság előmozdítására irányuló szakpolitikákat kell elfogadniuk. A reaktív reagálás helyett az aktív kiberbiztonság a hálózatbiztonságot fenyegető betörések aktív módon történő megelőzését, észlelését, nyomon követését, elemzését és mérséklését jelenti, a támadás áldozatául esett hálózaton belül és azon kívül telepített képességek igénybevételével kombinálva. Ez magában foglalhatja azt, hogy a tagállamok ingyenes szolgáltatásokat vagy eszközöket kínálnak egyes szervezetek számára, többek között önkiszolgáló ellenőrzéseket, felderítési eszközöket és eltávolítási szolgáltatásokat. A hálózati és információs rendszerek elleni támadások sikeres megelőzésére, észlelésére, kezelésére és megakadályozására irányuló erőfeszítéseknek egységeseknek kell lenniük, ezért alapvető fontosságú a fenyegetésekre vonatkozó információk és elemzések, a kibertevékenységre figyelmeztető riasztások és a válaszintézkedések gyors és automatikus megosztása és megértése. Az aktív kiberbiztonság olyan védelmi stratégián alapul, amely kizárja az offenzív intézkedéseket.

(58) Mivel a hálózati és információs rendszerek sérülékenységeinek kiaknázása jelentős zavarokat és kárt okozhat, az ilyen sérülékenységek gyors azonosítása és elhárítása fontos tényező a kockázat csökkentésében. Az említett rendszereket fejlesztő vagy kezelő szervezeteknek ezért megfelelő eljárásokat kell kidolgozniuk a sérülékenységek felfedezéskor történő kezelésére. Mivel a sérülékenységeket gyakran harmadik felek fedezik fel és teszik közzé, az IKT-termékek vagy IKT-szolgáltatások gyártójának vagy szolgáltatójának szintén be kell vezetnie a sérülékenységre vonatkozó információk harmadik felektől történő fogadásához szükséges eljárásokat. Ebben a tekintetben az ISO/IEC 30111 és az ISO/IEC 29147 nemzetközi szabvány útmutatást nyújt a sérülékenységek kezeléséhez, illetve a sérülékenység közzétételéhez. A sérülékenységek közzétételére vonatkozó önkéntes keret előmozdítása érdekében különösen fontos az adatszolgáltatásra kötelezett természetes és jogi személyek és az IKT-termékek vagy IKT-szolgáltatások gyártói vagy nyújtói közötti koordináció megerősítése. A sérülékenység összehangolt közzététele strukturált folyamatot határoz meg, amelyen keresztül a potenciálisan sérülékeny IKT-termékek vagy IKT-szoltáltatások gyártói vagy nyújtói számára a sérülékenységeket oly módon jelentik, hogy a szervezet diagnosztizálhassa és orvosolhassa a sérülékenységet, mielőtt a sérülékenységre vonatkozó részletes információkat harmadik felek vagy a nyilvánosság számára közzétenné. A sérülékenység összehangolt közzétételének magában kell foglalnia az adatszolgáltatásra kötelezett természetes és jogi személy és a potenciálisan sérülékeny IKT-termékek vagy IKT-szoltáltatások gyártói vagy nyújtói közötti koordinációt a sérülékenységek orvoslásának és közzétételének időzítése tekintetében.

(59) A Bizottságnak, az ENISA-nak és a tagállamoknak továbbra is elő kell mozdítaniuk a nemzetközi szabványokkal és a meglévő ágazati bevált gyakorlatokkal való összehangolást a kiberbiztonsági kockázatkezelés területén, például az ellátási lánc biztonságának értékelése, az információmegosztás és a sérülékenységek közzététele terén.

(60) A tagállamoknak az ENISA-val együttműködve intézkedéseket kell hozniuk a sérülékenységek összehangolt közzétételének egy megfelelő nemzeti szakpolitika kialakításával történő megkönnyítésére. Nemzeti szakpolitikájuk részeként a tagállamoknak törekedniük kell arra, hogy – a nemzeti joggal összhangban – a lehető legnagyobb mértékben kezeljék a sérülékenységeket kutatók előtt álló kihívásokat, beleértve a büntetőjogi felelősségre vonásnak való potenciális kitettségüket is. Tekintettel arra, hogy a sérülékenységeket vizsgáló természetes és jogi személyek egyes tagállamokban büntetőjogi és polgári jogi szempontból felelősségre vonhatók, a tagállamokat arra ösztönzik, hogy fogadjanak el iránymutatásokat az információbiztonsági kutatók büntetőeljárás alá vonásának mellőzésére és a tevékenységeikkel kapcsolatos polgári jogi felelősség alóli mentességre vonatkozóan.

(61) A tagállamoknak ki kell jelölniük valamelyik CSIRT-jüket koordinátornak, amely megbízható közvetítőként jár el a bejelentő természetes vagy jogi személyek és – a sérülékenység által valószínűleg érintett – IKT-termékek vagy IKT-szolgáltatások gyártói vagy nyújtói között, amennyiben ez szükséges. A koordinátorként kijelölt CSIRT feladatai közé tartozik az érintett szervezetek azonosítása és a velük való kapcsolatfelvétel, a sérülékenységet bejelentő természetes vagy jogi személyek támogatása, a közzétételi ütemtervek megtárgyalása és a több szervezetet érintő

sérülékenységek kezelése (több felet érintő sérülékenységek összehangolt közzététele). Ha a bejelentett sérülékenység több tagállamban is jelentős hatást gyakorolhat bizonyos szervezetekre, a koordinátorként kijelölt CSIRT-eknek adott esetben együtt kell működniük a CSIRT-hálózaton belül.

(62) Az IKT-termékeket és IKT-szolgáltatásokat érintő sérülékenységekkel kapcsolatos helyes és időszerű információkhoz való hozzáférés hozzájárul a jobb kiberbiztonsági kockázatkezeléshez. A sérülékenységekről nyilvánosan elérhető információk forrásai fontos eszköznek minősülnek a szervezetek és azok szolgáltatásainak felhasználói, de az illetékes hatóságok és a CSIRT-ek számára is. Emiatt az ENISA-nak európai sérülékenység-adatbázist kell létrehoznia, amelyben a szervezetek – függetlenül attól, hogy ezen irányelv hatálya alá tartoznak-e – és a hálózati és információs rendszereket biztosító beszállítóik, valamint az illetékes hatóságok és a CSIRT-ek önkéntes alapon közzétehetik és regisztrálhatják a nyilvánosan ismert sérülékenységeket annak érdekében, hogy lehetővé tegyék a felhasználók számára a megfelelő mérséklési intézkedések megtételét. Az adatbázis célja, hogy kezelje azokat az egyedi kihívásokat, amelyeket a kockázatok jelentenek az unióbeli szervezetek számára. Ezen túlmenően az ENISA-nak megfelelő eljárást kell létrehoznia a közzétételi folyamat tekintetében annak érdekében, hogy elegendő idő álljon a szervezetek rendelkezésére arra, hogy mérséklési intézkedéseket hozzanak sérülékenységeik tekintetében, és a legkorszerűbb kiberbiztonsági kockázatkezelési intézkedéseket, valamint géppel olvasható adatkészleteket és megfelelő interfészeket alkalmazzanak. A sérülékenységek közzététele kultúrájának ösztönzése érdekében a közzétételnek nem szabad káros hatást gyakorolnia a bejelentő természetes vagy jogi személyekre.

(63) Noha léteznek hasonló sérülékenység-nyilvántartások vagy adatbázisok, ezeket nem az Unióban letelepedett szervezetek üzemeltetik és tartják fenn. Az ENISA által fenntartott európai sérülékenység-adatbázis átláthatóbbá tenné a sérülékenységek hivatalos közzététele előtti közzétételi folyamatot, és rezilienciát biztosítana a hasonló szolgáltatások nyújtásának megszakadása vagy zavara esetén. A kettős erőfeszítések lehető legnagyobb mértékű megelőzése és a kiegészítő jelleg elérése érdekében az ENISA-nak fel kell tárnia a harmadik országok joghatósága alá tartozó hasonló nyilvántartásokkal vagy adatbázisokkal kialakítandó strukturált együttműködési megállapodások megkötésének lehetőségét. Az ENISA-nak különösen meg kell vizsgálnia a gyakori sérülékenységek és kitettségek (CVE) rendszere üzemeltetőivel való szoros együttműködés lehetőségét.

(64) Az együttműködési csoportnak támogatnia kell és elő kell segítenie a stratégiai együttműködést és az információcserét, valamint erősítenie kell a tagállamok közötti bizalmat. Az együttműködési csoportnak kétévente munkaprogramot kell kidolgoznia. A munkaprogramnak tartalmaznia kell az együttműködési csoport céljainak és feladatainak végrehajtása érdekében meghozandó intézkedéseket. Az ezen irányelv szerinti első munkaprogram kialakításának időkeretét összhangba kell hozni az (EU) 2016/1148 irányelv szerint kialakított utolsó munkaprogram időkeretével az együttműködési csoport munkájában bekövetkező esetleges zavarok elkerülése érdekében.

(65) Az együttműködési csoportnak az útmutató dokumentumok kidolgozása során következetesen fel kell térképeznie a nemzeti megoldásokat és tapasztalatokat, fel kell mérnie az együttműködési csoport eredményeinek nemzeti megközelítésekre gyakorolt hatását, meg kell vitatnia a végrehajtási kihívásokat és konkrét ajánlásokat kell megfogalmaznia, különös tekintettel ezen irányelv átültetésének a tagállamok közti összehangolása elősegítésére, amelyet a meglévő szabályok jobb végrehajtása révén kell elérni. Az együttműködési csoportnak annak érdekében is fel kell térképeznie a nemzeti megoldásokat, hogy előmozdítsa az egyes ágazatokra Unió-szerte alkalmazott kiberbiztonsági megoldások összeegyeztethetőségét. Ez különösen releváns azokban az ágazatokban, amelyek nemzetközi és határokon átnyúló jellegűek.

(66) Az együttműködési csoportnak továbbra is rugalmas fórumnak kell maradnia, és reagálnia kell a változó és új szakpolitikai prioritásokra és kihívásokra, az erőforrások rendelkezésre állásának figyelembevételével. Rendszeres közös megbeszéléseket szervezhetne az Unió egész területéről érkező magánszférabeli érdekelt felekkel, hogy megvitassák az együttműködési csoport tevékenységeit, és adatokat és információkat gyűjtsenek a felmerülő szakpolitikai kihívásokról. Emellett az együttműködési csoportnak rendszeresen értékelnie kellene a kiberfenyegetések vagy -események, például a zsarolóvírusok helyzetét. Az uniós szintű együttműködés fokozása érdekében az együttműködési csoportnak fontolóra kell vennie a kiberbiztonsági szakpolitikában részt vevő uniós intézmények, szervek, hivatalok és ügynökségek, például az Európai Parlament, az Europol, az Európai Adatvédelmi

Testület, az Európai Unió (EU) 2018/1139 rendelettel létrehozott Repülésbiztonsági Ügynöksége és az Európai Unió (EU) 2021/696 európai parlamenti és tanácsi rendelettel ([14]) létrehozott Űrprogramügynöksége meghívását a munkájában történő részvételre.

(67) A tagállamok közötti együttműködés javítása és a bizalom erősítése érdekében az illetékes hatóságok és a CSIRT-ek számára lehetővé kell tenni, hogy konkrét keretek között és adott esetben az ilyen csereprogramokban részt vevő tisztviselők számára előírt szükséges biztonsági tanúsítvány megszerzésétől függően részt vegyenek a más tagállamok tisztviselőire vonatkozó csereprogramokban. Az illetékes hatóságoknak meg kell hozniuk a szükséges intézkedéseket annak érdekében, hogy más tagállamok tisztviselői tényleges szerepet tölthessenek be a fogadó illetékes hatóság vagy a fogadó CSIRT tevékenységeiben.

(68) A tagállamoknak hozzá kell járulniuk az (EU) 2017/1584 bizottsági ajánlásban ([15]) meghatározott uniós kiberbiztonsági válságelhárítási keret létrehozásához a meglévő együttműködési hálózatokon, különösen az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatán (a továbbiakban: EU-CyCLONe), a CSIRT-hálózaton és az együttműködési csoporton keresztül. Az EU-CyCLONe-nak és a CSIRT-hálózatnak az együttműködés részleteit meghatározó eljárási megállapodások alapján kell együttműködniük és el kell kerülniük a feladatok megkettőződését. Az EU-CyCLONe eljárási szabályzatának részletesen meg kell határoznia az említett hálózat működésének szabályait, ideértve a hálózat szerepét, az együttműködési módokat, az egyéb érintett szereplőkkel folytatott interakciókat és az információmegosztási sablonokat, valamint a kommunikáció eszközeit. Az uniós szintű válságkezelés során az érintett feleknek az (EU) 2018/1993 tanácsi végrehajtási határozat ([16]) szerinti uniós politikai szintű integrált válságelhárítási mechanizmusra (IPCR-mechanizmus) kell támaszkodniuk. A Bizottságnak az említett célra az ARGUS magas szintű, ágazatok közötti válságkoordinációs folyamatát kell alkalmaznia. Ha a válságnak fontos külső vagy közös biztonság- és védelempolitikai dimenziója van, aktiválni kell az Európai Külügyi Szolgálat válságelhárítási mechanizmusát.

(69) Az (EU) 2017/1584 ajánlás mellékletével összhangban nagyszabású kiberbiztonsági eseménynek azt az eseményt kell tekinteni, amely olyan mértékű zavart okoz, amely meghaladja valamely tagállamnak az arra való reagálása képességét, vagy amely legalább két tagállamra jelentős hatást gyakorol. Okuktól és hatásuktól függően a nagyszabású kiberbiztonsági események eszkalálódhatnak, és olyan teljes körű válsággá válhatnak, amely nem teszi lehetővé a belső piac megfelelő működését, illetve súlyos közrendi és közbiztonsági kockázatot jelent a szervezetekre vagy a polgárokra nézve több tagállamban vagy az Unió egészében. Tekintettel az említett események széles hatókörére és a legtöbb esetben határokon átnyúló jellegére, a tagállamoknak és az érintett uniós intézményeknek, szerveknek, hivataloknak és ügynökségeknek technikai, operatív és politikai szinten együtt kell működniük a reagálás Unión belüli megfelelő összehangolása érdekében.

(70) A nagyszabású kiberbiztonsági események és válságok uniós szinten összehangolt fellépést tesznek szükségessé a gyors és hatékony reagálás biztosítása érdekében, az ágazatok és a tagállamok közötti nagyfokú kölcsönös függőség miatt. A kibertámadásokkal szemben reziliens hálózati és információs rendszerek rendelkezésre állása, valamint az adatok rendelkezésre állása, bizalmas jellege és integritása létfontosságú az Unió biztonsága, polgárainak, vállalkozásainak és intézményeinek az eseményekkel és kiberfenyegetésekkel szembeni védelme, valamint az egyének és szervezetek abba vetett bizalmának növelése szempontjából, hogy az Unió képes előmozdítani és megvédeni az emberi jogokon, az alapvető szabadságokon, a demokrácián és a jogállamiságon alapuló globális, nyitott, szabad, stabil és biztonságos kiberteret.

([14]) Az Európai Parlament és a Tanács (EU) 2021/696 rendelete (2021. április 28.) az uniós űrprogram és az Európai Unió Űrprogramügynökségének a létrehozásáról, valamint a 912/2010/EU, az 1285/2013/EU és a 377/2014/EU rendelet és az 541/2014/EU határozat hatályon kívül helyezéséről (HL L 170., 2021.5.12., 69. o.).

([15]) A Bizottság (EU) 2017/1584 ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról (HL L 239., 2017.9.19., 36. o.).

([16]) A Tanács (EU) 2018/1993 végrehajtási határozata (2018. december 11.) az uniós politikai szintű integrált válságelhárítási mechanizmusról (HL L 320., 2018.12.17., 28. o.).

(71) Az EU-CyCLONe-nak közvetítőként kell működnie a technikai és politikai szint között a nagyszabású kiberbiztonsági események és válságok során, fokoznia kell az operatív szintű együttműködést, és támogatnia kell a politikai szintű döntéshozatalt. Tekintettel a Bizottság válságkezelési hatáskörére, az EU-CyCLONe-nak a Bizottsággal együttműködésben a CSIRT-hálózat megállapításaira kell építenie, és fel kell használnia saját kapacitásait a nagyszabású kiberbiztonsági események és válságok hatásvizsgálatának elkészítésére.

(72) A kibertámadások határokon átnyúló jellegűek, és egy jelentős esemény megzavarhatja és károsíthatja azokat a kritikus információs infrastruktúrákat, amelyektől a belső piac zavartalan működése függ. Az (EU) 2017/1584 ajánlás valamennyi érintett szereplő szerepével foglalkozik. Ezen túlmenően az 1313/2013/EU európai parlamenti és tanácsi határozattal ([17]) létrehozott uniós polgári védelmi mechanizmus keretében a Bizottság felelős az általános felkészültségi intézkedésekért, ideértve a Veszélyhelyzet-reagálási Koordinációs Központ és a közös veszélyhelyzeti kommunikációs és tájékoztatási rendszer irányítását, a helyzetismereti és -elemzési képesség fenntartását és továbbfejlesztését, valamint a szakértői csoportok valamely tagállam vagy harmadik ország segítségkérése esetén történő mozgósítására és kiküldésére vonatkozó képesség létrehozását és irányítását. A Bizottság feladata továbbá, hogy elemző jelentéseket készítsen az (EU) 2018/1993 végrehajtási határozat szerinti IPCR-mechanizmus számára, többek között a kiberbiztonsági helyzetismeretről és felkészültségről, valamint a helyzetismeretről és a válságelhárításról a mezőgazdaság, a kedvezőtlen időjárási viszonyok, a konfliktusok feltérképezése és előrejelzése, a természeti katasztrófákra vonatkozó korai előrejelző rendszerek, az egészségügyi vészhelyzetek, a fertőző betegségek felügyelete, a növényegészségügy, a vegyi események, az élelmiszer- és takarmánybiztonság, az állategészségügy, a migráció, a vámügy, a nukleáris és radiológiai vészhelyzetek és az energiaügy területén.

(73) Az Unió adott esetben nemzetközi megállapodásokat köthet az EUMSZ 218. cikkével összhangban harmadik országokkal vagy nemzetközi szervezetekkel, lehetővé téve és megszervezve részvételüket az együttműködési csoport, a CSIRT-hálózat és az EU-CyCLONe egyes tevékenységeiben. Az ilyen megállapodásoknak védeniük kell az Unió érdekeit és biztosítaniuk kell az adatok megfelelő védelmét. Ez nem zárja ki a tagállamok azon jogát, hogy együttműködjenek harmadik országokkal a sérülékenységek és a kiberbiztonsági kockázatok kezelése terén, megkönnyítve ezáltal a jelentéstételt és az általános információmegosztást az uniós joggal összhangban.

(74) Ezen irányelv – többek között a sérülékenységek kezelése, a kiberbiztonsági kockázatkezelési intézkedések, a jelentéstételi kötelezettségek és a kiberbiztonsági információmegosztási megállapodások tekintetében történő – hatékony végrehajtásának elősegítése érdekében a tagállamok együttműködhetnek harmadik országokkal, és folytathatnak e célból megfelelőnek ítélt tevékenységeket, ideértve többek között a kiberfenyegetésekre, eseményekre, sérülékenységekre, eszközökre és módszerekre, taktikákra, technikákra és eljárásokra, a kiberbiztonsági válságok kezelésére való felkészültségre és az erre irányuló gyakorlatokra, képzésre, bizalomépítésre és strukturált információmegosztási megállapodásokra vonatkozó információcserét.

(75) A kölcsönös bizalom erősítése és a kiberbiztonság egységesen magas szintjének elérése érdekében szakértői értékeléseket kell bevezetni. A szakértői értékelések értékes felismeréseket és ajánlásokat eredményezhetnek, erősítve az általános kiberbiztonsági képességeket, újabb funkcionális útvonalat teremtve a bevált gyakorlatok tagállamok közötti megosztásához, és hozzájárulva a tagállamok kiberbiztonsággal kapcsolatos érettségi szintjének javításához. Ezen túlmenően a szakértői értékeléseknek figyelembe kell venniük a hasonló mechanizmusok – például a CSIRT-hálózat szakértői értékelési rendszere – eredményeit, hozzáadott értéket kell teremteniük, és el kell kerülniük a párhuzamos munkavégzést. A szakértői értékelések megvalósítása nem sértheti a bizalmas és minősített adatok védelmére vonatkozó uniós vagy nemzeti jogot.

(76) Az együttműködési csoportnak önértékelési módszertant kell kidolgoznia a tagállamok számára, törekedve olyan tényezők beemelésére, mint a kiberbiztonsági kockázatkezelési intézkedések és jelentéstételi kötelezettségek végrehajtásának szintje, az illetékes hatóságok képességeinek szintje és feladatai ellátásának hatékonysága, a CSIRT-ek operatív képességei, a kölcsönös segítségnyújtás végrehajtási szintje, a kiberbiztonsági információmegosztási megállapodások végrehajtási szintje, illetve a határokon vagy ágazatokon átnyúló jellegű konkrét kérdések. A tagállamokat ösztönözni kell az önértékelések rendszeres elvégzésére és önértékeléseik eredményeinek az együttműködési csoporton belüli ismertetésére és megvitatására.

([17]) Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról (HL L 347., 2013.12.20., 924. o.).

(77) A hálózati és információs rendszer biztonságának biztosítása nagymértékben az alapvető és a fontos szervezetek felelőssége. Ösztönözni és fejleszteni kell a kockázatértékeléseket és a felmerülő kockázatok súlyosságának megfelelő kiberbiztonsági kockázatkezelési intézkedések végrehajtását egyaránt magában foglaló kockázatkezelési kultúrát.

(78) A kiberbiztonsági kockázatkezelési intézkedéseknek figyelembe kell venniük az alapvető vagy fontos szervezet hálózati és információs rendszerektől való függőségének mértékét, és intézkedéseket kell tartalmazniuk az események kockázatainak azonosítására, az események megelőzésére, észlelésére, az azokra való reagálásra és azokat követően a működés helyreállítására, valamint azok hatásainak mérséklésére. A hálózati és információs rendszerek biztonságának magában kell foglalnia a tárolt, továbbított és kezelt adatok biztonságát. A kiberbiztonsági kockázatkezelési intézkedéseknek rendszerszintű elemzést kell biztosítaniuk, figyelembe véve az emberi tényezőt annak érdekében, hogy teljes képet lehessen alkotni a hálózati és információs rendszer biztonságáról.

(79) Mivel a hálózati és információs rendszerek biztonságát fenyegető veszélyek különböző eredetűek lehetnek, a kiberbiztonsági kockázatkezelési intézkedéseknek minden veszélyre kiterjedő megközelítésen kell alapulniuk, amelynek célja a hálózati és információs rendszereknek és azok fizikai környezetének a védelme minden olyan eseménytől, mint például a lopás, a tűz, az árvíz, a távközlési és áramellátási zavarok, vagy valamely alapvető vagy fontos szervezet információs és információfeldolgozó létesítményeihez való jogosulatlan fizikai hozzáférés, az azokban keletkezett kár és az azokon végrehajtott beavatkozás, amely veszélyeztetheti a tárolt, továbbított vagy kezelt adatok vagy a hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, integritását vagy bizalmas jellegét. A kiberbiztonsági kockázatkezelési intézkedéseknek ezért a hálózati és információs rendszerek fizikai és a környezetbiztonságával is foglalkozniuk kell azáltal, hogy magukban foglalnak olyan intézkedéseket az európai és nemzetközi szabványokkal, például az ISO/IEC 27000 szabványsorozatban foglalt szabványokkal összhangban, amelyek célja, hogy védjék az ilyen rendszereket a rendszerhibákkal, az emberi hibával, a rosszindulatú cselekményekkel vagy a természeti jelenségekkel szemben. E tekintetben az alapvető és fontos szervezeteknek kiberbiztonsági kockázatkezelési intézkedéseik részeként foglalkozniuk kell az emberi erőforrásokhoz kapcsolódó biztonsággal is, és megfelelő hozzáférés-ellenőrzési szabályzatokkal kell rendelkezniük. Ezeknek az intézkedéseknek összhangban kell lenniük az (EU) 2022/2557 irányelvvel.

(80) A kiberbiztonsági kockázatkezelési intézkedéseknek való megfelelés igazolása céljából, valamint az (EU) 2019/881 európai parlamenti és tanácsi rendelettel ([18]) összhangban elfogadott megfelelő európai kiberbiztonsági tanúsítási rendszerek hiányában a tagállamoknak – az együttműködési csoporttal és az európai kiberbiztonsági tanúsítási csoporttal konzultálva – elő kell mozdítaniuk a vonatkozó európai és nemzetközi szabványok alapvető és fontos szervezetek általi használatát, vagy előírhatják a szervezetek számára, hogy tanúsított IKT-termékeket, IKT-szolgáltatásokat és IKT-folyamatokat használjanak.

(81) Az alapvető és fontos szervezetekre aránytalan pénzügyi és adminisztratív terhek előírásának elkerülése érdekében a kiberbiztonsági kockázatkezelési intézkedéseknek arányosnak kell lenniük az érintett hálózati és információs rendszert fenyegető kockázattal, figyelembe véve az ilyen intézkedések legkorszerűbb állását és adott esetben a vonatkozó európai és nemzetközi szabványokat, valamint végrehajtásuk költségeit.

(82) A kiberbiztonsági kockázatkezelési intézkedéseknek arányosnak kell lenniük az alapvető vagy fontos szervezet kockázatoknak való kitettségének mértékével, valamint azon társadalmi és gazdasági hatással, amellyel az esemény járna. Az alapvető és fontos szervezetekhez igazított kiberbiztonsági kockázatkezelési intézkedések meghatározásakor megfelelően figyelembe kell venni az alapvető és fontos szervezetek eltérő kockázati kitettségét, például a szervezet kritikus jellegét, azokat a kockázatokat – köztük társadalmi kockázatokat is –, amelyeknek a szervezet ki van téve, a szervezet méretét és az események bekövetkezésének valószínűségét, valamint azok súlyosságát, ideértve társadalmi és gazdasági hatásukat is.

([18]) Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).

(83) Az alapvető és fontos szervezeteknek biztosítaniuk kell a tevékenységük során használt hálózati és információs rendszerek biztonságát. Ezek a rendszerek elsősorban magánhálózatok és információs rendszerek, amelyeket az alapvető és fontos szervezetek belső informatikai személyzete kezel, vagy amelyek biztonságát kiszervezték. Az ezen irányelvben megállapított kiberbiztonsági kockázatkezelési intézkedéseket és jelentéstételi kötelezettségeket az érintett alapvető és fontos szervezetekre alkalmazni kell, függetlenül attól, hogy az említett szervezetek házon belül végzik-e hálózatuk és információs rendszereik karbantartását vagy kiszervezik azt.

(84) A határokon átnyúló jellegükre tekintettel uniós szinten magasabb fokú harmonizációt kell alkalmazni a következőkre: DNS-szolgáltatók, legfelső szintű doménnév-nyilvántartók, felhőszolgáltatók, adatközpont-szolgáltatók, tartalomszolgáltató hálózati szolgáltatók, irányított szolgáltatók és irányított biztonsági szolgáltatók, az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatói, valamint bizalmi szolgáltatók. A kiberbiztonsági kockázatkezelési intézkedések e szervezetek tekintetében való végrehajtását ezért végrehajtási jogi aktussal kell elősegíteni.

(85) A szervezet ellátási láncából és a beszállítóival – például az adattárolási és adatkezelési szolgáltatókkal vagy az irányított biztonsági szolgáltatókkal és szoftverszerkesztőkkel – való kapcsolatából eredő kockázatok kezelése különösen fontos, tekintettel az olyan események előfordulási gyakoriságára, amikor a szervezetek kibertámadások áldozatává válnak, és amikor a rosszindulatú elkövetők azzal tudják veszélyeztetni a szervezet hálózatának és információs rendszereinek biztonságát, hogy harmadik fél termékeit és szolgáltatásait érintő sérülékenységeket kihasználnak. Az alapvető és fontos szervezeteknek ezért fel kell mérniük és figyelembe kell venniük beszállítóik és szolgáltatóik termékeinek, szolgáltatásainak, az azokba beépített kiberbiztonsági kockázatkezelési intézkedéseknek, valamint kiberbiztonsági gyakorlatainak általános minőségét és rezilienciáját, beleértve a biztonságos fejlesztési eljárásaikat is. Az alapvető és fontos szervezeteket különösen arra kell ösztönözni, hogy a kiberbiztonsági kockázatkezelési intézkedéseket építsék be a közvetlen beszállítókkal és szolgáltatókkal kötött szerződéses megállapodásokba. Az említett szervezetek figyelembe vehetik a más szintű beszállítóktól és szolgáltatóktól eredő kockázatokat is.

(86) A szolgáltatók közül az irányított biztonsági szolgáltatók olyan területeken, mint az eseményekre való reagálás, behatolási tesztek, biztonsági auditok és tanácsadás, különösen fontos szerepet töltenek be abban, hogy segítsék a szervezeteket az események megelőzésében, észlelésében, az azokra való reagálásban, vagy az eseményt követően a működés helyreállításában. Azonban maguk az irányított biztonsági szolgáltatók is kibertámadások célpontjai, és a szervezetek működésébe való szoros integrációjuk miatt különös kockázatot jelentenek. Az alapvető és fontos szervezeteknek ezért fokozott gondossággal kell eljárniuk az irányított biztonsági szolgáltató kiválasztása során.

(87) Az illetékes hatóságok a felügyeleti feladataikkal összefüggésben olyan kiberbiztonsági szolgáltatásokat is igénybe vehetnek, mint például a biztonsági auditok, a behatolási tesztek vagy az eseményekre való reagálás.

(88) Az alapvető és fontos szervezeteknek foglalkozniuk kell azon kockázatokkal is, amelyek egy szélesebb ökoszisztémán belüli más érdekelt felekkel folytatott interakcióikból és kapcsolataikból fakadnak, többek között az ipari kémkedés elleni küzdelem és az üzleti titkok védelme tekintetében. Az említett szervezeteknek különösen meg kell tenniük a megfelelő intézkedéseket annak biztosítása érdekében, hogy az egyetemekkel és a kutatóintézetekkel folytatott együttműködésük kiberbiztonsági szabályzatukkal összhangban történjen, és a bevált gyakorlatokat kövessék az információkhoz való általános hozzáférés és terjesztés, valamint különösen a szellemi tulajdon védelme tekintetében. Hasonlóképpen – tekintettel az adatoknak az alapvető és fontos szervezetek tevékenysége szempontjából fennálló fontosságára és értékére – amennyiben az adatok átalakítására és harmadik felektől származó adatelemzési szolgáltatásokra támaszkodnak, az említett szervezeteknek meg kell tenniük a megfelelő kiberbiztonsági kockázatkezelési intézkedéseket.

(89) Az alapvető és fontos szervezeteknek az alapvető kiberhigiéniai gyakorlatok széles skáláját kell alkalmazniuk, például a zéró bizalom alapelveit, a szoftverfrissítéseket, az eszközkonfigurációt, a hálózatszegmentálást, a személyazonosság- és hozzáférés-kezelést vagy a felhasználói tudatosságot, továbbá képzéseket kell szervezniük alkalmazottaik számára és fel kell hívniuk a figyelmet a kiberfenyegetésekre, illetve az adathalászatra vagy a pszichológiai manipulációs technikákra. Ezen túlmenően az említett szervezeteknek értékelniük kell saját kiberbiztonsági képességeiket, és adott esetben törekedniük kell a kiberbiztonságot erősítő technológiák, például a mesterséges intelligencia vagy a gépi tanulásra épülő rendszerek integrálására képességeik, valamint a hálózati és információs rendszerek biztonságának fokozása érdekében.

(90) Az ellátási lánc kulcsfontosságú kockázatainak további kezelése és az ezen irányelv hatálya alá tartozó ágazatokban működő alapvető és fontos szervezetek számára az ellátási lánccal és a szállítóval kapcsolatos kockázatok megfelelő kezelésének elősegítése érdekében az együttműködési csoportnak a Bizottsággal és az ENISA-val együttműködve, és adott esetben az érintett érdekelt felekkel, többek között az ágazati szereplőkkel folytatott konzultációt követően összehangolt biztonsági kockázatértékeléseket kell végeznie a kritikus ellátási láncokra vonatkozóan, az (EU) 2019/534 bizottsági ajánlást ([19]) követően az 5G hálózatok esetében már megtettek szerint, annak meghatározása céljából, hogy az egyes ágazatokban melyek a kritikus IKT-szolgáltatások, -rendszerek vagy -termékek, a releváns fenyegetések és a sérülékenységek. Ezeknek az összehangolt biztonsági kockázatértékeléseknek azonosítaniuk kell a kritikus függőségekkel, az esetleges egyedi hibapontokkal, a fenyegetésekkel, a sérülékenységekkel és az ellátási lánchoz kapcsolódó egyéb kockázatokkal szembeni intézkedéseket, kockázatcsökkentési terveket és bevált gyakorlatokat, és fel kell tárniuk, hogy miként lehetne még inkább ösztönözni az alapvető és fontos szervezetek általi szélesebb körű elfogadásukat. A potenciális nem technikai kockázati tényezők – például valamely harmadik ország által beszállítókra és szolgáltatásnyújtókra gyakorolt indokolatlan befolyás, különösen alternatív irányítási modellek esetében – közé tartoznak a rejtett sérülékenységek vagy „hátsó ajtók”, valamint az ellátás esetleges rendszerszintű zavarai, különösen technológiai bezáródás („lock-in”) vagy a szolgáltatóktól való függés esetén.

(91) A kritikus ellátási láncokra vonatkozó összehangolt biztonsági kockázatértékeléseknek az érintett ágazat sajátosságaira figyelemmel figyelembe kell venniük a műszaki és adott esetben a nem technikai tényezőket, ideértve az (EU) 2019/534 ajánlásban, az 5G hálózatok kiberbiztonságának uniós összehangolt kockázatértékelése során és az együttműködési csoport által elfogadott 5G kiberbiztonsági uniós eszköztárban meghatározottakat is. Az összehangolt biztonsági kockázatértékelés alá eső ellátási láncok azonosításához a következő kritériumokat kell figyelembe venni: i. az alapvető és fontos szervezetek mennyiben használnak bizonyos kritikus IKT-szolgáltatásokat, -rendszereket vagy -termékeket, és mennyiben támaszkodnak azokra; ii. a konkrét kritikus IKT-szolgáltatások, -rendszerek vagy -termékek relevanciája a kritikus vagy érzékeny funkciók ellátása tekintetében, ideértve a személyes adatok kezelését is; iii. alternatív IKT-szolgáltatások, -rendszerek vagy -termékek elérhetősége; iv. az IKT-szolgáltatások, -rendszerek vagy -termékek teljes ellátási láncának rezilienciája teljes életciklusuk során a zavaró eseményekkel szemben és v. a megjelenő IKT-szolgáltatások, -rendszerek vagy -termékek esetében azok jövőbeli jelentősége a szervezetek tevékenysége szempontjából. Ezenkívül különös hangsúlyt kell fektetni azokra az IKT-szolgáltatásokra, -rendszerekre és -termékekre, amelyekre harmadik országok egyedi követelményei vonatkoznak.

(92) A nyilvános elektronikus hírközlő hálózatok vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatások szolgáltatóira, valamint a bizalmi szolgáltatókra a hálózati és információs rendszereik biztonságával kapcsolatban előírt kötelezettségek észszerűsítése, valamint annak lehetővé tétele érdekében, hogy az említett szervezetek és az (EU) 2018/1972 európai parlamenti és tanácsi irányelv ([20]), illetve a 910/2014/EU rendelet szerinti illetékes hatóságok kiaknázhassák az ezen irányelv által létrehozott jogi keret előnyeit (ideértve az események kezeléséért felelős CSIRT kijelölését, valamint az érintett illetékes hatóságok részvételét az együttműködési csoport és a CSIRT-hálózat tevékenységeiben), ezeknek a szervezeteknek ezen irányelv hatálya alá kell tartozniuk. A 910/2014/EU rendelet és az (EU) 2018/1972 irányelv megfelelő, az említett típusú szervezetekre vonatkozó biztonsági és bejelentési követelmények előírásával kapcsolatos rendelkezéseit ezért el kell hagyni. Az ezen irányelvben a jelentési kötelezettségekre vonatkozóan megállapított szabályok nem érinthetik az (EU) 2016/679 rendeletet és a 2002/58/EK irányelvet.

(93) Az ezen irányelvben megállapított kiberbiztonsági kötelezettségeket úgy kell tekinteni, mint amelyek kiegészítik a 910/2014/EU rendeletben a bizalmi szolgáltatókra vonatkozóan előírt követelményeket. A bizalmi szolgáltatók számára elő kell írni, hogy tegyenek meg minden megfelelő és arányos intézkedést a szolgáltatásaikat fenyegető – többek között a fogyasztókkal és a szolgáltatást igénybe vevő harmadik felekkel kapcsolatos – kockázatok kezelésére, valamint hogy jelentsék be az ezen irányelv szerinti eseményeket. Ezeknek a kiberbiztonsági és bejelentési kötelezettségeknek ki kell terjedniük a nyújtott szolgáltatások fizikai védelmére is. A 910/2014/EU rendelet 24. cikkében a minősített bizalmi szolgáltatókra vonatkozóan meghatározott követelmények továbbra is alkalmazandók.

([19]) A Bizottság (EU) 2019/534 ajánlása (2019. március 26.) az 5G hálózatok kiberbiztonságáról (HL L 88., 2019.3.29., 42. o.).

([20]) Az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról (HL L 321., 2018.12.17., 36. o.).

(94) A tagállamok a bizalmi szolgáltatásokért felelős illetékes hatóságok szerepét a 910/2014/EU rendelet szerinti felügyeleti szervekre ruházhatják annak érdekében, hogy biztosítsák a jelenlegi gyakorlatok folytatását és biztosítsák az említett rendelet alkalmazása során szerzett ismeretek és tapasztalatok hasznosítását. Ilyen esetben az ezen irányelv szerinti illetékes hatóságoknak szorosan és kellő időben együtt kell működniük az említett felügyeleti szervekkel azáltal, hogy megosztják egymással a releváns információkat annak érdekében, hogy biztosítsák a bizalmi szolgáltatók hatékony felügyeletét és az ezen irányelvben, valamint 910/2014/EU rendeletben megállapított követelményeknek való megfelelésüket. Adott esetben a CSIRT-nek vagy az ezen irányelv szerinti illetékes hatóságnak haladéktalanul tájékoztatnia kell a 910/2014/EU rendelet szerinti felügyeleti szervet minden olyan bejelentett jelentős kiberfenyegetésről vagy eseményről, amely a bizalmi szolgáltatásokat érinti, valamint ezen irányelvnek valamely bizalmi szolgáltató általi bármely megsértéséről. A jelentéstétel céljából a tagállamok adott esetben igénybe vehetik az események mind a 910/2014/EU rendelet szerinti felügyeleti szervnek, mind a CSIRT-nek vagy az ezen irányelv szerinti illetékes hatóságnak történő közös és automatikus bejelentésére létrehozott egyedüli kapcsolattartó pontot.

(95) Adott esetben és a szükségtelen zavarok elkerülése érdekében ezen irányelv átültetése során figyelembe kell venni az (EU) 2018/1972 irányelv 40. és 41. cikkében meghatározott biztonsági intézkedésekre vonatkozó szabályok átültetésére elfogadott, meglévő nemzeti iránymutatásokat, ezáltal építve az (EU) 2018/1972 irányelv alapján a biztonsági intézkedésekkel és az események bejelentésével kapcsolatos, már megszerzett ismeretekre és készségekre. Az ENISA emellett a harmonizáció és az átmenet megkönnyítése, valamint a fennakadások minimálisra csökkentése érdekében iránymutatásokat dolgozhat ki a nyilvános elektronikus hírközlő hálózatok szolgáltatóira és a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatókra vonatkozó biztonsági és jelentéstételi kötelezettségekre vonatkozóan. A tagállamok az elektronikus hírközlésért felelős illetékes hatóságok szerepét az (EU) 2018/1972 irányelv szerinti nemzeti szabályozó hatóságokra bízhatják annak érdekében, hogy biztosítsák a jelenlegi gyakorlatok folytatását és biztosítsák az említett irányelv alkalmazása során szerzett ismeretek és tapasztalatok hasznosítását.

(96) Az (EU) 2018/1972 irányelvben meghatározott számfüggetlen személyközi hírközlési szolgáltatások növekvő jelentőségére tekintettel biztosítani kell, hogy az említett szolgáltatások sajátos jellegére és gazdasági jelentőségére figyelemmel azok megfeleljenek célszerű biztonsági követelményeknek is. A támadási felület folyamatos bővülésével a számfüggetlen személyközi hírközlési szolgáltatások, például az üzenetküldő szolgáltatások egyre elterjedtebb támadási vektorokká válnak. A rosszindulatú elkövetők platformokat használnak arra, hogy kommunikáljanak az áldozatokkal, és az áldozatokat a feltört honlapokra csábítsák, ezáltal növelve a személyes adatok felhasználását, valamint ahhoz kapcsolódóan a hálózati és információs rendszerek biztonságát érintő események valószínűségét. A számfüggetlen személyközi hírközlési szolgáltatásokat nyújtó szolgáltatóknak biztosítaniuk kell, hogy a hálózati és információs rendszerek biztonsága megfeleljen a lehetséges kockázatoknak. Tekintettel arra, hogy a számfüggetlen személyközi hírközlési szolgáltatások szolgáltatói általában nem gyakorolnak tényleges ellenőrzést a hálózatokon keresztüli jelátvitel felett, az említett szolgáltatásokat érintő kockázatok mértéke bizonyos szempontból alacsonyabbnak tekinthető, mint a hagyományos elektronikus hírközlési szolgáltatások esetében. Ugyanez vonatkozik az (EU) 2018/1972 irányelvben meghatározott személyközi hírközlési szolgáltatásokra, amelyek számokat használnak, és amelyek nem gyakorolnak tényleges ellenőrzést a jelátvitel felett.

(97) A belső piac minden eddiginél jobban támaszkodik az internet működésére. Majdnem minden alapvető és fontos szervezet szolgáltatásai az interneten keresztül nyújtott szolgáltatásoktól függenek. Az alapvető és fontos szervezetek által nyújtott szolgáltatások zavartalanságának biztosítása érdekében fontos, hogy a nyilvános elektronikus hírközlő hálózatok valamennyi szolgáltatója megfelelő kiberbiztonsági kockázatkezelési intézkedésekkel rendelkezzen, és jelentse az ezekkel kapcsolatos jelentős eseményeket. A tagállamoknak biztosítaniuk kell a nyilvános elektronikus hírközlő hálózatok biztonságának fenntartását, valamint alapvető fontosságú biztonsági érdekeik védelmét a szabotázstól és a kémkedéstől. Mivel a nemzetközi konnektivitás fokozza és felgyorsítja az Unió és gazdaságának versenyképes digitalizációját, a tenger alatti kommunikációs kábeleket érintő eseményeket jelenteni kell a CSIRT-nek vagy adott esetben az illetékes hatóságnak. A tagállamok nemzeti kiberbiztonsági stratégiájának adott esetben figyelembe kell vennie a tenger alatti kommunikációs kábelek kiberbiztonságát, és a legmagasabb szintű védelem biztosítása érdekében tartalmaznia kell a potenciális kiberbiztonsági kockázatok feltérképezését és mérséklési intézkedéseket.

(98) A nyilvános elektronikus hírközlő hálózatok és a nyilvánosan elérhető elektronikus hírközlési szolgáltatások biztonságának védelme érdekében elő kell mozdítani a titkosítási technológiák alkalmazását, különösen a végponttól végpontig terjedő titkosítást, valamint az olyan adatközpontú biztonsági koncepciókat, mint a feltérképezés, a szegmentálás, a címkézés, a hozzáférési politika és a hozzáférés-kezelés, valamint az automatizált hozzáférés-megadás. Szükség esetén a titkosítás, különösen a végponttól végpontig terjedő titkosítás használatát kötelezővé kell tenni a nyilvános elektronikus hírközlő hálózatok szolgáltatói és a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók számára, az alapértelmezett és beépített biztonság és adatvédelem elveivel összhangban, ezen irányelv alkalmazásában. A végponttól végpontig terjedő titkosítás használatát össze kell egyeztetni a tagállamok azon hatáskörével, hogy biztosítsák alapvető biztonsági érdekeik és közbiztonságuk védelmét, valamint lehetővé tegyék a bűncselekmények megelőzését, kivizsgálását, felderítését és a büntetőeljárás alá vonását az uniós joggal összhangban. Ez azonban nem gyengítheti a végponttól végpontig terjedő titkosítást, amely az adatok és a magánélet hatékony védelme és a kommunikáció biztonsága szempontjából kritikus technológia.

(99) A nyilvános elektronikus hírközlő hálózatok és a nyilvánosan elérhető elektronikus hírközlési szolgáltatások biztonságának védelme, valamint az azokkal való visszaélés és manipuláció megelőzése érdekében elő kell mozdítani a biztonságos útválasztási szabványok alkalmazását annak érdekében, hogy az internetszolgáltatók teljes ökoszisztémájában biztosítani lehessen az útválasztási funkciók integritását és megbízhatóságát.

(100) Az internet funkcionalitásának és integritásának megőrzése, valamint a DNS biztonságának és rezilienciájának előmozdítása érdekében ösztönözni kell az érdekelt feleket, köztük az uniós magánszektorbeli szervezeteket, a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtóit, különösen az internet-hozzáférési szolgáltatókat és az online keresőprogram-szolgáltatókat, hogy fogadjanak el stratégiát a DNS címfeloldás diverzifikálására. A tagállamoknak ösztönözniük kell továbbá egy nyilvános és biztonságos európai DNS-címfeloldási szolgáltatás kifejlesztését és használatát.

(101) Ez az irányelv többlépcsős megközelítést állapít meg a jelentős események bejelentésével kapcsolatban annak érdekében, hogy megtalálja a megfelelő egyensúlyt egyrészt a gyors bejelentések között, amelyek segítenek enyhíteni a jelentős események potenciális terjedését, és lehetővé teszik az alapvető és fontos szervezetek számára, hogy segítségnyújtást kérjenek, másrészt pedig az olyan mélyreható jelentés érdekében, amely értékes tanulságokat von le az egyes eseményekből, és idővel javítja az egyes szervezetek és teljes ágazatok kiberrezilienciáját. E tekintetben ezen irányelvnek ki kell terjednie azon események bejelentésére is, amelyek az érintett szervezet által elvégzett első értékelés alapján jelentős működési zavarokhoz vagy pénzügyi veszteséghez vezethetnek az adott szervezet számára, vagy jelentős vagyoni vagy nem vagyoni kár okozásával hátrányosan érinthetnek más természetes vagy jogi személyeket. Ennek az első értékelésnek figyelembe kell vennie többek között az érintett hálózati és információs rendszereket és különösen fontosságukat a szervezet szolgáltatásainak nyújtásában, a kiberfenyegetés súlyosságát és műszaki jellemzőit, minden kihasznált mögöttes sérülékenységet, valamint a szervezet hasonló eseményekkel kapcsolatos tapasztalatait. Annak meghatározásában, hogy a szolgáltatás működési zavara súlyos-e, fontos szerepet játszhatnak olyan mutatók, mint a szolgáltatás működésére gyakorolt hatás mértéke, az esemény időtartama vagy a szolgáltatások érintett igénybe vevőinek száma.

(102) Az alapvető és fontos szervezetek számára elő kell írni, hogy amennyiben jelentős eseményről szereznek tudomást, indokolatlan késedelem nélkül és minden esetben 24 órán belül nyújtsanak be egy első bejelentést. Ezt az első bejelentést eseménybejelentésnek kell követnie. Az érintett szervezeteknek indokolatlan késedelem nélkül, és minden esetben a jelentős eseményről való tudomásszerzéstől számított 72 órán belül eseménybejelentést kell benyújtaniuk, különösen azzal a céllal, hogy frissítsék az első bejelentés keretében benyújtott információkat, és közöljék a jelentős esemény első értékelését, beleértve annak súlyosságát és hatását, valamint – amennyiben rendelkezésre állnak – a fertőzöttségi mutatókat. Legkésőbb az eseménybejelentéstől számított egy hónapon belül zárójelentést kell benyújtani. Az első bejelentésnek csak azokat az információkat kell tartalmaznia, amelyek szükségesek ahhoz, hogy a CSIRT-ek vagy adott esetben az illetékes hatóságok értesüljenek a jelentős eseményről, és lehetővé tegyék az érintett szervezet számára, hogy szükség esetén segítséget kérjen. Ennek az első bejelentésnek adott esetben jeleznie kell, hogy feltételezhető-e, hogy a jelentős eseményt jogellenes vagy rosszhiszemű cselekmények okozták, és hogy valószínűsíthető-e, hogy az esemény határokon átnyúló hatásokkal jár. A tagállamoknak gondoskodniuk kell arról, hogy az említett első bejelentés vagy az azt követő eseménybejelentés benyújtásának kötelezettsége ne vonja el a bejelentő szervezet erőforrásait az esemény kezelésével kapcsolatos tevékenységektől, amelyeket kiemelten kell kezelni annak megelőzése érdekében, hogy az eseménybejelentési

kötelezettségek erőforrásokat vonjanak el a jelentős események kezelésétől, vagy más módon veszélybe sodorják a szervezet e tekintetben tett erőfeszítéseit. Abban az esetben, ha az esemény a zárójelentés benyújtásának időpontjában folyamatban van, a tagállamoknak biztosítaniuk kell, hogy az érintett szervezetek az adott időpontban az addig elért eredményekről szóló jelentést, a jelentős esemény általuk való kezelését követő egy hónapon belül pedig zárójelentést nyújtsanak be.

(103) Adott esetben az alapvető és fontos szervezeteknek indokolatlan késedelem nélkül közölniük kell szolgáltatásuk igénybe vevőivel minden olyan intézkedést vagy fenyegetést orvosló lehetőséget, amelyet a jelentős kiberfenyegetésből eredő kockázatok mérséklése érdekében hozhatnak. Az említett szervezeteknek adott esetben és különösen akkor, ha a jelentős kiberfenyegetés valószínűsíthetően bekövetkezik, magáról a fenyegetésről is tájékoztatniuk kell a szolgáltatás igénybe vevőit. A szolgáltatás említett igénybe vevői jelentős kiberfenyegetésekről történő tájékoztatásának követelményét a legnagyobb gondosság elve alapján kell teljesíteni, de az nem mentesítheti az említett szervezeteket azon kötelezettség alól, hogy saját költségükre megfelelő és azonnali intézkedéseket hozzanak az ilyen fenyegetések megelőzésére vagy elhárítására, valamint a szolgáltatás normál biztonsági szintjének helyreállítására. A jelentős kiberfenyegetésekkel kapcsolatos említett információkat a szolgáltatást igénybe vevőknek ingyenesen kell megkapniuk, és azokat könnyen érthető módon kell megfogalmazni.

(104) A nyilvános elektronikus hírközlő hálózatok szolgáltatóinak vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatóknak beépített és alapértelmezett biztonságot kell alkalmazniuk, és tájékoztatniuk kell a szolgáltatást igénybe vevőket a jelentős kiberfenyegetésekről, valamint azokról az intézkedésekről, amelyeket megtehetnek az eszközeik és a kommunikáció biztonságának védelme érdekében, például bizonyos típusú szoftverek vagy titkosítási technológiák használata révén.

(105) A kiberfenyegetések proaktív megközelítése a kiberbiztonsági kockázatok kezelését célzó intézkedések alapvető eleme, amely várhatóan lehetővé fogja tenni az illetékes hatóságok számára, hogy hatékonyan megakadályozzák, hogy a kiberfenyegetések esetlegesen jelentős vagyoni vagy nem vagyoni kárt okozó biztonsági eseményekké váljanak. E célból kulcsfontosságú a kiberbiztonsági fenyegetések bejelentése. Ennek érdekében a szervezetek számára javasolt, hogy önkéntes alapon tegyenek jelentést a kiberbiztonsági fenyegetésekről.

(106) Az ezen irányelvben előírt információk bejelentésének egyszerűsítése, valamint a szervezetekre háruló adminisztratív terhek csökkentése érdekében a tagállamoknak a bejelentendő releváns információk benyújtása céljából gondoskodniuk kell technikai eszközökről, például egyedüli kapcsolattartó pontokról, automatizált rendszerekről, online űrlapokról, felhasználóbarát interfészekről, sablonokról, kifejezetten a szervezetek használatára létrehozott platformokról, függetlenül attól, hogy a szervezetek ezen irányelv hatálya alá tartoznak-e vagy sem. Az ezen irányelv végrehajtását – különösen az (EU) 2021/694 európai parlamenti és tanácsi rendelettel ([21]) létrehozott Digitális Európa program keretében – támogató uniós finanszírozás magában foglalhatja az egyedüli kapcsolattartó pontok támogatását is. Emellett az alapvető és fontos szervezetek gyakran vannak olyan helyzetben, amikor egy adott eseményről – jellemzői miatt – különféle jogi eszközökben szereplő bejelentési kötelezettségek eredményeként különböző hatóságoknak kell jelentést tenniük. Az említett esetek további adminisztratív terhet jelentenek, és bizonytalansághoz vezethetnek az említett bejelentések formátumát és eljárásait illetően is. Egyedüli kapcsolattartó pont létrehozása esetén a tagállamok számára javasolt az is, hogy ezt az egyedüli kapcsolattartó pontot vegyék igénybe a biztonsági események más uniós jogszabályok, például az (EU) 2016/679 rendelet és a 2002/58/EK irányelv által előírt bejelentésére is. Az említett egyedüli kapcsolattartó pontnak a biztonsági események (EU) 2016/679 rendelet és 2002/58/EK irányelv szerinti bejelentésére történő felhasználása nem érintheti az (EU) 2016/679 rendelet és a 2002/58/EK irányelv rendelkezéseinek – különösen az azokban említett hatóságok függetlenségére vonatkozó rendelkezések – alkalmazását. Az ENISA-nak az együttműködési csoporttal együttműködve közös bejelentési sablonokat kell kidolgoznia az uniós jog alapján bejelentendő információk egyszerűsítésére és összehangolására, valamint a bejelentő szervezetekre nehezedő teher csökkentésére irányuló iránymutatások révén.

(107) Ha felmerül a gyanú, hogy egy esemény az uniós vagy a nemzeti jog szerint súlyos bűncselekményekhez kapcsolódik, a tagállamoknak az uniós joggal összhangban alkalmazandó büntetőeljárási szabályok alapján ösztönözniük kell az alapvető és fontos szervezeteket a vélhetően súlyos bűncselekménynek minősülő események illetékes bűnüldöző hatóságoknak történő bejelentésére. Adott esetben és az Europolra irányadó, a személyes adatok védelmére vonatkozó szabályok sérelme nélkül kívánatos, hogy a Kiberbűnözés Elleni Európai Központ (EC3) és az ENISA megkönnyítse a koordinációt a különböző tagállamok illetékes hatóságai és bűnüldöző hatóságai között.

([21]) Az Európai Parlament és a Tanács (EU) 2021/694 rendelete (2021. április 29.) a Digitális Európa program létrehozásáról és az (EU) 2015/2240 határozat hatályon kívül helyezéséről (HL L 166., 2021.5.11., 1. o.).

(108) Az események következtében sok esetben személyes adatok kerülnek veszélybe. Ebben az összefüggésben az illetékes hatóságoknak minden releváns kérdésben együtt kell működniük és információt kell cserélniük az (EU) 2016/679 rendeletben és a 2002/58/EK irányelvben említett hatóságokkal.

(109) A doménnév-nyilvántartási adatok (WHOIS-adatok) pontos és teljes adatbázisainak gondozása és az említett adatokhoz való jogszerű hozzáférés biztosítása elengedhetetlen a DNS biztonságának, stabilitásának és rezilienciájának biztosításához, ami viszont hozzájárul az Unió egészére kiterjedő, egységesen magas szintű kiberbiztonsághoz. E konkrét célból a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek számára elő kell írni az e cél eléréséhez szükséges egyes adatok kezelését. Ennek az adatkezelésnek az (EU) 2016/679 rendelet 6. cikke (1) bekezdésének c) pontja értelmében vett jogi kötelezettségnek kell minősülnie. E kötelezettség nem érinti a doménnév-nyilvántartási adatok más célból, például más uniós vagy nemzeti jogban meghatározott szerződéses megállapodások vagy jogi követelmények alapján történő gyűjtésének lehetőségét. E kötelezettség célja a nyilvántartási adatok teljes és pontos voltának biztosítása, és nem eredményezheti ugyanazon adatok többszöri gyűjtését. A legfelső szintű doménnév-nyilvántartóknak és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteknek együtt kell működniük egymással az e feladattal kapcsolatos átfedések elkerülése érdekében.

(110) A doménnév-nyilvántartási adatok jogosult hozzáférés-igénylők számára való elérhetősége és időben történő hozzáférhetősége alapvető fontosságú a DNS-sel való visszaélések megelőzése és leküzdése, valamint az események megelőzése, észlelése és az azokra való reagálás szempontjából. Jogosult hozzáférés-igénylőnek tekintendő minden olyan természetes vagy jogi személy, aki vagy amely az uniós vagy a nemzeti jog alapján kérelmet nyújt be. Közéjük tartozhatnak az ezen irányelv alapján illetékes hatóságok, valamint a bűncselekmények megelőzése, kivizsgálása, felderítése vagy büntetőeljárás alá vonása céljából az uniós vagy nemzeti jog alapján illetékes hatóságok, valamint a CERT-ek vagy a CSIRT-ek. A legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek számára elő kell írni, hogy az uniós és nemzeti joggal összhangban tegyék lehetővé a jogosult hozzáférés-igénylők számára a jogszerű hozzáférést a hozzáférés iránti kérelemhez szükséges meghatározott doménnév-nyilvántartási adatokhoz. A jogszerű hozzáférés-igénylők kérelméhez indokolást kell csatolni, amely lehetővé teszi az adatokhoz való hozzáférés szükségességének értékelését.

(111) A pontos és teljes doménnév-nyilvántartási adatok rendelkezésre állásának biztosítása érdekében a legfelső szintű doménnév-nyilvántartóknak és a doménnév-nyilvántartási szolgáltatást nyújtó szervezeteknek össze kell gyűjteniük a doménnevek nyilvántartási adatait, és garantálniuk kell azok integritását és rendelkezésre állását. Különösen a legfelső szintű doménnév-nyilvántartóknak és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteknek szabályzatokat és eljárásokat kell kidolgozniuk a pontos és teljes doménnév-nyilvántartási adatok összegyűjtése és vezetése, valamint az uniós adatvédelmi jogszabályokkal összhangban a pontatlan nyilvántartási adatok megelőzése és kijavítása céljából. E szabályzatoknak és eljárásoknak a lehető legnagyobb mértékben figyelembe kell venniük a több érdekelt felet tömörítő irányítási struktúrák által nemzetközi szinten kidolgozott normákat. A legfelső szintű doménnév-nyilvántartóknak és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteknek arányos eljárásokat kell elfogadniuk és végrehajtaniuk a doménnév-nyilvántartási adatok ellenőrzése céljából. Ezen eljárásoknak tükrözniük kell az ágazatban alkalmazott bevált gyakorlatokat és – amennyire lehetséges – az elektronikus azonosítás terén elért eredményeket. Az ellenőrzési eljárások közé tartozhatnak például a nyilvántartásba vételkor végzett előzetes ellenőrzések és a nyilvántartásba vételt követően végzett utólagos ellenőrzések. A legfelső szintű doménnév-nyilvántartóknak és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteknek különösen a bejegyzést igénylő legalább egy kapcsolatfelvételi módját ellenőrizniük kell.

(112) A legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek számára elő kell írni, hogy tegyék nyilvánosan hozzáférhetővé az uniós adatvédelmi jog hatálya alá nem tartozó doménnév-nyilvántartási adatokat, például – az (EU) 2016/679 rendelet preambulumával összhangban – a jogi személyeket érintő adatokat. Jogi személyek esetében a legfelső szintű doménnév-nyilvántartóknak és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteknek legalább a bejegyzést igénylő nevét és kapcsolattartási telefonszámát nyilvánosan hozzáférhetővé kell tenniük. A kapcsolattartási e-mail-címet is közzé kell tenni, feltéve, hogy az nem tartalmaz személyes adatokat, így például az e-mail aliasok vagy a funkcionális fiókok esetében. A legfelső szintű doménnév-nyilvántartóknak és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteknek lehetővé kell tenniük a jogosult hozzáférés-igénylők számára, hogy jogszerű módon, az uniós adatvédelmi joggal összhangban hozzáférjenek a természetes személyekre vonatkozó meghatározott doménnév-nyilvántartási adatokhoz is. A tagállamoknak elő kell írniuk a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek számára, hogy indokolatlan késedelem nélkül reagáljanak a jogosult hozzáférés-igénylők doménnév-nyilvántartási adatok nyilvánosságra hozatalára irányuló kérelmeire. A legfelső szintű doménnév-nyilvántartóknak és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteknek szabályzatokat és eljárásokat kell kidolgozniuk a nyilvántartási adatok közzétételére és nyilvánosságra hozatalára vonatkozóan,

beleértve a szolgáltatási szintre vonatkozó megállapodásokat is, a jogosult hozzáférés-igénylők kérelmeinek kezelése céljából. E szabályzatoknak és eljárásoknak a lehető legnagyobb mértékben figyelembe kell venniük minden iránymutatást és a több érdekelt felet tömörítő irányítási struktúrák által nemzetközi szinten kidolgozott normákat. A hozzáférési eljárás magában foglalhatja egy interfész, portál vagy más technikai eszközök használatát, hogy hatékony rendszert lehessen biztosítani a nyilvántartási adatok lekérésére és elérésére. A Bizottság a belső piacon a harmonizált gyakorlatok előmozdítása érdekében – az Európai Adatvédelmi Testület hatáskörének sérelme nélkül – iránymutatásokat nyújthat az említett eljárásokról, amelyek a lehető legnagyobb mértékben figyelembe veszik a több érdekelt felet tömörítő irányítási struktúrák által nemzetközi szinten kidolgozott normákat. A tagállamoknak biztosítaniuk kell, hogy a személyes és nem személyes doménnév-nyilvántartási adatokhoz való bármilyen típusú hozzáférés ingyenes legyen.

(113) Az ezen irányelv hatálya alá tartozó szervezeteket a letelepedésük szerinti tagállam joghatósága alá tartozónak kell tekinteni. A nyilvános elektronikus hírközlő hálózatok szolgáltatóit vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatókat azonban azon tagállam joghatósága alá tartozónak kell tekinteni, ahol szolgáltatásaikat nyújtják. A DNS-szolgáltatókat, a legfelső szintű doménnév-nyilvántartókat és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteket, a felhőszolgáltatókat, az adatközpont-szolgáltatókat, a tartalomszolgáltató hálózati szolgáltatókat, az irányított szolgáltatókat és az irányított biztonsági szolgáltatókat, valamint az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatóit azon tagállam joghatósága alá tartozónak kell tekinteni, ahol Unión belüli üzleti tevékenységük fő helye található. A közigazgatási szervezetek az őket létrehozó tagállam joghatósága alá tartozónak kell tekinteni. Ha a szervezet több tagállamban nyújt szolgáltatásokat vagy több tagállamban is letelepedett, annak külön és egyidejűleg minden érintett tagállam joghatósága alá kell tartoznia. E tagállamok illetékes hatóságainak együtt kell működniük, kölcsönös segítséget kell nyújtaniuk egymásnak, és adott esetben közös felügyeleti intézkedéseket kell végrehajtaniuk. Joghatóságuk gyakorlása során a tagállamok – a ne bis in idem elvének megfelelően – nem írhatnak elő egynél többször végrehajtási intézkedéseket vagy szankciókat ugyanazon magatartásért.

(114) A DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók és az irányított biztonsági szolgáltatók, valamint az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatói szolgáltatásai és működése határokon átnyúló jellegének figyelembevétele érdekében e szervezetek felett csak egy tagállamnak lehet joghatósága. A joghatóságot annak a tagállamnak kell tulajdonítani, ahol az érintett szervezet Unión belüli üzleti tevékenységének fő helye található. A letelepedési kritérium ezen irányelv alkalmazásában a tevékenység állandó megállapodások útján történő tényleges gyakorlását jelenti. Ebben a tekintetben nem meghatározó tényező az említett megállapodások jogi formája, függetlenül attól, hogy fióktelepen vagy jogi személyiséggel rendelkező leányvállalaton keresztül kötötték-e azokat. E kritérium teljesülése nem függhet attól, hogy a hálózat és az információs rendszerek fizikailag egy adott helyen találhatók-e; az említett rendszerek jelenléte és használata önmagukban nem képezi az üzleti tevékenység említett fő helyét, ezért nem meghatározó kritériumok az üzleti tevékenység fő helyének meghatározásához. Az üzleti tevékenység fő helyének azt kell tekinteni, ahol az Unióban túlnyomórészt meghozzák a kiberbiztonsági kockázatkezelési intézkedésekkel kapcsolatos döntéseket. Ez általában megfelel a vállalatok uniós központi ügyvezetése helyének. Ha ilyen tagállam nem határozható meg, vagy az ilyen döntéseket nem az Unióban hozzák meg, akkor úgy kell tekinteni, hogy az üzleti tevékenység fő helye abban a tagállamban található, ahol a kiberbiztonsági műveleteket végzik. Ha ilyen tagállam nem határozható meg, akkor az üzleti tevékenység fő helyét abban a tagállamban levőnek kell tekinteni, ahol a szervezetnek az Unióban a legmagasabb munkavállalói létszámmal rendelkező telephelye található. Ha a szolgáltatásokat vállalkozások csoportja végzi, az irányító vállalkozás üzleti tevékenysége fő helyét a vállalkozáscsoport üzleti tevékenysége fő helyének kell tekinteni.

(115) Amennyiben egy nyilvános elektronikus hírközlő hálózatokat üzemeltető vagy nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltató kizárólag az internet-hozzáférési szolgáltatás részeként nyújt nyilvánosan elérhető rekurzív DNS-szolgáltatást, úgy kell tekinteni, hogy a szervezet valamennyi olyan tagállamnak a joghatósága alá tartozik, amelyben a szolgáltatásait nyújtja.

(116) Olyan esetekben, amikor az Unióban nem letelepedett DNS-szolgáltató, legfelső szintű doménnév-nyilvántartó és doménnév-nyilvántartási szolgáltatásokat nyújtó szervezet, felhőszolgáltató, adatközpont-szolgáltató, tartalomszolgáltató hálózati szolgáltató, irányított szolgáltató és irányított biztonsági szolgáltató, valamint online piactér, online keresőprogram vagy közösségimédia-szolgáltatási platform szolgáltatója az Unión belül kínál szolgáltatásokat, ki kell jelölnie egy Unión belüli képviselőt. Annak eldöntése érdekében, hogy az említett szervezet kínál-e szolgáltatásokat az Unión belül, meg kell győződni arról, hogy a szervezetnek szándékában áll-e szolgáltatásokat nyújtani személyek számára egy vagy több tagállamban. A szervezet vagy valamely közvetítő webhelyének, az e-mail-címnek és más elérhetőségeknek az Unióban való puszta elérhetősége, vagy a szervezet letelepedési helye szerinti harmadik országban általánosan használt nyelv használata önmagában nem elegendő információ az említett szándék megállapításához. Ha azonban például a szervezet olyan nyelvet vagy pénznemet használ, amely egy vagy több tagállamban is általánosan használatos, és így lehetőséget biztosít szolgáltatásoknak az említett nyelven történő megrendelésére, vagy unióbeli fogyasztókra vagy felhasználókra tesz utalást, az egyértelműen jelezheti, hogy a digitális szolgáltató szolgáltatásokat szándékozik kínálni az Unión belül. A képviselőnek a szervezet nevében kell eljárnia, és az illetékes hatóságok vagy a CSIRT-ek számára lehetővé kell tenni, hogy a képviselőhöz forduljanak. A szervezetnek írásban kifejezetten fel kell hatalmaznia a képviselőt arra, hogy a nevében eljárjon az ezen irányelvben megállapított kötelezettségei vonatkozásában, ideértve a biztonsági események bejelentését is.

(117) Annak érdekében, hogy biztosítsa az Unióban szolgáltatásokat nyújtó és ezen irányelv hatálya alá tartozó DNS-szolgáltatók, legfelső szintű doménnév-nyilvántartók és doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek, felhőszolgáltatók, adatközpont-szolgáltatók, tartalomszolgáltató hálózati szolgáltatók, irányított szolgáltatók és irányított biztonsági szolgáltatók, valamint az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatói világos áttekinthetőségét, az ENISA-nak a tagállamoktól – adott esetben a szervezetek számára a saját maguk bejegyeztetésére létrehozott nemzeti mechanizmusokon keresztül – kapott információk alapján nyilvántartást kell létrehoznia és vezetnie ezekről a szervezetekről. Az egyedüli kapcsolattartó pontoknak továbbítaniuk kell az ENISA-nak az információkat és azok változásait. Az említett nyilvántartásban feltüntetendő információk pontosságának és teljességének biztosítása céljából a tagállamok benyújthatják az ENISA számára a nemzeti nyilvántartásaikban e szervezetekre vonatkozóan rendelkezésre álló információkat. Az ENISA-nak és a tagállamoknak intézkedéseket kell hozniuk az ilyen nyilvántartások interoperabilitásának elősegítésére, biztosítva ugyanakkor a bizalmas vagy minősített adatok védelmét. Az ENISA-nak megfelelő információosztályozási és kezelési protokollokat kell létrehoznia a közzétett információk biztonságának és bizalmas jellegének biztosítása, valamint az ilyen információk elérésének, tárolásának és a szándékolt felhasználók számára történő továbbításának korlátozása érdekében.

(118) Amennyiben a nemzeti vagy az uniós joggal összhangban minősített információkat ezen irányelv alapján kicserélik, jelentik vagy más módon megosztják, a minősített információk kezelésére vonatkozó különös szabályokat alkalmazni kell. Emellett az ENISA-nak rendelkeznie kell az érzékeny és minősített adatok kezeléséhez szükséges infrastruktúrával, eljárásokkal és szabályokkal, az EU-minősített adatok védelmére vonatkozó biztonsági szabályokkal összhangban.

(119) A kiberfenyegetések bonyolultabbá és kifinomultabbá válásával e fenyegetések jó észlelése és a megelőzési intézkedések nagymértékben függenek a fenyegetésekre és sérülékenységekre vonatkozó információk szervezetek közötti rendszeres megosztásától. Az információmegosztás hozzájárul a kiberfenyegetésekkel kapcsolatos tudatosság erősítéséhez, ami viszont fokozza a szervezetek azon képességét, hogy megakadályozzák e fenyegetések eseményekké válását, és lehetővé teszi a szervezetek számára, hogy jobban visszaszorítsák az események hatásait, és hatékonyabbá tegyék a működés helyreállítását. Uniós szintű útmutatás hiányában, úgy tűnik, számos tényező gátolta az említett információmegosztást, különösen a verseny- és felelősségi szabályokkal való összeegyeztethetőség bizonytalansága.

(120) A tagállamoknak ösztönözniük és segíteniük kell a szervezeteket, hogy stratégiai, taktikai és operatív szinten együttesen hasznosítsák egyéni tudásukat és gyakorlati tapasztalataikat annak érdekében, hogy javítsák képességeiket az események megfelelő megelőzésére, felderítésére, az azokra való reagálásra, az azokat követő helyreállításra, és hatásaik enyhítésére. Ezért lehetővé kell tenni az önkéntes kiberbiztonsági információmegosztási megállapodások uniós szintű kialakulását. Ennek érdekében a tagállamoknak aktív segítséget és ösztönönzést kell nyújtaniuk az olyan szervezetek számára, mint például a kiberbiztonsági szolgáltatásokat és kutatásokat végző szervezetek, és az ezen irányelv hatálya alá nem tartozó érintett szervezetek számára, hogy részt vegyenek az említett kiberbiztonsági információmegosztási megállapodásokban. Ezeket a megállapodásokat az uniós versenyszabályokkal és az uniós adatvédelmi joggal teljes összhangban kell kialakítani.

(121) A személyes adatok kezelése – a hálózati és információs rendszerek biztonságának az alapvető és fontos szervezetek általi biztosítása céljából szükséges és arányos mértékben – jogszerűnek tekinthető azon az alapon, hogy az adatkezelés megfelel az adatkezelőre vonatkozó jogi kötelezettségnek, az (EU) 2016/679 rendelet 6. cikke (1) bekezdésének c) pontjában és 6. cikkének (3) bekezdésében foglalt követelményekkel összhangban. A személyes adatok kezelése az alapvető és fontos szervezetek, valamint az e szervezetek nevében eljáró, biztonsági technológiákat és szolgáltatásokat nyújtó szolgáltatók jogos érdekei miatt is szükséges lehet az (EU) 2016/679 rendelet 6. cikke (1) bekezdésének f) pontja értelmében, ideértve azt az esetet is, amikor az adatkezelés kiberbiztonsági információmegosztási megállapodásokhoz vagy a releváns információk ezen irányelvvel összhangban történő önkéntes bejelentéséhez szükséges. Az események megelőzésével, észlelésével, azonosításával, megfékezésével, elemzésével és az azokra való reagálással kapcsolatos intézkedések, a konkrét kiberfenyegetésekkel kapcsolatos tudatosság növelését célzó intézkedések, a sérülékenységek elhárításával és az összehangolt közzététellel kapcsolatos információmegosztás, valamint az ezekre az eseményekre, valamint a kiberfenyegetésekre és sérülékenységekre, a kompromisszummutatókra, taktikákra, technikákra és eljárásokra, kiberbiztonsági figyelmeztetésekre és konfigurációs eszközökre vonatkozó önkéntes információmegosztás szükségessé tehetik a személyes adatok bizonyos kategóriáinak, például IP-címeknek, egységes forrásazonosítóknak (URL-ek), doménneveknek, e-mail-címeknek, és – amennyiben személyes adatokat fednek fel – időbélyegzőknek a kezelését. A személyes adatok illetékes hatóságok, egyedüli kapcsolattartó pontok és CSIRT-ek általi kezelése az (EU) 2016/679 rendelet 6. cikke (1) bekezdésének c) vagy e) pontja és 6. cikkének (3) bekezdése értelmében jogi kötelezettségnek minősülhet, vagy közérdekűnek vagy szükségesnek tekinthető az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához vagy az említett rendelet 6. cikke (1) bekezdésének f) pontjában említett alapvető és fontos szervezetek jogos érdekének érvényesítéséhez. Ezen túlmenően a nemzeti jog megállapíthat olyan szabályokat, amelyek lehetővé teszik az illetékes hatóságok, az egyedüli kapcsolattartó pontok és a CSIRT-ek számára, hogy az alapvető és fontos szervezetek hálózati és információs rendszerei biztonságának biztosítása céljából szükséges és arányos mértékben az (EU) 2016/679 rendelet 9. cikkével összhangban kezeljék a személyes adatok különleges kategóriáit, különösen azáltal, hogy megfelelő és konkrét intézkedéseket írnak elő a természetes személyek alapvető jogainak és érdekeinek védelme érdekében, beleértve az ilyen adatok további felhasználására vonatkozó technikai korlátozásokat, valamint a legkorszerűbb biztonsági és adatvédelmi intézkedések alkalmazását, például az álnevesítést vagy titkosítást, amennyiben az anonimizálás jelentősen befolyásolhatja a kitűzött célt.

(122) A tényleges megfelelés biztosítását elősegítő felügyeleti hatáskörök és intézkedések megerősítése érdekében ennek az irányelvnek rendelkeznie kell azon felügyeleti intézkedések és eszközök minimumlistájáról, amelyek révén az illetékes hatóságok felügyelhetik az alapvető és a fontos szervezeteket. Ezen túlmenően ennek az irányelvnek eltérő felügyeleti rendszert kell meghatároznia az alapvető és a fontos szervezetek vonatkozásában annak érdekében, hogy biztosítsa a kötelezettségek méltányos egyensúlyát az említett szervezetek és az illetékes hatóságok számára. Ezért az alapvető szervezetekre teljes körű (előzetes és utólagos) felügyeleti rendszert kell alkalmazni, míg a fontos szervezetekre könnyített, csak utólagos felügyeleti rendszer alkalmazandó. Ezért a fontos szervezetek számára nem kell előírni a kiberbiztonsági kockázatkezelési intézkedéseknek való megfelelés szisztematikus dokumentálását, míg az illetékes hatóságoknak reaktív utólagos felügyeleti megközelítést kell alkalmazniuk, és ezért nem terheli azokat általános kötelezettség az említett szervezetek felügyeletére. A fontos szervezetek utólagos felügyeletét az illetékes hatóságok tudomására hozott olyan bizonyíték, jelzés vagy információ alapján lehet elindítani, amelyről e hatóságok úgy vélik, hogy ezen irányelv lehetséges megsértésére utal. Ilyen bizonyíték, jelzés vagy információ lehet például a más hatóságok, szervezetek, állampolgárok, a média vagy más források által az illetékes hatóságok rendelkezésére bocsátott információ, továbbá a nyilvánosan hozzáférhető információk, illetve az származhat az illetékes hatóságok által a feladataik ellátása során végzett egyéb tevékenységekből is.

(123) A felügyeleti feladatok illetékes hatóságok általi végrehajtása nem akadályozhatja szükségtelen módon az érintett szervezet üzleti tevékenységét. Alapvető szervezetekkel kapcsolatos felügyeleti feladataik – többek között helyszíni ellenőrzések és külső felügyelet elvégzése, ezen irányelv megsértésének kivizsgálása, biztonsági ellenőrzések vagy biztonsági átvilágítások lefolytatása – elvégzése során az illetékes hatóságoknak minimálisra kell korlátozniuk az érintett szervezet üzleti tevékenységére gyakorolt hatást.

(124) Az előzetes felügyelet végrehajtása során az illetékes hatóságok számára lehetővé kell tenni, hogy arányos módon döntsenek a rendelkezésükre álló felügyeleti intézkedések és eszközök alkalmazásának rangsorolásáról. Ez azt jelenti, hogy az illetékes hatóságok e rangsorolásról olyan felügyeleti módszerek alapján dönthetnek, amelyeknek kockázatalapú megközelítést kell követniük. Konkrétabban, ezek a módszerek tartalmazhatnak kritériumokat vagy referenciaértékeket az alapvető szervezetek kockázati kategóriákba sorolására és a megfelelő felügyeleti intézkedésekre, valamint kockázati kategóriánként ajánlott eszközökre, például a helyszíni ellenőrzések vagy célzott biztonsági ellenőrzések vagy biztonsági vizsgálatok használatára, gyakoriságára vagy típusára, a bekérendő információk típusára és ezen információk részletességének szintjére. Ezeket a felügyeleti módszereket

munkaprogramok is kísérhetik, továbbá rendszeresen értékelni kell és felül kell vizsgálni azokat, többek között olyan szempontok alapján, mint az erőforrások elosztása és a szükségletek. A közigazgatási szervek tekintetében a felügyeleti hatásköröket a nemzeti jogalkotási és intézményi keretekkel összhangban kell gyakorolni.

(125) Az illetékes hatóságoknak biztosítaniuk kell, hogy az alapvető és fontos szervezetekkel kapcsolatos felügyeleti feladataikat képzett szakemberek végezzék, akiknek rendelkezniük kell a szóban forgó feladatok elvégzéséhez szükséges készségekkel, különösen a helyszíni ellenőrzések és a külső felügyelet elvégzése tekintetében, beleértve az adatbázisok, a hardverek, a tűzfalak, a titkosítás és a hálózatok hiányosságainak azonosítását is. Ezeket az ellenőrzéseket és a felügyeletet objektív módon kell végrehajtani.

(126) Kellően indokolt esetekben, amikor az illetékes hatóság jelentős kiberfenyegetésről vagy közvetlen kockázatról szerez tudomást, lehetővé kell tenni számára, hogy azonnali végrehajtási határozatokat hozzon valamely biztonsági esemény megelőzése vagy az arra való reagálás céljából.

(127) A végrehajtás hatásossága érdekében meg kell határozni az ezen irányelvben előírt kiberbiztonsági kockázatkezelési intézkedések és jelentéstételi kötelezettségek megszegése esetén gyakorolható végrehajtási hatáskörök minimumlistáját, az említett végrehajtás vonatkozásában az egész Unióban egyértelmű és következetes keretet létrehozva. Megfelelő figyelmet kell fordítani ezen irányelv megsértésének jellegére, súlyosságára és időtartamára, az okozott vagyoni vagy nem vagyoni kárra, a jogsértés szándékos vagy gondatlan jellegére, az elszenvedett vagyoni vagy nem vagyoni kár megelőzésére vagy enyhítésére tett intézkedésekre, a felelősség mértékére vagy bármely releváns korábbi jogsértésre, az illetékes hatósággal való együttműködés mértékére és minden egyéb súlyosbító vagy enyhítő tényezőre. A végrehajtási intézkedéseknek – beleértve a közigazgatási bírságokat is – arányosaknak kell lenniük, és kiszabásukra megfelelő eljárási biztosítékoknak kell vonatkozniuk az uniós jog általános elveivel és az Európai Unió Alapjogi Chartájával (a továbbiakban: a Charta) összhangban, ideértve a hatékony bírói védelemhez, a jogszerű eljáráshoz, az ártatlanság vélelméhez és a védelemhez való jogot.

(128) Ez az irányelv nem írja elő a tagállamok számára, hogy a valamely szervezet ezen irányelvnek való megfelelésének biztosításáért felelős természetes személyek tekintetében büntetőjogi vagy polgári jogi felelősséget írjanak elő az ezen irányelv megsértése miatt harmadik felek által elszenvedett károkért.

(129) Az ezen irányelvben megállapított kötelezettségek hatékony végrehajtásának biztosítása érdekében minden illetékes hatóságnak rendelkeznie kell hatáskörrel közigazgatási bírság kiszabására vagy ilyen bírság kiszabásának kérelmezésére.

(130) Ha a közigazgatási bírságot olyan alapvető vagy fontos szervezetre szabják ki, amely vállalkozás, akkor a vállalkozás fogalmát e célból az EUMSZ 101. és 102. cikkében meghatározott vállalkozásokra vonatkozó szabályoknak megfelelően kell értelmezni. Amennyiben vállalkozásnak nem minősülő személyre szabnak ki közigazgatási bírságot, a bírság megfelelő összegének mérlegelésekor az illetékes hatóságnak figyelembe kell vennie a tagállam általános jövedelemszintjét, valamint a személy anyagi helyzetét. A tagállamok feladata annak meghatározása, hogy a közhatalmi szervekkel szemben alkalmazható legyen-e közigazgatási bírság, és ha igen, milyen mértékben. A közigazgatási bírság kiszabása nem érinti az illetékes hatóságok egyéb hatásköreinek alkalmazását vagy az ezen irányelvet átültető nemzeti szabályokban megállapított egyéb szankciók alkalmazását.

(131) A tagállamok számára lehetővé kell tenni az ezen irányelvet átültető nemzeti szabályok megsértése esetén alkalmazandó büntetőjogi szankciók szabályainak megállapítását. Az említett tagállami szabályok megsértésére vonatkozó büntetőjogi szankciók, illetve közigazgatási szankciók kiszabása azonban nem eredményezheti az Európai Unió Bíróságának értelmezése szerinti ne bis in idem elv megsértését.

(132) Ha ez az irányelv nem harmonizálja a közigazgatási szankciókat, vagy szükség esetén más esetekben, például ezen irányelv súlyos megsértése esetén, a tagállamoknak olyan rendszert kell bevezetniük, amely hatékony, arányos és visszatartó erejű szankciókat ír elő. E szankciók jellegét és azok büntetőjogi vagy közigazgatási természetét a nemzeti jogban kell meghatározni.

(133) Az ezen irányelv megsértése esetén alkalmazandó szankciók hatékonyságának és visszatartó erejének további erősítése érdekében az illetékes hatóságokat fel kell hatalmazni arra, hogy az alapvető szervezet által nyújtott összes releváns szolgáltatásra vagy azok egy részére vonatkozó tanúsítványt vagy engedélyt ideiglenesen felfüggesszék vagy kérelmezzék annak ideiglenes felfüggesztését, és kérelmezzék bármely, vezérigazgatói vagy jogi képviselői szinten eljáró természetes személy irányítási feladatok ellátásától való ideiglenes eltiltását. Az említett ideiglenes felfüggesztéseket és eltiltásokat csak a jogsértés súlyosságával arányosan lehet alkalmazni – tekintettel azok súlyosságára és a szervezetek tevékenységére, és végső soron a felhasználókra gyakorolt hatására –, figyelembe véve minden egyes eset sajátos körülményeit, beleértve a jogsértés szándékos vagy gondatlan jellegét, valamint a vagyoni és nem vagyoni károk megelőzése vagy enyhítése érdekében tett intézkedéseket. Ezeket az ideiglenes felfüggesztéseket és eltiltásokat csak végső megoldásként szabad alkalmazni, vagyis csak az ezen irányelvben megállapított egyéb vonatkozó végrehajtási intézkedések kimerítése után, és csak addig, amíg az érintett szervezet meghozza a szükséges intézkedéseket a hiányosságok orvoslására vagy az illetékes hatóság követelményeinek – amelyekkel kapcsolatban az ideiglenes felfüggesztéseket és eltiltásokat alkalmazták – való megfelelésre. Az említett ideiglenes felfüggesztések vagy tiltások kiszabására megfelelő eljárási biztosítékok vonatkoznak, az uniós jog általános elveivel és a Chartával összhangban, ideértve a tényleges jogorvoslathoz és a tisztességes eljáráshoz való jogot, az ártatlanság vélelmét és a védelemhez való jogot.

(134) Annak biztosítása érdekében, hogy a szervezetek megfeleljenek az ezen irányelvben megállapított kötelezettségeiknek, a tagállamoknak együtt kell működniük, és segíteniük kell egymást a felügyeleti és végrehajtási intézkedések tekintetében, különösen abban az esetben, ha valamely szervezet egynél több tagállamban nyújt szolgáltatásokat, vagy ha annak hálózati és információs rendszerei a szolgáltatásnyújtás helye szerinti tagállamtól eltérő tagállamban találhatók. A segítségnyújtás során a megkeresett illetékes hatóságnak a nemzeti jognak megfelelő felügyeleti vagy végrehajtási intézkedéseket kell hoznia. Az ezen irányelv szerinti kölcsönös segítségnyújtás zökkenőmentes működésének biztosítása érdekében az illetékes hatóságoknak az együttműködési csoportot kell fórumként felhasználniuk az ügyek és az egyedi segítségnyújtás iránti megkeresések megvitatására.

(135) A hatékony felügyelet és végrehajtás biztosítása érdekében – különösen a határokon átnyúló dimenzióval rendelkező helyzetekben – azon tagállamnak, amely kölcsönös segítségnyújtás iránti megkeresést kapott, a megkeresés alapján szükséges keretek között megfelelő felügyeleti és végrehajtási intézkedéseket kell hoznia az említett megkeresés alanyát képező szervezettel kapcsolatban, amely az említett tagállam területén szolgáltatásokat nyújt vagy hálózati és információs rendszerrel rendelkezik.

(136) Ennek az irányelvnek az (EU) 2016/679 rendelet értelmében meg kell határoznia az illetékes hatóságok és a felügyeleti hatóságok közötti együttműködési szabályokat az ezen irányelv személyes adatokkal kapcsolatos megsértésének kezelése érdekében.

(137) Ezen irányelv célja, hogy biztosítsa a kiberbiztonsági kockázatkezelési intézkedésekért és a jelentéstételi kötelezettségekért viselt magas szintű felelősséget az alapvető és fontos szervezetek szintjén. Ezen okok miatt az alapvető és fontos szervezetek vezető testületeinek jóvá kell hagyniuk a kiberbiztonsági kockázatkezelési intézkedéseket, és felügyelniük kell azok végrehajtását.

(138) A kiberbiztonság egységesen magas szintjének Unió-szerte történő biztosítása érdekében a Bizottságot fel kell hatalmazni arra, hogy az EUMSZ 290. cikkével összhangban jogi aktusokat fogadjon el ezen irányelv kiegészítése céljából, meghatározva, hogy az alapvető és fontos szervezetek mely kategóriái kötelesek bizonyos tanúsított IKT-termékeket, IKT-szolgáltatásokat és IKT-folyamatokat használni vagy tanúsítványt szerezni valamely európai kiberbiztonsági tanúsítási rendszer keretében. Különösen fontos, hogy a Bizottság az előkészítő munka során – többek között szakértői szinten – megfelelő konzultációkat folytasson, és a konzultációkra a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban ([22]) foglalt elvekkel összhangban kerüljön sor. Így különösen a felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlament és a Tanács a tagállamok szakértőivel egyidejűleg kap kézhez minden dokumentumot, és szakértőik rendszeresen részt vehetnek a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein.

([22]) HL L 123., 2016.5.12., 1. o.

(139) Ezen irányelv végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságot végrehajtási hatáskörökkel kell felruházni annak érdekében, hogy megállapítsa az együttműködési csoport működéséhez szükséges eljárási szabályokat, valamint a kiberbiztonsági kockázatkezelési intézkedésekhez kapcsolódó technikai, módszertani és ágazati követelményeket, és tovább pontosítsa az információk típusát, az események, kiberfenyegetések és majdnem bekövetkezett (near miss) események bejelentése, továbbá a jelentős kiberfenyegetésekre vonatkozó kommunikáció formátumát és eljárását, valamint azokat az eseteket, amelyekben valamely biztonsági esemény jelentősnek minősül. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek ([23]) megfelelően kell gyakorolni.

(140) A Bizottságnak az érdekelt felekkel folytatott konzultációt követően rendszeresen felül kell vizsgálnia ezt az irányelvet, különösen annak megállapítása céljából, hogy a társadalmi, politikai, technológiai vagy piaci feltételek változásai fényében helyénvaló-e módosításokat javasolni. E felülvizsgálatok részeként a Bizottságnak értékelnie kell, hogy az ezen irányelv mellékleteiben említett szervezetek mérete, ágazatai, alágazatai és típusai mennyire relevánsak a gazdaság és a társadalom működése szempontjából a kiberbiztonság tekintetében. A Bizottságnak többek között értékelnie kell, hogy az (EU) 2022/2065 európai parlamenti és tanácsi rendelet ([24]) 33. cikke értelmében online óriásplatformnak kijelölt, ezen irányelv hatálya alá tartozó szolgáltatók ezen irányelv értelmében azonosíthatók-e alapvető szervezetként.

(141) Ez az irányelv új feladatokat hoz létre az ENISA számára, ezáltal növelve szerepét, ami azt is eredményezheti, hogy az ENISA-nak a korábbinál magasabb szinten kell ellátnia az (EU) 2019/881 rendelet szerinti meglévő feladatait. Annak biztosítása érdekében, hogy az ENISA rendelkezzen a meglévő és új feladatai ellátásához szükséges pénzügyi és emberi erőforrásokkal, valamint hogy magasabb szinten végre tudja hajtani a megerősített szerepéből eredő feladatokat, költségvetését ennek megfelelően növelni kell. Ezen túlmenően az erőforrások hatékony felhasználásának biztosítása érdekében az ENISA számára nagyobb rugalmasságot kell biztosítani a források belső elosztásának módja tekintetében, hogy feladatait eredményesen ellássa, és eleget tegyen az elvárásoknak.

(142) Mivel ezen irányelv célját, nevezetesen a kiberbiztonság Unión belüli egységesen magas szintjének megvalósítását a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban az intézkedés hatásai miatt e cél jobban megvalósítható, az Unió intézkedéseket hozhat a szubszidiaritásnak az Európai Unióról szóló szerződés 5. cikkében foglalt elvével összhangban. Az arányosságnak az említett cikkben foglalt elvével összhangban ez az irányelv nem lépi túl az e cél eléréséhez szükséges mértéket.

(143) Az irányelv tiszteletben tartja az alapvető jogokat, és figyelembe veszi különösen a Charta által elismert elveket, mindenekelőtt a magánélet és a magáncélú kommunikáció tiszteletben tartásához való jogot, a személyes adatok védelméhez való jogot, a vállalkozás szabadságát, a tulajdonhoz való jogot, a hatékony jogorvoslathoz és a tisztességes eljáráshoz való jogot, az ártatlanság vélelmét, valamint a védelemhez való jogot. A hatékony jogorvoslathoz való jog kiterjed az alapvető és fontos szervezetek által nyújtott szolgáltatások igénybe vevőire. Ezt az irányelvet az említett jogokkal és elvekkel összhangban kell végrehajtani.

(144) Az európai adatvédelmi biztossal az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([25]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos 2021. március 11-én véleményt nyilvánított ([26]),

([23]) Az Európai Parlament és a Tanács 182/2011/EU rendelete (2011. február 16.) a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról (HL L 55., 2011.2.28., 13. o.).

([24]) Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet) (HL L 277., 2022.10.27., 1. o.).

([25]) 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.).

([26]) HL C 183., 2021.5.11., 3. o.

ELFOGADTA EZT AZ IRÁNYELVET:

I. FEJEZET

II. ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy

(1) Ez az irányelv a belső piac működésének javítása érdekében intézkedéseket határoz meg az egységesen magas szintű kiberbiztonság Unión belüli elérése céljából.

(2) Ennek érdekében ezen irányelv a következőket állapítja meg:

a) a tagállamok számára azt előíró kötelezettségek, hogy nemzeti kiberbiztonsági stratégiákat fogadjanak el, valamint illetékes hatóságokat, kiberválságok kezelésével foglalkozó hatóságokat, kiberbiztonsággal foglalkozó egyedüli kapcsolattartó pontokat (a továbbiakban: egyedüli kapcsolattartó pontok) és számítógép-biztonsági eseményekre reagáló csoportokat (a továbbiakban: CSIRT-ek) jelöljenek ki vagy hozzanak létre;

b) kiberbiztonsági kockázatkezelési intézkedések és bejelentési kötelezettségek az I. vagy a II. mellékletben említett típusú szervezetek, valamint az (EU) 2022/2557 irányelv szerint kritikus szervezetként azonosított szervezetek számára;

c) szabályok és kötelezettségek a kiberbiztonsági információk megosztására vonatkozóan;

d) felügyeleti és végrehajtási kötelezettségek a tagállamok számára.

2. cikk

Hatály

(1) Ezt az irányelvet az I. vagy II. mellékletben említett típusú olyan állami vagy magánszervezetekre kell alkalmazni, amelyek a 2003/361/EK ajánlás mellékletének 2. cikke szerint középvállalkozásoknak minősülnek vagy meghaladják az említett cikkben a középvállalkozásokra vonatkozóan előírt küszöbértékeket, és amelyek az Unión belül nyújtják szolgáltatásaikat vagy végzik tevékenységeiket.

Az említett ajánlás melléklete 3. cikkének (4) bekezdése ezen irányelv alkalmazásában nem alkalmazandó.

(2) Ez az irányelv – méretüktől függetlenül – az I. vagy II. mellékletben említett típusú szervezetekre is alkalmazandó, amennyiben:

a) a szolgáltatásokat a következők nyújtják:

   i. nyilvános elektronikus hírközlő hálózatok szolgáltatói vagy nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók;

   ii. bizalmi szolgáltatók;

   iii. legfelső szintű doménnév-nyilvántartók és doménnévrendszer-szolgáltatók;

b) a szervezet egy tagállamban az egyetlen szolgáltató egy olyan szolgáltatás tekintetében, amely elengedhetetlen a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához;

c) a szervezet által nyújtott szolgáltatás zavara jelentős hatással lehet a közvédelemre, a közbiztonságra vagy a közegészségre;

d) a szervezet által nyújtott szolgáltatás zavara jelentős rendszerszintű kockázatot idézhet elő, különösen azokban az ágazatokban, ahol az említett zavarnak határokon átnyúló hatása lehet;

e) a szervezet kritikus, mivel nemzeti vagy regionális szinten különös fontossággal bír az adott ágazat vagy szolgáltatás típusa, vagy a tagállam más, kölcsönösen függő ágazatai szempontjából;

f) a szervezet:

i. valamely tagállam által annak nemzeti jogával összhangban meghatározott, központi kormányzathoz tartozó közigazgatási szerv; vagy

ii. valamely tagállam által annak nemzeti jogával összhangban meghatározott, regionális szintű közigazgatási szerv, amely kockázatalapú értékelés alapján olyan szolgáltatásokat nyújt, amelyek zavara jelentős hatást gyakorolhat kritikus fontosságú társadalmi vagy gazdasági tevékenységekre.

(3) Ez az irányelv – méretüktől függetlenül – az (EU) 2022/2557 irányelv szerint kritikus szervezetként azonosított szervezetekre is alkalmazandó.

(4) Ez az irányelv – méretüktől függetlenül – a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetekre is alkalmazandó.

(5) A tagállamok rendelkezhetnek úgy, hogy ez az irányelv alkalmazandó a következőkre:

a) helyi szintű közigazgatási szervek;

b) oktatási intézmények, különösen, ha kritikus fontosságú kutatási tevékenységeket végeznek.

(6) Ez az irányelv nem érinti a tagállamoknak a nemzetbiztonság védelmével kapcsolatos felelősségüket és az egyéb alapvető állami funkciók védelmére vonatkozó hatáskörüket, beleértve az állam területi integritásának biztosítását és a közrend fenntartását.

(7) Ez az irányelv nem alkalmazandó azokra a közigazgatási szervekre, amelyek a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés – többek között a bűncselekmények megelőzése, kivizsgálása, felderítése és büntetőeljárás alá vonása – területén végzik tevékenységeiket.

(8) A tagállamok egyes olyan szervezeteket, amelyek a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés – többek között a bűncselekmények megelőzése, kivizsgálása, felderítése és büntetőeljárás alá vonása – területén végzik tevékenységeiket vagy amelyek kizárólag az e cikk (7) bekezdésében említett közigazgatási szervek számára nyújtanak szolgáltatásokat, az említett tevékenységek vagy szolgáltatások tekintetében mentesíthetnek a 21. vagy 23. cikkben megállapított kötelezettségek alól. Ilyen esetekben a VII. fejezetben említett felügyeleti és végrehajtási intézkedések nem alkalmazandók az említett egyes tevékenységekre vagy szolgáltatásokra. Amennyiben a szervezetek kizárólag az e bekezdésben említett típusú tevékenységeket végeznek vagy ilyen típusú szolgáltatásokat nyújtanak, a tagállamok ezeket a szervezeteket is mentesíthetik a 3. és 27. cikkben megállapított kötelezettségek alól.

(9) A (7) és (8) bekezdés nem alkalmazandó, ha a szervezet bizalmi szolgáltatóként tevékenykedik.

(10) Ez az irányelv nem alkalmazandó azokra a szervezetekre, amelyeket a tagállamok mentesítettek az (EU) 2022/2554 rendelet hatálya alól az említett rendelet 2. cikkének (4) bekezdésével összhangban.

(11) Az ezen irányelvben meghatározott kötelezettségek nem foglalják magukban olyan információk szolgáltatását, amelyek közzététele ellentétes lenne a tagállamok nemzetbiztonságának, közbiztonságának vagy védelmének alapvető érdekeivel.

(12) Ezt az irányelvet az (EU) 2016/679 rendelet, a 2002/58/EK irányelv, a 2011/93/EU ([27]) és a 2013/40/EU ([28]) európai parlamenti és tanácsi irányelv, valamint az (EU) 2022/2557 irányelv sérelme nélkül kell alkalmazni.

(13) Az EUMSZ 346. cikkének sérelme nélkül az uniós vagy nemzeti szabályok értelmében bizalmas információkat – például az üzleti titoktartási szabályokat – csak akkor lehet megosztani a Bizottsággal és az ezen irányelv szerinti más érintett hatóságokkal, ha az említett információcsere ezen irányelv alkalmazásához szükséges. A megosztott információnak az információcsere célja szempontjából lényeges és arányos mértékre kell korlátozódnia. Az információcsere során meg kell őrizni a rendelkezésre bocsátott információk bizalmas jellegét, és óvni kell az érintett szervezetek biztonsági és kereskedelmi érdekeit.

([27]) Az Európai Parlament és a Tanács 2011/93/EU irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról (HL L 335., 2011.12.17., 1. o.).

([28]) Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról (HL L 218., 2013.8.14., 8. o.).

(14) A szervezetek, az illetékes hatóságok, az egyedüli kapcsolattartó pontok és a CSIRT-ek az ezen irányelv céljaihoz szükséges mértékig és az (EU) 2016/679 rendelettel összhangban folytatnak személyesadat-kezelést, és ezen adatkezelés során különösen az említett rendelet 6. cikkére támaszkodnak.

A személyes adatok ezen irányelv szerinti kezelését a nyilvános elektronikus hírközlő hálózatok szolgáltatói vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók az adatvédelemre és a magánélet védelmére vonatkozó uniós joggal, különösen a 2002/58/EK irányelvvel összhangban végzik.

3. cikk

Alapvető és fontos szervezetek

(1) Ezen irányelv alkalmazásában a következő szervezeteket kell alapvető szervezetnek tekinteni:

a) az I. mellékletben említett típusú azon szervezetek, amelyek meghaladják a 2003/361/EK ajánlás melléklete 2. cikkének (1) bekezdésében a középvállalkozásokra vonatkozóan előírt küszöbértékeket;

b) a minősített bizalmi szolgáltatók és a legfelső szintű doménnév-nyilvántartók, valamint a DNS-szolgáltatók, méretüktől függetlenül;

c) a nyilvános elektronikus hírközlő hálózatok szolgáltatói vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók, amelyek a 2003/361/EK ajánlás mellékletének 2. cikke szerint középvállalkozásoknak minősülnek;

d) a 2. cikk (2) bekezdése f) pontjának i. alpontjában említett közigazgatási szervek;

e) az I. vagy II. mellékletben említett típusú bármely egyéb szervezetek, amelyeket egy tagállam a 2. cikk (2) bekezdésének b)–e) pontja alapján alapvető szervezetekként azonosított;

f) az ezen irányelv 2. cikkének (3) bekezdésében említett, az (EU) 2022/2557 irányelv értelmében kritikus szervezetként azonosított szervezetek;

g) amennyiben a tagállam úgy rendelkezik, azon szervezetek, amelyeket az adott tagállam 2023. január 16. előtt az (EU) 2016/1148 irányelvvel vagy a nemzeti joggal összhangban alapvető szolgáltatásokat nyújtó szereplőként azonosított.

(2) Ezen irányelv alkalmazásában az I. vagy II. mellékletben említett típusú összes olyan szervezetet, amely az e cikk (1) bekezdése értelmében nem minősül alapvető szervezetnek, fontos szervezetnek kell tekinteni. Ebbe beletartoznak azok a szervezetek, amelyeket a tagállamok a 2. cikk (2) bekezdésének b)–e) pontja alapján fontos szervezetként azonosítottak.

(3) A tagállamok 2025. április 17-ig összeállítják az alapvető és fontos szervezetek, valamint a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek jegyzékét. A tagállamok az említett jegyzéket rendszeresen, de az említett időpontot követően legalább kétévente felülvizsgálják, és adott esetben frissítik.

(4) A (3) bekezdésben említett jegyzék összeállítása céljából a tagállamok előírják az említett bekezdésben említett szervezetek számára, hogy az illetékes hatóságoknak nyújtsák be legalább a következő információkat:

a) a szervezet neve;

b) a cím és naprakész elérhetőségek, beleértve az e-mail-címeket, IP-tartományokat és telefonszámokat;

c) adott esetben az I. vagy II. mellékletben említett megfelelő ágazat és alágazat; valamint

d) adott esetben azon tagállamok jegyzéke, ahol az ezen irányelv hatálya alá tartozó szolgáltatásokat nyújtják.

A (3) bekezdésben említett szervezetek haladéktalanul, és minden esetben a változás időpontjától számított két héten belül bejelentenek az e bekezdés első albekezdése alapján benyújtott adatokban bekövetkező bármely változást.

A Bizottság az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) segítségével indokolatlan késedelem nélkül iránymutatásokat nyújt és sablonokat bocsát rendelkezésre ez e bekezdésben megállapított kötelezettségekre vonatkozóan.

A tagállamok nemzeti mechanizmusokat hozhatnak létre abból a célból, hogy a szervezetek bejegyeztessék magukat.

(5) 2025. április 17-ig és azt követően kétévente az illetékes hatóságok bejelentik:

a) a Bizottságnak és az együttműködési csoportnak az I. vagy a II. mellékletben említett egyes ágazatok és alágazatok tekintetében a (3) bekezdés szerint a jegyzékben felsorolt alapvető és fontos szervezetek számát; valamint

b) a Bizottságnak a 2. cikk (2) bekezdésének b)–e) pontja alapján azonosított alapvető és fontos szervezetek számáról, az I. vagy a II. mellékletben említett ágazatukról és alágazatukról, az általuk nyújtott szolgáltatás típusáról, valamint a 2. cikk (2) bekezdésének b)–e) pontjában megállapítottak közül az azonosításuk alapjául szolgáló rendelkezésről szóló releváns információkat.

(6) 2025. április 17-ig és a Bizottság kérésére a tagállamok bejelenthetik a Bizottságnak az (5) bekezdés b) pontjában említett alapvető és fontos szervezetek nevét.

4. cikk

Ágazatspecifikus uniós jogi aktusok

(1) Amennyiben az ágazatspecifikus uniós jogi aktusok előírják, hogy az alapvető vagy fontos szervezetek kiberbiztonsági kockázatkezelési intézkedéseket fogadjanak el, vagy bejelentsék a jelentős biztonsági eseményeket, és ha ezek a követelmények hatásukban legalább egyenértékűek az ezen irányelvben meghatározott kötelezettségekkel, akkor ezen irányelv vonatkozó rendelkezései – beleértve a VII. fejezetben meghatározott, a felügyeletre és a végrehajtásra vonatkozó rendelkezéseket – nem alkalmazandók az említett szervezetekre. Amennyiben az ágazatspecifikus uniós jogi aktusok hatálya nem terjed ki az ezen irányelv hatálya alá tartozó, adott ágazatban működő valamennyi szervezetre, ezen irányelv vonatkozó rendelkezései továbbra is alkalmazandók azokra a szervezetekre, amelyek nem tartoznak az említett ágazatspecifikus uniós jogi aktusok hatálya alá.

(2) Az e cikk (1) bekezdésében említett követelmények az ezen irányelvben megállapított kötelezettségekkel hatásukban egyenértékűnek tekintendők, ha:

a) a kiberbiztonsági kockázatkezelési intézkedések hatásukban legalább egyenértékűek a 21. cikk (1) és (2) bekezdésében megállapítottakkal; vagy

b) az ágazatspecifikus uniós jogi aktus előírja az eseménybejelentésekhez való azonnali – adott esetben automatikus és közvetlen – hozzáférést a CSIRT-ek, az illetékes hatóságok vagy az ezen irányelv szerinti egyedüli kapcsolattartó pontok számára, és ha a jelentős események bejelentésére vonatkozó követelmények hatásukban legalább egyenértékűek az ezen irányelv 23. cikkének (1)–(6) bekezdésében megállapítottakkal.

(3) A Bizottság 2023. július 17-ig iránymutatásokat ad ki, amelyekben pontosítja az (1) és (2) bekezdés alkalmazását. A Bizottság rendszeresen felülvizsgálja az említett iránymutatásokat. Az említett iránymutatások kidolgozása során a Bizottság figyelembe veszi az együttműködési csoport és az ENISA valamennyi észrevételét.

5. cikk

Minimális harmonizáció

Ez az irányelv nem akadályozza meg a tagállamokat abban, hogy magasabb szintű kiberbiztonságot biztosító rendelkezéseket fogadjanak el vagy tartsanak fenn, feltéve, ha e rendelkezések összhangban vannak a tagállamok uniós jogban megállapított kötelezettségeivel.

6. cikk

Fogalommeghatározások

Ezen irányelv alkalmazásában:

1. „hálózati és információs rendszer”:

   a) az (EU) 2018/1972 irányelv 2. cikkének 1. pontjában meghatározott elektronikus hírközlő hálózat;

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatikus kezelését végzi; vagy

c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

2. „hálózati és információs rendszerek biztonsága”: a hálózati és információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát;

3. „kiberbiztonság”: az (EU) 2019/881 rendelet 2. cikkének 1. pontjában meghatározott kiberbiztonság;

4. „nemzeti kiberbiztonsági stratégia”: valamely tagállam koherens kerete, amely meghatározza a kiberbiztonság területén követendő stratégiai célokat és prioritásokat és a megvalósításukhoz szükséges irányítási intézkedéseket az adott tagállamban;

5. „majdnem bekövetkezett (near miss) esemény”: olyan esemény, amely veszélyeztethette volna a hálózati és információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát, de amelynek bekövetkezését sikerült megakadályozni, vagy amely nem következett be;

6. „esemény”: olyan esemény, amely veszélyezteti a hálózati és információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát;

7. „nagyszabású kiberbiztonsági esemény”: olyan esemény, amely olyan mértékű zavart okoz, amely meghaladja valamely tagállamnak az arra való reagálása képességét, vagy amely legalább két tagállamra jelentős hatást gyakorol;

8. „eseménykezelés”: minden olyan tevékenység és eljárás, amelynek célja az esemény megelőzése, észlelése, elemzése és elszigetelése vagy az eseményre való reagálás és az eseményt követően a működés helyreállítása;

9. „kockázat”: egy esemény által okozott veszteség vagy zavar lehetősége, amelyet az említett veszteség vagy zavar nagyságrendje és az adott esemény bekövetkezési valószínűsége kombinációjaként kell kifejezni;

10. „kiberfenyegetés”: az (EU) 2019/881 rendelet 2. cikkének 8. pontjában meghatározott kiberfenyegetés;

11. „jelentős kiberfenyegetés”: olyan kiberfenyegetés, amelyről – technikai jellemzői alapján – feltételezhető, hogy jelentős vagyoni vagy nem vagyoni kárt okozva súlyos hatást gyakorolhat egy szervezet hálózati és információs rendszereire vagy a szervezet szolgáltatásainak felhasználóira;

12. „IKT-termék”: az (EU) 2019/881 rendelet 2. cikkének 12. pontjában meghatározott IKT-termék;

13. „IKT-szolgáltatás”: az (EU) 2019/881 rendelet 2. cikkének 13. pontjában meghatározott IKT-szolgáltatás;

14. „IKT-folyamat”: az (EU) 2019/881 rendelet 2. cikkének 14. pontjában meghatározott IKT-folyamat;

15. „sérülékenység”: valamely IKT-termék vagy IKT-szolgáltatás gyengesége, érzékenysége vagy hiányossága, amely egy kiberfenyegetés során kihasználható;

16. „szabvány”: az 1025/2012/EU európai parlamenti és tanácsi rendelet ([29]) 2. cikkének 1. pontjában meghatározott szabvány;

17. „műszaki előírás”: az 1025/2012/EU rendelet 2. cikkének 4. pontjában meghatározott műszaki előírás;

([29]) Az Európai Parlament és a Tanács 1025/2012/EU rendelete (2012. október 25.) az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről (HL L 316., 2012.11.14., 12. o.).

18. „internetes exchange pont” olyan hálózati létesítmény, amely elsősorban az internetes forgalomcsere megkönnyítése érdekében lehetővé teszi kettőnél több, egymástól független hálózat összekapcsolását (a továbbiakban: autonóm rendszerek), amely kizárólag autonóm rendszerek részére biztosít összekapcsolást, és amely nem kívánja meg, hogy a részt vevő bármely két autonóm rendszer között zajló internetes forgalom egy bármely harmadik autonóm rendszeren is áthaladjon, továbbá nem változtatja meg az említett forgalmat, és egyéb módon sem avatkozik be abba;

19. „doménnévrendszer” vagy „DNS”: hierarchikusan felépülő elnevezési rendszer, amely lehetővé teszi az internetes szolgáltatások és erőforrások azonosítását, lehetővé téve a végfelhasználók eszközei számára az internetes útvonal-meghatározási és összekapcsolási szolgáltatások igénybevételét e szolgáltatások és erőforrások elérése érdekében;

20. „DNS-szolgáltató”: olyan szervezet, amely a következőket nyújtja:

    a) nyilvánosan elérhető rekurzív doménnév-feloldási szolgáltatások az internetes végfelhasználók számára; vagy

    b) hiteles doménnév-feloldási szolgáltatások harmadik felek általi felhasználásra, a gyökérnévszerverek kivételével;

21. „legfelső szintű doménnév-nyilvántartó”: olyan szervezet, amelyre egy meghatározott legfelső szintű domént bíztak, és amely felelős egyrészt a legfelső szintű domén kezeléséért – ideértve a legfelső szintű domén alatti doménnevek nyilvántartásba vételét –, másrészt a legfelső szintű domén technikai üzemeltetéséért, amely magában foglalja a névszervereinek üzemeltetését, adatbázisainak karbantartását és a legfelső szintű domén zónafájlok elosztását a névszerverek között, függetlenül attól, hogy ezen üzemeltetési tevékenységek bármelyikét maga a szervezet végzi vagy azokat kiszervezi, kivéve azonban azon eseteket, amikor a legfelső szintű doménneveket a nyilvántartó kizárólag saját használatra veszi igénybe;

22. „doménnév-nyilvántartási szolgáltatásokat nyújtó szervezet”: regisztrátor vagy regisztrátorok nevében eljáró ügynök, például titkosított vagy meghatalmazott regisztrációs szolgáltató vagy viszonteladó;

23. „digitális szolgáltatás”: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv ([30]) 1. cikke (1) bekezdésének b) pontjában meghatározott szolgáltatás;

24. „bizalmi szolgáltatás”: a 910/2014/EU rendelet 3. cikkének 16. pontjában meghatározott bizalmi szolgáltatás;

25. „bizalmi szolgáltató”: a 910/2014/EU rendelet 3. cikkének 19. pontjában meghatározott bizalmi szolgáltató;

26. „minősített bizalmi szolgáltatás”: a 910/2014/EU rendelet 3. cikkének 17. pontjában meghatározott minősített bizalmi szolgáltatás;

27. „minősített bizalmi szolgáltató”: a 910/2014/EU rendelet 3. cikkének 20. pontjában meghatározott minősített bizalmi szolgáltató;

28. „online piactér”: a 2005/29/EK európai parlamenti és tanácsi irányelv ([31]) 2. cikkének n) pontjában meghatározott online piactér;

29. „online keresőprogram”: az (EU) 2019/1150 európai parlamenti és tanácsi rendelet ([32]) 2. cikkének 5. pontjában meghatározott online keresőprogram;

30. „felhőszolgáltatás”: olyan digitális szolgáltatás, amely igény szerinti adminisztrációt és kiterjedt távoli hozzáférést tesz lehetővé megosztható számítástechnikai erőforrások méretezhető és rugalmas készletéhez, beleértve azt is, amikor ezeket az erőforrásokat több helyszínen osztják el;

([30]) Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve (2015. szeptember 9.) a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról (HL L 241., 2015.9.17., 1. o.).

([31]) Az Európai Parlament és a Tanács 2005/29/EK irányelve (2005. május 11.) a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól, valamint a 84/450/EGK tanácsi irányelv, a 97/7/EK, a 98/27/EK és a 2002/65/EK európai parlamenti és tanácsi irányelvek, valamint a 2006/2004/EK európai parlamenti és tanácsi rendelet módosításáról („Irányelv a tisztességtelen kereskedelmi gyakorlatokról”) (HL L 149., 2005.6.11., 22. o.).

([32]) Az Európai Parlament és a Tanács (EU) 2019/1150 rendelete (2019. június 20.) az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról (HL L 186., 2019.7.11., 57. o.).

31. „adatközpont-szolgáltatás”: olyan szolgáltatás, amelynek részét képezik olyan struktúrák vagy struktúracsoportok, amelyek az adattárolási, -kezelési és -továbbítási szolgáltatásokat nyújtó informatikai és hálózati berendezések központosított elhelyezésére, összekapcsolására és működtetésére szolgálnak az energia-elosztás és a környezetvédelmi ellenőrzés összes létesítményével és infrastruktúrájával együtt;

32. „tartalomszolgáltató hálózat”: földrajzilag elosztott szerverek hálózata, amelynek célja a tartalomszolgáltatók és a szolgáltatásokat nyújtók nevében biztosítani, hogy a digitális tartalmak és szolgáltatások széleskörűen, akadálymentesen és gyorsan az internetfelhasználók rendelkezésére álljanak;

33. „közösségimédia-szolgáltatási platform”: olyan platform, amely lehetővé teszi a végfelhasználók számára, hogy több eszközön keresztül kapcsolódjanak, tartalmakat osszanak meg és fedezzenek fel és kommunikáljanak egymással, különösen csevegések, bejegyzések, videók és ajánlások révén;

34. „képviselő”: az Unióban letelepedett minden olyan természetes vagy jogi személy, akit vagy amelyet kifejezetten kijelöltek arra, hogy valamely, az Unióban nem letelepedett DNS-szolgáltató, legfelső szintű doménnév-nyilvántartó, doménnév-nyilvántartási szolgáltatásokat nyújtó szervezet, felhőszolgáltató, adatközpont-szolgáltató, tartalomszolgáltató hálózati szolgáltató, irányított szolgáltató, irányított biztonsági szolgáltató, vagy egy online piactér, online keresőprogram vagy közösségimédia-szolgáltatási platform szolgáltatója nevében eljárjon, és akihez vagy amelyhez az illetékes nemzeti hatóság vagy a CSIRT a szervezet ezen irányelv szerinti kötelezettségeit illetően az adott szervezet helyett fordulhat;

35. „közigazgatási szerv”: olyan szerv, amelyet az adott tagállam a nemzeti joggal összhangban ilyenként elismer, kivéve az igazságszolgáltatást, a parlamenteket és a központi bankokat, és amely megfelel a következő kritériumoknak:

    a) az általános érdekű szükségletek kielégítése céljából jött létre, és nincs ipari vagy kereskedelmi jellege;

    b) jogi személyiséggel rendelkezik, vagy jogszabály alapján jogosult egy másik, jogi személyiséggel rendelkező szervezet nevében eljárni;

    c) finanszírozását többnyire az állam, regionális hatóságok vagy más, közjog által szabályozott szervek végzik, irányítása az említett hatóságok vagy szervek felügyelete alatt áll, vagy van olyan igazgatási, irányító vagy felügyelő testülete, amely tagjainak több mint felét az állam, a regionális hatóságok vagy más, közjog által szabályozott szervek nevezik ki;

    d) hatásköre van arra, hogy természetes vagy jogi személyekhez a személyek, áruk, szolgáltatások vagy tőke határokon átnyúló mozgásával kapcsolatos jogaikat érintő közigazgatási határozatokat vagy szabályozási döntéseket intézzen;

36. „nyilvános elektronikus hírközlő hálózat”: az (EU) 2018/1972 irányelv 2. cikkének 8. pontjában meghatározott nyilvános elektronikus hírközlő hálózat;

37. „elektronikus hírközlési szolgáltatás”: az (EU) 2018/1972 irányelv 2. cikkének 4. pontjában meghatározott elektronikus hírközlési szolgáltatás;

38. „szervezet”: olyan természetes vagy jogi személy, amelyet letelepedési helyének nemzeti joga alapján hoztak létre és elismertek, és amely a saját nevében eljárva jogokat gyakorolhat és kötelezettségei lehetnek;

39. „irányított szolgáltató”: olyan szervezet, amely IKT-termékek, -hálózatok, -infrastruktúra, -alkalmazások vagy bármely más hálózati és információs rendszer telepítésével, irányításával, üzemeltetésével vagy karbantartásával kapcsolatos szolgáltatásokat nyújt az ügyfelek helyiségeiben vagy távolról végzett segítségnyújtás vagy aktív adminisztráció révén;

40. „irányított biztonsági szolgáltató”: olyan irányított szolgáltató, amely a kiberbiztonsági kockázatok kezeléséhez kapcsolódó tevékenységeket végez, vagy segítséget nyújt ilyen tevékenységekhez;

41. „kutatóhely”: olyan szervezet, amelynek elsődleges célja alkalmazott kutatás vagy kísérleti fejlesztés folytatása az említett kutatás eredményeinek kereskedelmi célokra való hasznosítása céljából, de amely nem foglalja magában az oktatási intézményeket.

II. FEJEZET

ÖSSZEHANGOLT KIBERBIZTONSÁGI KERETEK

7. cikk

Nemzeti kiberbiztonsági stratégia

(1) A magas szintű kiberbiztonság elérése és fenntartása céljából minden tagállam nemzeti kiberbiztonsági stratégiát fogad el, amely előírja a stratégiai célokat, az e célok eléréséhez szükséges erőforrásokat, valamint a megfelelő szakpolitikai és szabályozási intézkedéseket. A nemzeti kiberbiztonsági stratégiának a következőket kell tartalmaznia:

a) a kiberbiztonságra vonatkozó tagállami stratégia céljai és prioritásai, különösen az I. és II. mellékletben említett ágazatokra vonatkozóan;

b) az e bekezdés a) pontjában említett célok és prioritások eléréséhez szükséges irányítási keretrendszer, ideértve a (2) bekezdésben említett szakpolitikákat;

c) a releváns érdekelt felek szerepét és felelősségi körét nemzeti szinten tisztázó irányítási keret, amely alapul szolgál az ezen irányelv szerinti illetékes hatóságok, egyedüli kapcsolattartó pontok és CSIRT-ek közötti nemzeti szintű együttműködéshez és koordinációhoz, valamint az említett szervek és az ágazatspecifikus uniós jogi aktusok szerinti illetékes hatóságok közötti koordinációhoz és együttműködéshez;

d) a releváns eszközök azonosítására szolgáló mechanizmus és a kockázatok értékelése az adott tagállamban;

e) az eseményekre való felkészültséget, az azokra való reagálási képességet és az eseményeket követően a működés helyreállítását biztosító intézkedések azonosítása, ideértve a köz- és magánszféra közötti együttműködést is;

f) a nemzeti kiberbiztonsági stratégia végrehajtásában részt vevő különféle hatóságok és érdekelt felek listája;

g) az ezen irányelv és az (EU) 2022/2557 irányelv szerinti illetékes hatóságok közötti, a kockázatokkal, a kiberfenyegetésekkel és az eseményekkel, továbbá a nem kiberbiztonsági jellegű kockázatokkal, fenyegetésekkel és eseményekkel kapcsolatos információk megosztását és adott esetben a felügyeleti feladatok ellátását célzó fokozott koordináció szakpolitikai kerete;

h) a kiberbiztonsággal kapcsolatos tudatosság általános szintjének a polgárok körében történő fokozását célzó terv, ideértve a szükséges intézkedéseket is.

(2) A nemzeti kiberbiztonsági stratégia részeként a tagállamok szakpolitikákat fogadnak el különösen:

a) a szervezetek által szolgáltatásaik nyújtásához használt IKT-termékek és IKT-szolgáltatások ellátási lánca kiberbiztonságának kezelésére;

b) az IKT-termékek és IKT-szolgáltatások kiberbiztonsággal kapcsolatos követelményeinek a közbeszerzésekbe történő felvételére és meghatározására vonatkozóan, többek között a kiberbiztonsági tanúsítás, a titkosítási követelmények és a nyílt forráskódú kiberbiztonsági termékek használata tekintetében;

c) a sérülékenységek kezelésére, amely magában foglalja a sérülékenységek 12. cikk (1) bekezdése szerinti összehangolt közzétételének előmozdítását és megkönnyítését;

d) a nyílt internet nyilvános alkotóelemei általános rendelkezésre állásának, sértetlenségének és bizalmasságának fenntartására vonatkozóan, beleértve adott esetben a tenger alatti kommunikációs kábelek kiberbiztonságát is;

e) a legkorszerűbb kiberbiztonsági kockázatkezelési intézkedések végrehajtását célzó megfelelő fejlett technológiák fejlesztésének és integrációjának előmozdítására;

f) a kiberbiztonsággal, a kiberbiztonsági készségekkel, a figyelemfelkeltéssel, valamint a kutatási és fejlesztési kezdeményezésekkel kapcsolatos oktatás és képzés, valamint a helyes kiberhigiéniai gyakorlatokkal és ellenőrzésekkel kapcsolatos, a polgárokat, az érdekelt feleket és a szervezeteket célzó iránymutatások előmozdítására és fejlesztésére;

g) a tudományos és kutatóintézetek támogatására a kiberbiztonsági eszközök és a biztonságos hálózati infrastruktúra fejlesztése, megerősítése és bevezetésének előmozdítása terén;

h) vonatkozó eljárások és megfelelő információmegosztási eszközök beépítésére a szervezetek közötti – az uniós jognak megfelelő – önkéntes kiberbiztonsági információmegosztás támogatása céljából;

i) a kis- és középvállalkozások – különösen az ezen irányelv hatálya alól kizárt kkv-k – alapszintű kiberbiztonsági ellenállóképességének és kiberhigiéniájának megerősítésére azok sajátos szükségleteihez igazodó, könnyen hozzáférhető iránymutatások és segítségnyújtás révén;

j) az aktív kiberbiztonság előmozdítására.

(3) A tagállamok az elfogadásuktól számított három hónapon belül értesítik a Bizottságot nemzeti kiberbiztonsági stratégiájukról. Ezen értesítésből a tagállamok kihagyhatják a nemzetbiztonságukkal kapcsolatos információkat.

(4) A tagállamok a fő teljesítménymutatók alapján rendszeresen, de legalább ötévente értékelik nemzeti kiberbiztonsági stratégiájukat, és szükség esetén aktualizálják azt. Az ENISA kérésre segítséget nyújt a tagállamoknak a nemzeti kiberbiztonsági stratégia és a stratégia értékelésére szolgáló fő teljesítménymutatók kidolgozásához vagy aktualizálásához annak érdekében, hogy összehangolja a stratégiát az ezen irányelvben megállapított követelményekkel és kötelezettségekkel.

8. cikk

Illetékes hatóságok és egyedüli kapcsolattartó pontok

(1) Minden tagállam kijelöl vagy létrehoz egy vagy több, a kiberbiztonságért és a VII. fejezetben említett felügyeleti feladatokért felelős illetékes hatóságot (a továbbiakban: illetékes hatóságok).

(2) Az (1) bekezdésben említett illetékes hatóságok nemzeti szinten nyomon követik ezen irányelv végrehajtását.

(3) Minden tagállam kijelöl vagy létrehoz egy egyedüli kapcsolattartó pontot. Amennyiben valamely tagállam az (1) bekezdés alapján csak egy illetékes hatóságot jelöl ki vagy hoz létre, ez az illetékes hatóság lesz a tagállam egyedüli kapcsolattartó pontja is.

(4) Minden egyes egyedüli kapcsolattartó pont összekötő feladatot lát el annak biztosítása érdekében, hogy tagállama hatóságai határokon átnyúlóan együttműködjenek a többi tagállam érintett hatóságaival és adott esetben a Bizottsággal és az ENISA-val, valamint az ágazatok közötti együttműködésnek a tagállama más illetékes nemzeti hatóságaival való biztosítása érdekében.

(5) A tagállamok biztosítják, hogy illetékes hatóságaik és egyedüli kapcsolattartó pontjaik elegendő erőforrással rendelkeznek a rájuk bízott feladatok hatékony és eredményes ellátásához és ezáltal ezen irányelv célkitűzéseinek teljesítéséhez.

(6) Minden tagállam indokolatlan késedelem nélkül értesíti a Bizottságot az (1) bekezdésben említett illetékes hatóságról és a (3) bekezdésben említett egyedüli kapcsolattartó pontról, az említett hatóságok feladatairól és azok minden későbbi változásáról. Minden tagállam nyilvánosságra hozza, hogy mely hatóság az illetékes hatósága. A Bizottság nyilvánosan elérhetővé teszi az egyedüli kapcsolattartó pontok jegyzékét.

9. cikk

Nemzeti kiberbiztonsági válságkezelési keretek

(1) Minden tagállam kijelöl vagy létrehoz egy vagy több illetékes hatóságot, amely felelős a nagyszabású kiberbiztonsági események és válságok kezeléséért (a továbbiakban: kiberválságok kezelésével foglalkozó hatóságok). A tagállamok biztosítják, hogy az említett hatóságok megfelelő forrásokkal rendelkezzenek a rájuk ruházott feladatok hatékony és eredményes ellátásához. A tagállamok biztosítják a koherenciát a meglévő általános nemzeti válságkezelési keretekkel.

(2) Amennyiben valamely tagállam az (1) bekezdés alapján egynél több, kiberválságok kezelésével foglalkozó hatóságot jelöl ki vagy hoz létre, egyértelműen meg kell jelölnie, hogy e hatóságok közül melyik látja el a koordinátor szerepét a nagyszabású kiberbiztonsági események és válságok kezelésében.

(3) Minden tagállam meghatározza azon képességeket, eszközöket és eljárásokat, amelyek válság esetén ezen irányelv alkalmazásában alkalmazhatók.

(4) Minden tagállam elfogad egy, a nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti tervet, amelyben meghatározza a nagyszabású kiberbiztonsági események és válságok kezelésének célkitűzéseit és szabályait. Az említett tervnek különösen a következőket kell meghatároznia:

a) a nemzeti felkészültségi intézkedések és tevékenységek célkitűzései;

b) a kiberválságok kezelésével foglalkozó hatóságok feladatai és felelősségei;

c) a kiberválságok kezelésére szolgáló eljárások, beleértve azok integrálását az általános nemzeti válságkezelési keretbe és az információcserére szolgáló csatornákba;

d) nemzeti felkészültségi intézkedések, beleértve a gyakorlatokat és a képzési tevékenységeket;

e) az érintett állami és magán érdekelt felek, valamint az érintett infrastruktúra azonosítása;

f) nemzeti eljárások és megállapodások az érintett nemzeti hatóságok és szervek között annak biztosítása érdekében, hogy a tagállam hatékonyan részt vegyen a nagyszabású kiberbiztonsági események és válságok uniós szintű összehangolt kezelésében és azt hatékonyan támogassa.

(5) Az (1) bekezdésben említett, kiberválságok kezelésével foglalkozó hatóság kijelölését vagy létrehozását követő három hónapon belül minden tagállam tájékoztatja a Bizottságot a hatóságáról és az azt érintő, minden későbbi változásról. A tagállamok benyújtják a Bizottságnak és az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatának (a továbbiakban: EU-CyCLONe) a nagyszabású kiberbiztonsági esemény- és válságelhárítási nemzeti terveikre vonatkozó, a (4) bekezdésben foglalt követelményekkel kapcsolatos releváns információkat az említett tervek elfogadását követő három hónapon belül. A tagállamok kihagyhatnak információkat, annyiban és amennyiben ez nemzetbiztonságuk szempontjából szükséges.

10. cikk

Számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek)

(1) Minden tagállam kijelöl vagy létrehoz egy vagy több CSIRT-et. A CSIRT-ek kijelölhetők vagy létrehozhatók egy illetékes hatóságon belül. A CSIRT-eknek meg kell felelniük a 11. cikk (1) bekezdésében meghatározott követelményeknek, legalább az I. és II. mellékletben említett ágazatokra, alágazatokra és szervezettípusokra ki kell terjedniük, és az események egy jól meghatározott folyamat szerinti kezeléséért kell felelniük.

(2) A tagállamok biztosítják, hogy minden CSIRT megfelelő erőforrásokkal rendelkezzen a 11. cikk (3) bekezdésében meghatározott feladatai hatékony végrehajtásához.

(3) A tagállamok biztosítják, hogy az alapvető és fontos szervezetekkel és más érintett érdekelt felekkel folytatott információcsere céljából minden CSIRT rendelkezzen megfelelő, biztonságos és reziliens kommunikációs és információs infrastruktúrával. E célból a tagállamok biztosítják, hogy minden CSIRT részt vegyen a biztonságos információmegosztó eszközök kiépítésében.

(4) A CSIRT-ek együttműködnek, és adott esetben a 29. cikkel összhangban releváns információkat cserélnek az alapvető és fontos szervezetek ágazati vagy ágazatközi csoportjaival.

(5) A CSIRT-ek részt vesznek a 19. cikkel összhangban szervezett szakértői értékelésekben.

(6) A tagállamok biztosítják, hogy a CSIRT-jeik hatékonyan, eredményesen és biztonságosan működjenek együtt a CSIRT-hálózatban.

(7) A CSIRT-ek együttműködési kapcsolatokat alakíthatnak ki harmadik országok nemzeti, számítógép-biztonsági eseményekre reagáló csoportjaival. Ezen együttműködési kapcsolatok részeként a tagállamok elősegítik a megfelelő információmegosztási protokollok – többek között a jelzőlámpa-protokoll (TLP) – használatával történő hatékony, eredményes és biztonságos információcserét harmadik országok nemzeti, számítógép-biztonsági eseményekre reagáló csoportjaival. A CSIRT-ek az uniós adatvédelmi joggal összhangban releváns információkat – többek között személyes adatokat – cserélhetnek harmadik országok nemzeti, számítógép-biztonsági eseményekre reagáló csoportjaival.

(8) A CSIRT-ek együttműködhetnek harmadik országok nemzeti, számítógép-biztonsági eseményekre reagáló csoportjaival vagy azokkal egyenértékű harmadik országbeli szervekkel különösen a célból, hogy kiberbiztonsági segítséget nyújtsanak részükre.

(9) Minden tagállam indokolatlan késedelem nélkül értesíti a Bizottságot az (1) bekezdésben említett CSIRT-ről és a 12. cikk (1) bekezdése értelmében koordinátorként kijelölt CSIRT-ről, az alapvető és fontos szervezetekkel összefüggő feladataikról, valamint az ezekkel kapcsolatos minden későbbi változásról.

(10) A tagállamok kérhetik az ENISA segítségét a CSIRT-jeik kialakításához.

11. cikk

A CSIRT-ekre vonatkozó követelmények, a CSIRT-ek technikai képességei és feladatai

(1) A CSIRT-eknek meg kell felelniük a következő követelményeknek:

a) a CSIRT-eknek a kritikus hibapontok kiküszöbölése révén biztosítaniuk kell a kommunikációs csatornáik magas szintű elérhetőségét, továbbá elérhetőségük és másokkal való kapcsolattartásuk céljára folyamatosan több eszközt kell fenntartaniuk; a CSIRT-eknek a kommunikációs csatornákat egyértelműen meg kell határozniuk, és azokat a felhasználóik és az együttműködési partnereik tudomására kell hozniuk;

b) a CSIRT-ek hivatali helyiségeit és a támogató információs rendszereket biztonságos helyszíneken kell elhelyezni;

c) a CSIRT-eknek megfelelő rendszerrel kell rendelkezniük a megkeresések kezelésére és továbbítására, különösen a hatékony és eredményes átadás megkönnyítése céljából;

d) a CSIRT-eknek biztosítaniuk kell műveleteik bizalmas jellegét és megbízhatóságát;

e) a CSIRT-eket elegendő személyzettel kell ellátni ahhoz, hogy szolgáltatásaik mindig rendelkezésre álljanak, és gondoskodniuk kell arról, hogy személyzetük megfelelően képzett legyen;

f) a CSIRT-eket redundáns rendszerekkel és tartalék munkaterülettel kell ellátni a szolgáltatásaik folyamatosságának biztosítása érdekében.

A CSIRT-ek részt vehetnek nemzetközi együttműködési hálózatokban.

(2) A tagállamok biztosítják, hogy CSIRT-jeik együttesen rendelkezzenek a (3) bekezdésben említett feladatok végrehajtásához szükséges technikai képességekkel. A tagállamok biztosítják, hogy elegendő erőforrást fordítsanak a CSIRT-jeikre a megfelelő személyzeti létszám biztosításához annak érdekében, hogy a CSIRT-ek fejleszthessék technikai képességeiket.

(3) A CSIRT-ek a következő feladatokat látják el:

a) a kiberfenyegetések, sérülékenységek és események nyomon követése és elemzése nemzeti szinten, valamint kérésre segítségnyújtás az érintett alapvető és fontos szervezetek számára a hálózataik és információs rendszereik valós idejű vagy közel valós idejű nyomon követése tekintetében;

b) a kiberfenyegetésekkel, a sérülékenységekkel és az eseményekkel kapcsolatos korai előrejelzések, riasztások, bejelentéstételek és információterjesztés az érintett alapvető és fontos szervezetek, valamint az illetékes hatóságok és az egyéb releváns érdekelt felek számára, lehetőség szerint közel valós időben;

c) reagálás az eseményekre és adott esetben segítségnyújtás az érintett alapvető és fontos szervezetek számára;

d) forenzikus adatok gyűjtése és elemzése, továbbá dinamikus kockázat- és eseményelemzés, valamint a kiberbiztonsággal kapcsolatos helyzetismeret biztosítása;

e) valamely alapvető vagy fontos szervezet kérésére az érintett szervezet hálózati és információs rendszerei proaktív átvizsgálásának biztosítása olyan sérülékenységek felderítése céljából, amelyek jelentős hatást gyakorolhatnak;

f) részvétel a CSIRT-hálózatban, valamint kapacitásaiknak és hatásköreiknek megfelelően kölcsönös segítségnyújtás a CSIRT-hálózat többi tagjának azok kérésére;

g) adott esetben a koordinátori szerep betöltése a sérülékenységeknek a 12. cikk (1) bekezdésében említett összehangolt közzététele céljából;

h) hozzájárulás a 10. cikk (3) bekezdése szerinti biztonságos információmegosztási eszközök bevezetéséhez.

A CSIRT-ek proaktív, behatolásmentes átvilágítást végezhetnek az alapvető és fontos szervezetek nyilvánosan hozzáférhető hálózati és információs rendszerein. Ezen átvilágítás célja a sérülékeny vagy nem biztonságosan konfigurált hálózati és információs rendszerek felderítése és az érintett szervezetek tájékoztatása. Ez az átvilágítás semmilyen negatív hatást nem gyakorolhat a szervezetek szolgáltatásainak működésére.

Az első albekezdésben említett feladatok végrehajtása során a CSIRT-ek kockázatalapú megközelítés alapján rangsorolhatnak bizonyos feladatokat.

(4) A CSIRT-ek együttműködési kapcsolatokat alakítanak ki a magánszektor érintett érdekelt feleivel ezen irányelv célkitűzéseinek elérése érdekében.

(5) A (4) bekezdésben említett együttműködés megkönnyítése érdekében a CSIRT-ek előmozdítják a közös vagy szabványosított gyakorlatok, osztályozási rendszerek és rendszertanok elfogadását és alkalmazását a következők tekintetében:

a) az események kezelésre vonatkozó eljárások;

b) válságkezelés; valamint

c) a sérülékenységeknek a 12. cikk (1) bekezdése szerinti összehangolt közzététele.

12. cikk

Sérülékenységek összehangolt közzététele és egy európai sérülékenység-adatbázis

(1) Minden tagállam kijelöli egyik CSIRT-jét koordinátorként a sérülékenységek összehangolt közzététele céljából. A koordinátorként kijelölt CSIRT megbízható közvetítőként jár el, szükség esetén megkönnyítve a sérülékenységet bejelentő természetes vagy jogi személy és a potenciálisan sérülékeny IKT-termékek vagy IKT-szolgáltatások gyártója vagy szolgáltatója közötti kapcsolattartást, bármely fél kérésére. A koordinátorként kijelölt CSIRT feladatai közé tartozik:

a) az érintett szervezetek azonosítása és a velük való kapcsolatfelvétel;

b) a sérülékenységet bejelentő természetes vagy jogi személyek segítése; és

c) a közzétételi ütemtervek megtárgyalása és a több szervezetet érintő sérülékenységek kezelése.

A tagállamok biztosítják, hogy a természetes vagy jogi személyek – kérésükre névtelenül – bejelenthessenek valamely sérülékenységet a koordinátorként kijelölt CSIRT-nek. A koordinátorként kijelölt CSIRT biztosítja, hogy a bejelentett sérülékenység tekintetében gondos nyomonkövetési intézkedések végrehajtására kerüljön sor, és biztosítja a sérülékenységet bejelentő természetes vagy jogi személy névtelenségét. Ha a bejelentett sérülékenység több tagállamban is jelentős hatást gyakorolhat a szervezetekre, az érintett tagállamok koordinátorként kijelölt CSIRT-jeinek adott esetben együtt kell működnie a többi koordinátorként kijelölt CSIRT-tel a CSIRT-hálózaton belül.

(2) Az ENISA az együttműködési csoporttal folytatott konzultációt követően kidolgozza és fenntartja az európai sérülékenység-adatbázist. E célból az ENISA létrehozza és fenntartja a megfelelő információs rendszereket, szabályzatokat és eljárásokat, valamint elfogadja az európai sérülékenység-adatbázis biztonságának és integritásának biztosításához szükséges műszaki és szervezeti intézkedéseket, különösen annak érdekében, hogy a szervezetek – függetlenül attól, hogy ezen irányelv hatálya alá tartoznak-e – és a hálózati és információs rendszereket biztosító beszállítóik számára lehetővé tegye az IKT-termékekben vagy az IKT-szolgáltatásokban található nyilvánosan ismert sérülékenységek önkéntes alapon történő közzétételét és nyilvántartását. Minden érdekelt fél számára hozzáférést kell biztosítani az európai sérülékenység-adatbázisban található sérülékenységekre vonatkozó információkhoz. Ezen adatbázisnak tartalmaznia kell:

a) a sérülékenységet leíró információkat;

b) az érintett IKT-terméket vagy IKT-szolgáltatásokat, valamint a sérülékenység súlyosságát azon körülmények szempontjából, amelyek között a sérülékenység kihasználható;

c) a kapcsolódó javítások elérhetőségét, valamint elérhető javítás hiányában az illetékes hatóságok vagy a CSIRT-ek által a sérülékeny IKT-termékek és IKT-szolgáltatások felhasználói számára a közzétett sérülékenységekből fakadó kockázatok mérséklésének módjáról kiadott útmutatást.

13. cikk

Nemzeti szintű együttműködés

(1) Ugyanazon tagállam illetékes hatóságai, egyedüli kapcsolattartó pontja, valamint CSIRT-jei – amennyiben különállóak – kötelesek együttműködni az ezen irányelvben meghatározott kötelezettségek végrehajtása tekintetében.

(2) A tagállamok biztosítják, hogy CSIRT-jeik vagy adott esetben illetékes hatóságaik a 23. cikk értelmében értesítést kapjanak a jelentős eseményekről, valamint a 30. cikk értelmében az eseményekről, kiberfenyegetésekről és majdnem bekövetkezett eseményekről.

(3) A tagállamok biztosítják, hogy CSIRT-jeik vagy adott esetben illetékes hatóságaik tájékoztassák egyedüli kapcsolattartó pontjukat az ezen irányelv alapján bejelentett eseményekről, kiberfenyegetésekről és majdnem bekövetkezett eseményekről.

(4) Annak érdekében, hogy biztosítsák az illetékes hatóságok, az egyedüli kapcsolattartó pontok és a CSIRT-ek feladatainak és kötelezettségeinek hatékony végrehajtását, a tagállamok az adott tagállamon belül lehetőség szerint biztosítják a megfelelő együttműködést az említett szervek és a bűnüldöző hatóságok, az adatvédelmi hatóságok, a 300/2008/EK és az (EU) 2018/1139 rendelet szerinti nemzeti hatóságok, a 910/2014/EU rendelet szerinti felügyeleti szervek, az (EU) 2022/2554 rendelet szerinti illetékes hatóságok, az (EU) 2018/1972 irányelv szerinti nemzeti szabályozó hatóságok, az (EU) 2022/2557 irányelv szerinti illetékes hatóságok, valamint az egyéb ágazatspecifikus uniós jogi aktusok szerinti illetékes hatóságok között.

(5) A tagállamok biztosítják, hogy az ezen irányelv szerinti illetékes hatóságaik és az (EU) 2022/2557 irányelv szerinti illetékes hatóságaik rendszeresen együttműködjenek és információt cseréljenek a kritikus szervezetek azonosításáról, a kockázatokról, a kiberfenyegetésekről és az eseményekről, továbbá az (EU) 2022/2557 irányelv szerint kritikus szervezetként azonosított alapvető szervezeteket érintő nem kiberbiztonsági kockázatokról, fenyegetésekről és eseményekről, valamint az említett kockázatokra, fenyegetésekre és eseményekre való reagálásként hozott intézkedésekről. A tagállamok biztosítják továbbá, hogy az ezen irányelv szerinti illetékes hatóságok és a 910/2014/EU rendelet, az (EU) 2022/2554 rendelet, valamint az (EU) 2018/1972 irányelv szerinti illetékes hatóságaik rendszeresen releváns információkat cseréljenek, többek között a releváns eseményekkel és kiberfenyegetésekkel kapcsolatban.

(6) A tagállamok a 23. és a 30. cikkben említett bejelentések tekintetében technikai eszközök révén egyszerűsítik a jelentéstételt.

III. FEJEZET

UNIÓS ÉS NEMZETKÖZI SZINTŰ EGYÜTTMŰKÖDÉS

14. cikk

Együttműködési csoport

(1) A tagállamok közötti stratégiai együttműködés és információcsere támogatása és megkönnyítése, valamint a bizalom erősítése érdekében együttműködési csoport kerül létrehozásra.

(2) Az együttműködési csoport feladatait a (7) bekezdésben említett kétéves munkaprogramok alapján látja el.

(3) Az együttműködési csoport a tagállamok, a Bizottság és az ENISA képviselőiből áll. Az Európai Külügyi Szolgálat megfigyelőként vesz részt az együttműködési csoport tevékenységeiben. Az európai felügyeleti hatóságok (a továbbiakban: EFH-k) és az (EU) 2022/2554 rendelet szerinti illetékes hatóságok az említett rendelet 47. cikkének (1) bekezdésével összhangban részt vehetnek az együttműködési csoport tevékenységeiben.

Adott esetben az együttműködési csoport meghívhatja az Európai Parlamentet és az érintett érdekelt felek képviselőit, hogy vegyenek részt a munkájában.

A titkárságot a Bizottság biztosítja.

(4) Az együttműködési csoport a következő feladatokat látja el:

a) iránymutatás nyújtása az illetékes hatóságok számára ezen irányelv átültetésével és végrehajtásával kapcsolatban;

b) iránymutatás nyújtása az illetékes hatóságok számára a sérülékenységek összehangolt közzétételére vonatkozó, a 7. cikk (2) bekezdésének c) pontjában említett szakpolitikák kidolgozásához és végrehajtásához;

c) az ezen irányelv végrehajtásával kapcsolatos bevált gyakorlatok és információk cseréje, többek között a kiberfenyegetések, az események, a sérülékenységek, a majdnem bekövetkezett események, a figyelemfelkeltő kezdeményezések, képzés, gyakorlatok és készségek, a kapacitásépítés, a szabványok és a műszaki előírások, valamint az alapvető és fontos szervezeteknek a 2. cikk (2) bekezdésének b)–e) pontja alapján történő azonosítása tekintetében;

d) tanácsadás és együttműködés a Bizottsággal a kialakítás alatt álló kiberbiztonsági szakpolitikai kezdeményezésekkel és az ágazatspecifikus kiberbiztonsági követelmények általános következetességével kapcsolatban;

e) tanácsadás és együttműködés a Bizottsággal az ezen irányelv alapján elfogadott felhatalmazáson alapuló vagy végrehajtási jogi aktusok tervezetével kapcsolatban;

f) bevált gyakorlatok és információk cseréje az érintett uniós intézményekkel, szervekkel, hivatalokkal és ügynökségekkel;

g) eszmecsere a kiberbiztonságra vonatkozó rendelkezéseket tartalmazó ágazatspecifikus uniós jogi aktusok végrehajtásáról;

h) adott esetben a 19. cikk (9) bekezdésében említett szakértői értékelésről szóló jelentések megvitatása, továbbá következtetések és ajánlások megfogalmazása;

i) a 22. cikk (1) bekezdésével összhangban a kritikus ellátási láncok összehangolt biztonsági kockázatértékelésének elvégzése;

j) a kölcsönös segítségnyújtás eseteinek megvitatása, beleértve a 37. cikkben említett, határokon átnyúló közös felügyeleti intézkedések tapasztalatait és eredményeit;

k) egy vagy több érintett tagállam kérésére a 37. cikkben említettek szerinti kölcsönös segítségnyújtás iránti konkrét megkeresések megvitatása;

l) stratégiai iránymutatás nyújtása a CSIRT-hálózat és az EU–CyCLONe számára konkrét felmerülő kérdésekben;

m) a CSIRT-hálózat és az EU-CyCLONe által levont tanulságok alapján eszmecsere a nagyszabású kiberbiztonsági eseményeket és válságokat követő nyomonkövetési intézkedésekre vonatkozó szakpolitikáról;

n) hozzájárulás a kiberbiztonsági képességekhez az egész Unióban a nemzeti tisztviselők cseréjének megkönnyítésével az illetékes hatóságok vagy CSIRT-ek munkatársait bevonó kapacitásépítő program révén;

o) rendszeres közös megbeszélések szervezése az Unió egész területéről érkező magánszférabeli érdekelt felekkel, hogy megvitassák az együttműködési csoport tevékenységeit, és információkat gyűjtsenek a felmerülő szakpolitikai kihívásokról;

p) a kiberbiztonsági gyakorlatokkal kapcsolatos munka megvitatása, ideértve az ENISA által végzett munkát is;

q) a 19. cikk (1) bekezdésében említett szakértői értékelések módszertanának és szervezeti szempontjainak megállapítása, valamint a 19. cikk (5) bekezdésével összhangban a tagállamok számára az önértékelési módszertan meghatározása a Bizottság és az ENISA segítségével, valamint a Bizottsággal és az ENISA-val együttműködésben a 19. cikk (6) bekezdésével összhangban a kijelölt kiberbiztonsági szakértők munkamódszereit alátámasztó magatartási kódexek kidolgozása;

r) a 40. cikkben említett felülvizsgálat céljából jelentések készítése a stratégiai szinten és a szakértői értékelésekből szerzett tapasztalatokról;

s) a kiberfenyegetések vagy -események, például a zsarolóvírusok aktuális helyzetének rendszeres megvitatása és értékelése.

Az együttműködési csoport benyújtja az első albekezdés r) pontjában említett jelentéseket a Bizottságnak, az Európai Parlamentnek és a Tanácsnak.

(5) A tagállamok biztosítják, hogy képviselőik hatékonyan, eredményesen és biztonságosan működnek együtt az együttműködési csoportban.

(6) Az együttműködési csoport műszaki jelentést kérhet a CSIRT-hálózattól kiválasztott témákról.

(7) Az együttműködési csoport 2024. február 1-ig, majd azt követően kétévente munkaprogramot állít össze a céljai és feladatai végrehajtása érdekében megvalósítandó intézkedésekről.

(8) A Bizottság végrehajtási jogi aktusokat fogadhat el, amelyek meghatározzák az együttműködési csoport működéséhez szükséges eljárási szabályokat.

Ezeket a végrehajtási jogi aktusokat a 39. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

A Bizottság a (4) bekezdés e) pontjával összhangban megosztja a szakértelmet és együttműködik az együttműködési csoporttal az e bekezdés első albekezdésében említett végrehajtási jogi aktusok tervezetével kapcsolatban.

(9) Az együttműködési csoport rendszeresen és mindenképpen évente legalább egy alkalommal ülésezik az (EU) 2022/2557 irányelv alapján létrehozott, a kritikus szervezetek rezilienciájával foglalkozó csoporttal a stratégiai együttműködés és az információcsere elősegítése és megkönnyítése érdekében.

15. cikk

A CSIRT-hálózat

(1) A bizalom fejlődéséhez való hozzájárulás és a tagállamok közötti gyors és hatékony operatív együttműködés előmozdítása érdekében létrehozásra kerül a nemzeti CSIRT-hálózat.

(2) A CSIRT-hálózat a 10. cikk alapján kijelölt vagy létrehozott CSIRT-ek, valamint az Unió intézményei, szervei és ügynökségei hálózatbiztonsági vészhelyzeteket elhárító csoportjának (CERT-EU) képviselőiből áll. A Bizottság megfigyelőként vesz részt a CSIRT-hálózatban. Az ENISA biztosítja a titkárságot, és aktívan segítséget nyújt a CSIRT-ek közötti együttműködéshez.

(3) A CSIRT-hálózat a következő feladatokat látja el:

a) információmegosztás a CSIRT-ek képességeiről;

b) a technológiák és a releváns intézkedések, szabályzatok, eszközök, eljárások, bevált gyakorlatok és keretek CSIRT-ek közötti megosztásának, átadásának és cseréjének megkönnyítése;

c) releváns információk cseréje az eseményekről, a majdnem bekövetkezett eseményekről, a kiberfenyegetésekről, a kockázatokról és a sérülékenységekről;

d) a kiberbiztonsági kiadványokkal és ajánlásokkal kapcsolatos információk cseréje;

e) az interoperabilitás biztosítása az információmegosztási előírások és protokollok tekintetében;

f) a CSIRT-hálózat valamely esemény által potenciálisan érintett tagjának kérésére az említett eseményre és a kapcsolódó kiberfenyegetésekre, kockázatokra és sérülékenységekre vonatkozó információk cseréje és azok megvitatása;

g) a CSIRT-hálózat tagjának kérésére az adott tagállam joghatósága alatt azonosított eseményre vonatkozó összehangolt válasz megvitatása és lehetőség szerint végrehajtása;

h) segítség nyújtása a tagállamoknak a határokon átnyúló események ezen irányelv szerinti kezelése érdekében;

i) együttműködés, a bevált gyakorlatok cseréje és segítségnyújtás a 12. cikk (1) bekezdése szerint koordinátorként kijelölt CSIRT-ek számára az olyan sérülékenységek összehangolt közzétételének kezelése tekintetében, amelyek több tagállamban is jelentős hatást gyakorolhatnak a szervezetekre;

j) az operatív együttműködés további formáinak megvitatása és meghatározása, beleértve a következők tekintetében:

   i. a kiberfenyegetések és események kategóriái;

   ii. korai előrejelzések;

   iii. kölcsönös segítségnyújtás;

   iv. a határokon átnyúló kockázatok és események elhárítása koordinálásának elvei és szabályai;

   v. tagállami kérésre hozzájárulás a 9. cikk (4) bekezdésében említett nemzeti nagyszabású kiberbiztonsági esemény- és válságelhárítási tervhez;

k) az együttműködési csoport tájékoztatása a tevékenységeiről és az operatív együttműködésnek a j) pont szerint megvitatott további formáiról, és adott esetben iránymutatás kérése az operatív együttműködésre nézve;

l) a kiberbiztonsági gyakorlatok számbavétele, beleértve az ENISA által szervezetteket is;

m) valamely CSIRT kérésére az említett CSIRT képességeinek és felkészültségének megvitatása;

n) együttműködés és információcsere a regionális és uniós szintű biztonsági műveleti központokkal annak érdekében, hogy az egész Unióban javuljon az eseményekkel és a kiberfenyegetésekkel kapcsolatos közös helyzetismeret;

o) adott esetben a 19. cikk (9) bekezdésében említett szakértői értékelési jelentések megvitatása;

p) iránymutatások nyújtása az operatív gyakorlatok konvergenciájának megkönnyítése érdekében e cikk operatív együttműködésre vonatkozó rendelkezéseinek alkalmazása tekintetében.

(4) 2025. január 17-ig, majd azt követően kétévente a CSIRT-hálózat a 40. cikkben említett felülvizsgálat céljából értékeli az operatív együttműködés tekintetében elért előrehaladást, és jelentést fogad el. A jelentés következtetéseket von le és ajánlásokat fogalmaz meg a 19. cikkben említett, a nemzeti CSIRT-ekkel kapcsolatban végzett szakértői értékelések eredményei alapján. Ezt a jelentést be kell nyújtani az együttműködési csoportnak.

(5) A CSIRT-hálózat elfogadja saját eljárási szabályzatát.

(6) A CSIRT-hálózatnak és az EU-CyCLONe-nak meg kell állapodnia az eljárási szabályokról, és azok alapján együtt kell működniük.

16. cikk

Az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (EU-CyCLONe)

(1) A nagyszabású kiberbiztonsági események és válságok operatív szintű összehangolt kezelésének támogatása, valamint a releváns információk tagállamok és az Unió intézményei, szervei, hivatalai és ügynökségei közötti rendszeres cseréjének biztosítása érdekében létrehozásra kerül az EU-CyCLONe.

(2) Az EU-CyCLONe a tagállamok kiberválságok kezelésével foglalkozó hatóságainak képviselőiből, valamint azokban az esetekben, amikor egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági esemény jelentős hatással van vagy valószínűleg jelentős hatást gyakorolhat az ezen irányelv hatálya alá tartozó szolgáltatásokra és tevékenységekre, a Bizottság képviselőiből áll. Más esetekben a Bizottság megfigyelőként vesz részt az EU-CyCLONe tevékenységeiben.

Az ENISA biztosítja az EU-CyCLONe titkárságát, támogatja a biztonságos információcserét, valamint szolgáltatja a tagállamok közötti együttműködés támogatásához szükséges eszközöket, ezáltal biztosítva a biztonságos információcserét.

Az EU-CyCLONe adott esetben az érintett érdekelt felek képviselőit is felkérheti, hogy megfigyelőként részt vegyenek a munkájában.

(3) Az EU-CyCLONe a következő feladatokat látja el:

a) a nagyszabású kiberbiztonsági események és válságok kezelésére való felkészültség szintjének növelése;

b) közös helyzetismeret kialakítása a nagyszabású kiberbiztonsági eseményekkel és válságokkal kapcsolatban;

c) a releváns nagyszabású kiberbiztonsági események és válságok következményeinek és hatásának értékelése, valamint javaslattétel lehetséges mérséklési intézkedésekre;

d) a nagyszabású kiberbiztonsági események és válságok kezelésének összehangolása és az ilyen eseményekkel és válságokkal kapcsolatos politikai szintű döntéshozatal támogatása;

e) valamely érintett tagállam kérésére a 9. cikk (4) bekezdésében említett nagyszabású nemzeti kiberbiztonsági eseményekre és válságokra való reagálási tervek megvitatása.

(4) Az EU-CyCLONe elfogadja eljárási szabályzatát.

(5) Az EU-CyCLONe rendszeresen jelentést tesz az együttműködési csoportnak a nagyszabású kiberbiztonsági események és válságok kezeléséről, valamint a tendenciákról, különös tekintettel az alapvető és fontos szervezetekre gyakorolt hatásukra.

(6) Az EU-CyCLONe együttműködik a CSIRT-hálózattal a 15. cikk (6) bekezdésében előírt megállapodás szerinti eljárási szabályok alapján.

(7) Az EU-CyCLONe 2024. július 17-ig, majd azt követően 18 havonta jelentést nyújt be az Európai Parlamentnek és a Tanácsnak munkája értékeléséről.

17. cikk

Nemzetközi együttműködés

Az Unió adott esetben nemzetközi megállapodásokat köthet az EUMSZ 218. cikkével összhangban harmadik országokkal vagy nemzetközi szervezetekkel, lehetővé téve és megszervezve részvételüket az együttműködési csoport, a CSIRT-hálózat és az EU-CyCLONe egyes tevékenységeiben. E megállapodásoknak meg kell felelniük az uniós adatvédelmi jognak.

18. cikk

Jelentés az uniós kiberbiztonsági helyzetről

(1) Az ENISA a Bizottsággal és az együttműködési csoporttal együttműködve kétéves jelentést ad ki az Unió kiberbiztonságának helyzetéről, és azt benyújtja és bemutatja az Európai Parlamentnek. A jelentést többek között géppel olvasható formátumban is elérhetővé kell tenni, és a következőket tartalmazza:

a) uniós szintű kiberbiztonsági kockázatértékelés, amely figyelembe veszi a kiberfenyegetettségi helyzetet;

b) a köz- és a magánszektorbeli kiberbiztonsági képességek egész Unióban megvalósított fejlesztésének értékelése;

c) a kiberbiztonsági tudatosság és a kiberhigiénia általános szintjének értékelése a polgárok és a szervezetek körében, beleértve a kis- és középvállalkozásokat is;

d) a 19. cikkben említett szakértői értékelések eredményének összesített értékelése;

e) kiberbiztonsági képességek és erőforrások érettségi szintjének összesített értékelése Unió-szerte, beleértve az ágazati szintűeket is, valamint a tagállamok nemzeti kiberbiztonsági stratégiái összehangolásának mértékére vonatkozó összesített értékelés.

(2) A jelentésnek konkrét szakpolitikai ajánlásokat kell tartalmaznia a hiányosságok kezelésére és a kiberbiztonság szintjének növelésére az Unió egész területén, valamint tartalmaznia kell az adott időszakra vonatkozó, az ENISA által az (EU) 2019/881 rendelet 7. cikkének (6) bekezdésével összhangban készített, az eseményekről és kiberfenyegetésekről szóló uniós kiberbiztonsági technikai helyzetjelentésekből származó megállapítások összefoglalását.

(3) Az ENISA a Bizottsággal, az együttműködési csoporttal és a CSIRT-hálózattal együttműködésben kidolgozza a módszertant, ezen belül az (1) bekezdés e) pontjában említett összesített értékelés releváns változóit, például a mennyiségi és minőségi indikátorokat.

19. cikk

Szakértői értékelés

(1) Az együttműködési csoport 2025. január 17-ig a Bizottság, az ENISA és adott esetben a CSIRT-hálózat segítségével kidolgozza a szakértői értékelések módszertanát és szervezeti vonatkozásait a közös tapasztalatokból való tanulás, a kölcsönös bizalom erősítése, a kiberbiztonság egységesen magas szintjének elérése, valamint az ezen irányelv végrehajtásához szükséges tagállami kiberbiztonsági képességek és szakpolitikák fejlesztése céljából. A szakértői értékelésekben való részvétel önkéntes. A szakértői értékelést kiberbiztonsági szakértők végzik. A kiberbiztonsági szakértőket legalább két, az értékelés alatt álló tagállamtól eltérő tagállamnak kell kijelölnie.

A szakértői értékelés a következők legalább egyikéből áll:

a) a 21. és 23. cikkben említett kiberbiztonsági kockázatkezelési intézkedések és jelentéstételi kötelezettségek végrehajtásának szintje;

b) a képességek szintje, ideértve a rendelkezésre álló pénzügyi, technikai és humán erőforrásokat, valamint az illetékes hatóságok feladatai ellátásának hatékonyságát;

c) a CSIRT-ek műveleti képességei;

d) a 37. cikkben említett kölcsönös segítségnyújtás végrehajtási szintje;

e) a 29. cikkben említett kiberbiztonsági információmegosztási megállapodások végrehajtási szintje;

f) határokon vagy ágazatokon átnyúló jellegű konkrét kérdések.

(2) Az (1) bekezdésben említett módszertannak objektív, megkülönböztetéstől mentes, igazságos és átlátható kritériumokat kell tartalmaznia, amelyek alapján a tagállamok kijelölik a szakértői értékelések elvégzésére jogosult kiberbiztonsági szakértőket. Az ENISA és a Bizottság megfigyelőként vesz részt a szakértői értékelésekben.

(3) A tagállamok az (1) bekezdés f) pontjában említett konkrét kérdéseket határozhatnak meg a szakértői értékelés céljából.

(4) Az (1) bekezdésben említett szakértői értékelés megkezdése előtt a tagállamok értesítik a részt vevő tagállamokat a szakértői értékelés hatóköréről, beleértve a (3) bekezdés alapján meghatározott konkrét kérdéseket is.

(5) A szakértői értékelés megkezdése előtt a szakértői értékelés alatt álló tagállamok önértékelést végezhetnek az értékelt szempontokról, és ezt az önértékelést átadhatják a kijelölt kiberbiztonsági szakértőknek. Az együttműködési csoport a Bizottság és az ENISA segítségével megállapítja a tagállamok önértékelésének módszertanát.

(6) A szakértői értékeléseknek részét képezik tényleges vagy virtuális helyszíni látogatások és a helyszínen kívüli információcsere. A jó együttműködés elvével összhangban a szakértői értékelés alatt álló tagállam – a bizalmas vagy minősített adatok védelmét szolgáló nemzeti vagy uniós jog sérelme nélkül, illetve az alapvető állami funkciók, például a nemzetbiztonság védelmének sérelme nélkül – a kijelölt kiberbiztonsági szakértőknek megadja az értékeléshez szükséges információkat. Az együttműködési csoport a Bizottsággal és az ENISA-val együttműködve megfelelő magatartási kódexeket dolgoz ki a kijelölt kiberbiztonsági szakértők munkamódszereinek alátámasztására. A szakértői értékelés során kapott információkat kizárólag erre a célra lehet felhasználni. A szakértői értékelésben részt vevő kiberbiztonsági szakértők semmilyen, az adott szakértői értékelés során kapott érzékeny vagy bizalmas információt nem közölhetnek harmadik személyekkel.

(7) A valamely tagállamban szakértői értékelésnek alávetett szempontokkal azonos szempontokat nem lehet az említett tagállamban további szakértői értékelésnek alávetni a szakértői értékelés lezárását követő két éven belül, kivéve, ha a tagállam azt kéri vagy arról az együttműködési csoport javaslata nyomán megállapodás született.

(8) A tagállamok biztosítják, hogy bármely, a kijelölt kiberbiztonsági szakértőket érintő összeférhetetlenség kockázatát a szakértői értékelés megkezdése előtt jelezzék a többi tagállamnak, az együttműködési csoportnak, a Bizottságnak és az ENISA-nak. A szakértői értékelés alatt álló tagállam a kijelölő tagállammal közölt, kellően megindokolt okokból kifogást emelhet egyes kiberbiztonsági szakértők kijelölésével szemben.

(9) A szakértői értékelésekben részt vevő kiberbiztonsági szakértők jelentést készítenek a szakértői értékelések eredményeiről és következtetéseiről. A szakértői értékelés alatt álló tagállamok észrevételeket tehetnek a rájuk vonatkozó jelentéstervezetekre vonatkozóan, és ezeket az észrevételeket csatolni kell a jelentésekhez. A jelentések ajánlásokat tartalmaznak, amelyek lehetővé teszik a helyzet javítását a szakértői értékelésben érintett szempontok területén. A jelentéseket adott esetben be kell nyújtani az együttműködési csoportnak és a CSIRT-hálózatnak. A szakértői értékelés alatt álló tagállam dönthet úgy, hogy jelentését vagy annak szerkesztett változatát nyilvánosan hozzáférhetővé teszi.

IV. FEJEZET

KIBERBIZTONSÁGI KOCKÁZATKEZELÉSI INTÉZKEDÉSEK ÉS JELENTÉSTÉTELI KÖTELEZETTSÉG

20. cikk

Irányítás

(1) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek vezető testületei jóváhagyják az e szervezetek által a 21. cikknek való megfelelés érdekében tett kiberbiztonsági kockázatkezelési intézkedéseket, felügyeljék annak végrehajtását és felelősségre vonhatók legyenek az említett cikknek a szervezetek általi megsértéséért.

E bekezdés alkalmazása nem érinti a közintézményekre alkalmazandó felelősségi szabályokat és a köztisztviselők és a megválasztott vagy kinevezett tisztviselők felelősségét előíró nemzeti jogot.

(2) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek vezető testületeinek tagjai számára kötelező legyen a képzéseken való részvétel, és ösztönzik az alapvető és fontos szervezeteket arra, hogy munkavállalóik számára rendszeresen hasonló képzéseket biztosítsanak annak érdekében, hogy elsajátítsák a kockázatok azonosításához és a kiberbiztonsági kockázatkezelési gyakorlatok, valamint azoknak a szervezet által nyújtott szolgáltatásokra gyakorolt hatása értékeléséhez szükséges tudást és készségeket.

21. cikk

A kiberbiztonsági kockázatkezelési intézkedések

(1) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek megfelelő és arányos technikai, operatív és szervezési intézkedéseket hozzanak annak érdekében, hogy kezeljék azokat a kockázatokat, amelyek a működésük vagy szolgáltatásaik nyújtása során használt hálózati és információs rendszerek biztonságát fenyegetik, és megelőzzék vagy minimalizálják az eseményeknek a szolgáltatásaik igénybe vevőire és más szolgáltatásokra gyakorolt hatásait.

Figyelembe véve a legkorszerűbb és adott esetben a vonatkozó európai és nemzetközi szabványokat, valamint a végrehajtás költségeit, az első albekezdésben említett intézkedéseknek biztosítaniuk kell a hálózati és információs rendszerek biztonságának a felmerülő kockázatoknak megfelelő szintjét. Ezen intézkedések arányosságának értékelésekor megfelelően figyelembe kell venni a szervezet kockázatoknak való kitettségének mértékét, a szervezet méretét és az események előfordulásának valószínűségét, valamint azok súlyosságát, beleértve társadalmi és gazdasági hatásukat is.

(2) Az (1) bekezdésben említett intézkedéseknek egy minden veszélyre kiterjedő megközelítésen kell alapulniuk, amelynek célja a hálózati és információs rendszerek, valamint e rendszerek fizikai környezetének védelme az eseményekkel szemben, és legalább a következőket kell magukban foglalniuk:

a) kockázatelemzési és az informatikai rendszerek biztonságára vonatkozó szabályzatok;

b) eseménykezelés;

c) üzletmenet-folytonosság, például tartalékrendszerek kezelése, valamint katasztrófa utáni helyreállítás és válságkezelés;

d) az ellátási lánc biztonsága, ideértve az egyes szervezetek és közvetlen beszállítóik vagy szolgáltatóik közötti kapcsolatok biztonságával kapcsolatos szempontokat;

e) biztonság a hálózati és információs rendszerek beszerzésében, fejlesztésében és karbantartásában, beleértve a sérülékenységek kezelését és közzétételét;

f) szabályzatok és eljárások a kiberbiztonsági kockázatkezelési intézkedések hatékonyságának értékelésére;

g) alapvető kiberhigiéniai gyakorlatok és kiberbiztonsági képzés;

h) a kriptográfia és adott esetben a titkosítás használatára vonatkozó szabályzatok és eljárások;

i) humánerőforrás-biztonság, hozzáférés-ellenőrzési szabályzatok és eszközgazdálkodás;

j) adott esetben többtényezős hitelesítési vagy folyamatos hitelesítési megoldások, biztonságos hang-, video- és szöveges kommunikáció, valamint biztonságos vészhelyzeti kommunikációs rendszerek használata a szervezeten belül.

(3) A tagállamok biztosítják, hogy a szervezetek – amikor azt mérlegelik, hogy az e cikk (2) bekezdésének d) pontjában említett intézkedések közül melyek megfelelők – figyelembe vegyék az egyes közvetlen beszállítókra és szolgáltatókra jellemző sérülékenységeket, valamint a beszállítóik és szolgáltatóik termékeinek és kiberbiztonsági gyakorlatainak – többek között biztonságos fejlesztési eljárásaiknak – az általános minőségét. A tagállamok biztosítják továbbá, hogy a szervezetek – amikor azt mérlegelik, hogy az említett pontban említett intézkedések közül melyek megfelelők – kötelesek legyenek figyelembe venni a 22. cikk (1) bekezdésének megfelelően a kritikus ellátási láncok vonatkozásában elvégzett összehangolt biztonsági kockázatértékelések eredményeit.

(4) A tagállamok biztosítják, hogy az a szervezet, amely megállapítja, hogy nem felel meg a (2) bekezdésben előírt intézkedéseknek, indokolatlan késedelem nélkül meghozza az összes szükséges, megfelelő és arányos korrekciós intézkedést.

(5) 2024. október 17-ig a Bizottság végrehajtási jogi aktusokat fogad el, amelyekben meghatározza a (2) bekezdésben említett intézkedések technikai és módszertani követelményeit a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatói, valamint a bizalmi szolgáltatók tekintetében.

A Bizottság végrehajtási jogi aktusokat fogadhat el, amelyekben az e bekezdés első albekezdésében említettektől eltérő alapvető és fontos szervezetek tekintetében meghatározza a (2) bekezdésben említett intézkedések technikai és módszertani követelményeit, valamint szükség esetén ágazati követelményeit.

Az e bekezdés első és második albekezdésében említett végrehajtási jogi aktusok előkészítése során a Bizottság a lehető legnagyobb mértékben követi az európai és nemzetközi szabványokat, valamint a vonatkozó műszaki előírásokat. A Bizottság a 14. cikk (4) bekezdésének e) pontjával összhangban megosztja a szakértelmet és együttműködik az együttműködési csoporttal és az ENISA-val a végrehajtási jogi aktusok tervezetével kapcsolatban.

Ezeket a végrehajtási jogi aktusokat a 39. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

22. cikk

A kritikus ellátási láncok uniós szintű összehangolt biztonsági kockázatértékelése

(1) Az együttműködési csoport a Bizottsággal és az ENISA-val együttműködve összehangolt biztonsági kockázatértékeléseket végezhet a kritikus IKT-szolgáltatások, IKT-rendszerek vagy IKT-termékek ellátási láncai tekintetében, figyelembe véve a technikai, és adott esetben a nem technikai kockázati tényezőket.

(2) A Bizottság az együttműködési csoporttal és az ENISA-val, valamint adott esetben az érdekelt felekkel folytatott konzultációt követően meghatározza azokat a kritikus IKT-szolgáltatásokat, IKT-rendszereket vagy IKT-termékeket, amelyekre az (1) bekezdésben említett összehangolt biztonsági kockázatértékelés vonatkozhat.

23. cikk

Jelentéstételi kötelezettség

(1) Minden tagállam biztosítja, hogy az alapvető és fontos szervezetek a (4) bekezdéssel összhangban indokolatlan késedelem nélkül értesítsék a CSIRT-jét vagy adott esetben az illetékes hatóságát minden olyan eseményről, amely jelentős hatással van a (3) bekezdésben említett szolgáltatásaik nyújtására (jelentős esemény). Adott esetben az érintett szervezetek indokolatlan késedelem nélkül értesítik a szolgáltatásaikat igénybe vevőket azon jelentős eseményekről, amelyek valószínűleg hátrányosan érintik az említett szolgáltatások nyújtását. Minden tagállam biztosítja, hogy ezek a szervezetek jelentsenek többek között minden olyan információt, amely lehetővé teszi a CSIRT vagy adott esetben az illetékes hatóság számára, hogy meghatározza az esemény határokon átnyúló hatásait. Pusztán a bejelentés következtében a bejelentő szervezetet többletfelelősség nem terhelheti.

Amennyiben az érintett szervezetek az első albekezdés szerint jelentős eseményről értesítik az illetékes hatóságot, a tagállam biztosítja, hogy az említett illetékes hatóság a kézhezvételt követően továbbítsa az értesítést a CSIRT-nek.

Határokon átnyúló vagy ágazatközi jelentős esemény esetén a tagállamok biztosítják, hogy egyedüli kapcsolattartó pontjaik kellő időben megkapják a (4) bekezdéssel összhangban bejelentett releváns információkat.

(2) Adott esetben a tagállamok biztosítják, hogy az alapvető és a fontos szervezetek indokolatlan késedelem nélkül közöljék a jelentős kiberfenyegetés által potenciálisan érintett szolgáltatásaik igénybe vevőivel azon intézkedéseket, illetve fenyegetést orvosló lehetőségeket, amelyeket a szolgáltatások igénybe vevői a fenyegetésre válaszul maguk megtehetnek, illetve amelyekkel élhetnek. Adott esetben a szervezetek az igénybe vevőket magáról a jelentős kiberfenyegetésről is tájékoztatják.

(3) Egy esemény akkor tekintendő jelentősnek, ha:

a) súlyos működési zavart okozott vagy képes okozni a szolgáltatásokban, vagy pénzügyi veszteséget okozott az érintett szervezetnek;

b) az esemény jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett vagy képes érinteni.

(4) A tagállamok biztosítják, hogy az (1) bekezdés szerinti bejelentés céljából az érintett szervezetek benyújtsanak a CSIRT-nek vagy adott esetben az illetékes hatóságnak:

a) indokolatlan késedelem nélkül és minden esetben a jelentős eseményről való tudomásszerzéstől számított 24 órán belül egy korai előrejelzést, amelyben adott esetben fel kell tüntetni, hogy a jelentős eseményt vélhetően jogellenes vagy rosszindulatú cselekmény okozta-e és hogy lehet-e határokon átnyúló hatása;

b) indokolatlan késedelem nélkül és minden esetben a jelentős eseményről való tudomásszerzéstől számított 72 órán belül egy eseménybejelentést, amely adott esetben aktualizálja az a) pontban említett információkat, és tartalmazza a jelentős esemény első értékelését, beleértve annak súlyosságát és hatását, valamint – amennyiben rendelkezésre állnak – a fertőzöttségi mutatókat;

c) a CSIRT vagy adott esetben az illetékes hatóság kérésére közbenső helyzetjelentést;

d) zárójelentést, legkésőbb a b) pont szerinti eseménybejelentés benyújtását követő egy hónapon belül, amely tartalmazza a következőket:

   i. az esemény részletes leírása, beleértve annak súlyosságát és hatását;

   ii. az eseményt valószínűleg kiváltó fenyegetés vagy kiváltó ok típusa;

   iii. alkalmazott és folyamatban lévő mérséklési intézkedések;

   iv. adott esetben az esemény határokon átnyúló hatása;

e) abban az esetben, ha a d) pontban említett zárójelentés benyújtásának időpontjában folyamatban van az esemény, a tagállamok biztosítják, hogy az említett időpontban az érintett szervezetek benyújtsanak egy jelentést az addig elért eredményekről, az esemény általuk való kezelését követő egy hónapon belül pedig egy zárójelentést.

Az első albekezdés b) pontjától eltérve a bizalmi szolgáltató indokolatlan késedelem nélkül és minden esetben a jelentős eseményről való tudomásszerzést követő 24 órán belül értesíti a CSIRT-et vagy adott esetben az illetékes hatóságot a bizalmi szolgáltatásai nyújtására hatást gyakorló jelentős eseményekről.

(5) A CSIRT vagy az illetékes hatóság haladéktalanul és – ha lehetséges – a (4) bekezdés a) pontjában említett korai előrejelzés kézhezvételétől számított 24 órán belül választ ad – többek között egy kezdeti visszajelzést küld a jelentős eseményről – a bejelentő szervezetnek, valamint – a szervezet kérésére – útmutatást vagy operatív tanácsokat nyújt a lehetséges mérséklési intézkedések végrehajtásáról. Ha nem a CSIRT az (1) bekezdésben említett bejelentés első címzettje, az útmutatást az illetékes hatóság a CSIRT-tel együttműködve nyújtja. A CSIRT további technikai támogatást nyújt, ha az érintett szervezet ezt kéri. Ha a jelentős esemény gyaníthatóan büntetőjogi természetű, a CSIRT vagy az illetékes hatóság a jelentős esemény bűnüldöző hatóságoknak történő bejelentésére vonatkozóan is útmutatást ad.

(6) Adott esetben, és különösen, ha a jelentős esemény két vagy több tagállamot érint, a CSIRT, az illetékes hatóság vagy az egyedüli kapcsolattartó pont haladéktalanul tájékoztatja a jelentős eseményről a többi érintett tagállamot és az ENISA-t. Ezeknek az információknak tartalmazniuk kell a (4) bekezdéssel összhangban kapott információk típusát. Ennek során a CSIRT-nek, az illetékes hatóságnak vagy az egyedüli kapcsolattartó pontnak az uniós vagy nemzeti joggal összhangban meg kell óvniuk a szervezet biztonsági és üzleti érdekeit, valamint a benyújtott információk titkosságát.

(7) Ha a jelentős esemény megelőzéséhez vagy egy folyamatban lévő jelentős esemény kezeléséhez lakossági figyelemfelkeltés szükséges, vagy ha a jelentős esemény nyilvánosságra hozatala egyébként közérdek, a tagállam CSIRT-je vagy adott esetben az illetékes hatósága, és adott esetben a többi érintett tagállam CSIRT-jei vagy illetékes hatóságai az érintett szervezettel folytatott konzultációt követően tájékoztathatják a nyilvánosságot a jelentős eseményről, vagy ezt előírhatják a szervezet számára.

(8) A CSIRT vagy az illetékes hatóság kérésére az egyedüli kapcsolattartó pont az (1) bekezdés alapján kapott bejelentéseket továbbítja a többi érintett tagállam egyedüli kapcsolattartó pontjának.

(9) Az egyedüli kapcsolattartó pont háromhavonta összefoglaló jelentést nyújt be az ENISA-nak, amely névtelen és összesített adatokat tartalmaz az e cikk (1) bekezdésével és a 30. cikkel összhangban bejelentett jelentős eseményekről, eseményekről, kiberfenyegetésekről és majdnem bekövetkezett eseményekről. Az összehasonlítható információk szolgáltatásához való hozzájárulás érdekében az ENISA technikai útmutatást fogadhat el az összefoglaló jelentésbe belefoglalandó információk paramétereiről. Az ENISA hathavonta tájékoztatja az együttműködési csoportot és a CSIRT-hálózatot a beérkezett bejelentésekről tett megállapításairól.

(10) A CSIRT-ek vagy adott esetben az illetékes hatóságok az (EU) 2022/2557 irányelv alapján kritikus szervezetként azonosított szervezetek által az e cikk (1) bekezdésével és a 30. cikkel összhangban bejelentett jelentős eseményekről, eseményekről, kiberfenyegetésekről és a majdnem bekövetkezett eseményekről tájékoztatják az (EU) 2022/2557 irányelv szerinti illetékes hatóságokat.

(11) A Bizottság végrehajtási jogi aktusokat fogadhat el, amelyek meghatározzák az információk típusát, valamint az e cikk (1) bekezdése és a 30. cikk alapján benyújtott bejelentés és az e cikk (2) bekezdése alapján benyújtott értesítés formátumát és eljárását.

2024. október 17-ig a Bizottság a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, valamint az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatói tekintetében végrehajtási jogi aktusokat fogad el, amelyekben részletesebben meghatározza azokat az eseteket, amikor egy esemény a (3) bekezdésben említettek szerint jelentősnek tekintendő. A Bizottság elfogadhat ilyen végrehajtási jogi aktusokat más alapvető és fontos szervezetek tekintetében is.

A Bizottság a 14. cikk (4) bekezdésének e) pontjával összhangban megosztja a szakértelmet és együttműködik az együttműködési csoporttal az e bekezdés első és második albekezdésében említett végrehajtási jogi aktusok tervezetével kapcsolatban.

Ezeket a végrehajtási jogi aktusokat a 39. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

24. cikk

Az európai kiberbiztonsági tanúsítási rendszerek használata

(1) A 21. cikk egyes követelményeinek való megfelelés igazolása érdekében a tagállamok előírhatják az alapvető és fontos szervezetek számára, hogy bizonyos – az alapvető vagy fontos szervezet által fejlesztett, vagy harmadik felektől beszerzett – az (EU) 2019/881 rendelet 49. cikke alapján elfogadott európai kiberbiztonsági tanúsítási rendszerek által tanúsított IKT-termékeket, IKT-szolgáltatásokat és IKT-folyamatokat használjanak. Ezenkívül a tagállamok ösztönzik az alapvető és fontos szervezeteket, hogy vegyenek igénybe minősített bizalmi szolgáltatásokat.

(2) A Bizottság felhatalmazást kap arra, hogy a 38. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el ezen irányelv kiegészítésére, meghatározva, hogy az alapvető és fontos szervezetek mely kategóriái számára kell előírni, hogy bizonyos, az (EU) 2019/881 rendelet 49. cikke alapján elfogadott európai kiberbiztonsági tanúsítási rendszerek keretében tanúsított IKT-termékeket, IKT-szolgáltatásokat és IKT-folyamatokat használjanak. Az említett felhatalmazáson alapuló jogi aktusokat abban az esetben kell elfogadni, ha elégtelen kiberbiztonsági szintet állapítanak meg, és azoknak végrehajtási időszakot kell előírniuk.

Az ilyen felhatalmazáson alapuló jogi aktusok elfogadása előtt a Bizottság az (EU) 2019/881 rendelet 56. cikkével összhangban hatásvizsgálatot végez és konzultációkat folytat.

(3) Amennyiben nem áll rendelkezésre megfelelő európai kiberbiztonsági tanúsítási rendszer e cikk (2) bekezdésének céljára, a Bizottság az együttműködési csoporttal és az európai kiberbiztonsági tanúsítási csoporttal folytatott konzultációt követően felkérheti az ENISA-t, hogy készítsen egy javasolt tanúsítási rendszert az (EU) 2019/881 rendelet 48. cikkének (2) bekezdése alapján.

25. cikk

Szabványosítás

(1) A 21. cikk (1) és (2) bekezdése konvergens végrehajtásának előmozdítása érdekében a tagállamok – anélkül, hogy előírnák vagy előnyben részesítenék egy adott típusú technológia alkalmazását – ösztönzik a hálózati és információs rendszerek biztonsága tekintetében releváns európai és nemzetközi szabványok és műszaki előírások alkalmazását.

(2) Az ENISA a tagállamokkal együttműködve és adott esetben az érintett érdekelt felekkel folytatott konzultációt követően tanácsokat és iránymutatásokat dolgoz ki az (1) bekezdéssel összefüggésben mérlegelendő technikai területekről, valamint a már meglévő szabványokról – beleértve a nemzeti szabványokat is –, amelyek lehetővé tennék az említett területek lefedését.

V. FEJEZET

JOGHATÓSÁG ÉS NYILVÁNTARTÁS

26. cikk

Joghatóság és területi elv

(1) Az ezen irányelv hatálya alá tartozó szervezeteket a letelepedésük szerinti tagállam joghatósága alá tartozónak kell tekinteni, kivéve:

a) a nyilvános elektronikus hírközlő hálózatok szolgáltatóit vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatókat, amelyeket úgy kell tekinteni, hogy a szolgáltatásnyújtásuk helye szerinti tagállam joghatósága alá tartoznak;

b) azokat a DNS-szolgáltatókat, legfelső szintű doménnév-nyilvántartókat és doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteket, felhőszolgáltatókat, adatközpont-szolgáltatókat, tartalomszolgáltató hálózati szolgáltatókat, irányított szolgáltatókat és irányított biztonsági szolgáltatókat, valamint az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatóit, amelyeket annak a tagállamnak a joghatósága alá tartozónak kell tekinteni, amelyben a (2) bekezdés alapján az Unióban üzleti tevékenységük fő helye található;

c) azokat a közigazgatási szerveket, amelyek az azokat létrehozó tagállam joghatósága alá tartozónak kell tekinteni.

(2) Ezen irányelv alkalmazásában úgy kell tekinteni, hogy az (1) bekezdés b) pontjában említett szervezet üzleti tevékenységének fő helye az Unióban abban a tagállamban van, ahol a kiberbiztonsági kockázatkezelési intézkedésekkel kapcsolatos döntéseket túlnyomórészt meghozzák. Ha ilyen tagállam nem határozható meg, vagy az ilyen döntéseket nem az Unióban hozzák meg, akkor úgy kell tekinteni, hogy az üzleti tevékenység fő helye abban a tagállamban található, ahol a kiberbiztonsági műveleteket végzik. Ha ilyen tagállam nem határozható meg, akkor az üzleti tevékenység fő helyét abban a tagállamban levőnek kell tekinteni, ahol az érintett szervezetnek az Unióban a legmagasabb munkavállalói létszámmal rendelkező telephelye van.

(3) Ha az (1) bekezdés b) pontjában említett szervezet nem az Unióban letelepedett, de az Unión belül kínál szolgáltatásokat, ki kell jelölnie egy képviselőt az Unióban. A képviselőnek azon tagállamok valamelyikében kell letelepedettnek lennie, ahol a szolgáltatásokat kínálják. Az ilyen szervezetet a képviselő letelepedése szerinti tagállam joghatósága alá tartozónak kell tekinteni. E bekezdés alapján az Unióban kijelölt képviselő hiányában bármely olyan tagállam, amelyben a szervezet szolgáltatásokat nyújt, jogi lépéseket tehet a szervezet ellen ezen irányelv megsértése miatt.

(4) A képviselő (1) bekezdés b) pontjában említett szervezet általi kijelölése nem érinti azokat a jogi lépéseket, amelyek maga a szervezet ellen kezdeményezhetők.

(5) Amennyiben egy tagállamhoz kölcsönös segítségnyújtás iránti megkeresés érkezik az (1) bekezdés b) pontjában említett szervezettel kapcsolatban, a megkeresés keretein belül felügyeleti és végrehajtási intézkedéseket hozhat azon érintett szervezettel kapcsolatban, amely a területén szolgáltatásokat nyújt vagy amelynek a hálózati és információs rendszere a területén található.

27. cikk

Az alapvető és fontos szervezetek nyilvántartása

(1) Az ENISA az egyedüli kapcsolattartó ponttól a (4) bekezdéssel összhangban kapott információk alapján létrehozza és fenntartja a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók és az irányított biztonsági szolgáltatók, valamint az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatói nyilvántartását. Az ENISA kérésre hozzáférést enged az illetékes hatóságok számára az említett nyilvántartáshoz, ugyanakkor biztosítva adott esetben az információk bizalmas jellegének védelmét.

(2) A tagállamok előírják az (1) bekezdésben említett szervezetek számára, hogy 2025. január 17-ig nyújtsák be a következő információkat az illetékes hatóságoknak:

a) a szervezet neve;

b) adott esetben az I. vagy II. mellékletben említett érintett ágazat, alágazat és szervezettípus;

c) a szervezet üzleti tevékenysége fő helyének és egyéb Unión belüli jogszerű telephelyének, vagy ha az Unióban nem letelepedett, a 26. cikk (3) bekezdése szerint kijelölt képviselőjének a címe;

d) a szervezet és adott esetben a 26. cikk (3) bekezdése szerint kijelölt képviselőjének naprakész elérhetőségei, beleértve e-mail-címét és telefonszámát is;

e) azok a tagállamok, ahol a szervezet szolgáltatásokat nyújt; továbbá

f) a szervezet IP-tartományai.

(3) A tagállamok biztosítják, hogy az (1) bekezdésben említett szervezetek a (2) bekezdés alapján benyújtott adatokban bekövetkezett minden változást haladéktalanul, és minden esetben a változás időpontjától számított három hónapon belül bejelentsenek az illetékes hatóságnak.

(4) A (2) és (3) bekezdésben említett információk – a (2) bekezdés f) pontjában említett információkat ide nem értve – kézhezvételét követően az érintett tagállam egyedüli kapcsolattartó pontja indokolatlan késedelem nélkül továbbítja ezeket az információkat az ENISA-nak.

(5) Az e cikk (2) és (3) bekezdésében említett információkat adott esetben a 3. cikk (4) bekezdésének negyedik albekezdésében említett nemzeti mechanizmus révén kell benyújtani.

28. cikk

A doménnevek nyilvántartási adatainak adatbázisa

(1) A DNS biztonságához, stabilitásához és rezilienciájához való hozzájárulás céljából a tagállamok előírják, hogy a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek – a személyes adatnak minősülő adatok tekintetében az uniós adatvédelmi jogszabályoknak megfelelően – a kellő gondossággal, egy erre kijelölt adatbázisban gyűjtsék és kezeljék a pontos és teljes doménnév-nyilvántartási adatokat.

(2) A tagállamok az (1) bekezdés alkalmazásában előírják, hogy a doménnév-nyilvántartási adatok adatbázisai tartalmazzák a szükséges információkat a doménnevek tulajdonosai és a legfelső szintű domének alatt bejegyzett doménneveket kezelő kapcsolattartó pontok azonosításához és a velük való kapcsolatfelvételhez. Az ilyen információk magukban foglalják:

a) a doménnevet;

b) a nyilvántartásba vétel időpontját;

c) a regisztráló nevét, kapcsolattartási e-mail címét és telefonszámát;

d) a doménnevet kezelő kapcsolattartó pont kapcsolattartási e-mail címét és telefonszámát, amennyiben azok eltérnek a regisztrálóétól.

(3) A tagállamok előírják, hogy a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek rendelkezzenek szabályzatokkal és eljárásokkal – többek között ellenőrzési eljárásokkal – annak biztosítására, hogy az (1) bekezdésben említett adatbázisok pontos és teljes információkat tartalmazzanak. A tagállamok előírják, hogy az említett szabályzatokat és eljárásokat nyilvánosan hozzáférhetővé kell tenni.

(4) A tagállamok előírják, hogy a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek a doménnév nyilvántartásba vétele után indokolatlan késedelem nélkül nyilvánosan hozzáférhetővé tegyék azokat a doménnév-nyilvántartási adatokat, amelyek nem személyes adatok.

(5) A tagállamok előírják a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek számára, hogy a jogosult hozzáférés-igénylők jogszerű és kellően indokolt kérésére az uniós adatvédelmi jogszabályokkal összhangban betekintést biztosítsanak meghatározott doménnév-nyilvántartási adatokba. A tagállamok előírják a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek számára, hogy indokolatlan késedelem nélkül – de minden esetben a kézhezvételtől számított 72 órán belül – megválaszoljanak minden hozzáférési kérelmet. A tagállamok előírják, hogy az ilyen adatok nyilvánosságra hozatalára vonatkozó szabályzatokat és eljárásokat nyilvánosan hozzáférhetővé kell tenni.

(6) Az (1)–(5) bekezdésben megállapított kötelezettségeknek való megfelelés nem eredményezheti a doménnév-nyilvántartási adatok gyűjtésének megkettőzését. E célból a tagállamok előírják a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek számára az egymással való együttműködést.

VI. FEJEZET

INFORMÁCIÓMEGOSZTÁS

29. cikk

Kiberbiztonsági információmegosztási megállapodások

(1) A tagállamok biztosítják, hogy az ezen irányelv hatálya alá tartozó szervezetek és adott esetben az ezen irányelv hatálya alá nem tartozó egyéb szervezetek önkéntes alapon megoszthassák egymással a vonatkozó kiberbiztonsági információkat, ideértve a kiberfenyegetésekre, a majdnem bekövetkezett eseményekre, a sérülékenységekre, a technikákra és eljárásokra, a fertőzöttségi mutatókra, az ellenséges taktikákra, az elkövetővel kapcsolatos információkra, a kiberbiztonsági figyelmeztetésekre, valamint a kibertámadások észlelésére szolgáló biztonságieszköz-konfigurációkra vonatkozó ajánlásokkal kapcsolatos információkat, amennyiben az említett információmegosztás:

a) célja, hogy megelőzze, észlelje az eseményeket, reagáljon azokra vagy az eseményeket követően helyreállítsa a működést, illetve mérsékelje az események hatását;

b) növeli a kiberbiztonság szintjét, különösen azáltal, hogy felhívja a figyelmet a kiberfenyegetésekre, korlátozza vagy gátolja az ilyen fenyegetések terjedési képességét, támogatja a védelmi képességek széles skáláját, a sérülékenység elhárítását és nyilvánosságra hozatalát, a fenyegetésészlelési, -korlátozási és -megelőzési technikákat, a mérséklési stratégiákat vagy az elhárítási és helyreállítási szakaszt, vagy előmozdítja az állami szervek és magánszervezetek közötti együttműködésen alapuló, kiberfenyegetésekkel kapcsolatos kutatásokat.

(2) A tagállamok biztosítják, hogy az információkat megosszák az alapvető és fontos szervezetek és adott esetben beszállítóik és szolgáltatóik közösségeiben. Az említett megosztást kiberbiztonsági információmegosztási megállapodások útján kell végrehajtani a megosztott információk potenciálisan érzékeny jellegét tiszteletben tartva.

(3) A tagállamok elősegítik az e cikk (2) bekezdésében említett kiberbiztonsági információmegosztási megállapodások létrehozását. Az ilyen megállapodások meghatározhatják az információmegosztási megállapodások működési elemeit – ideértve dedikált IKT-platformok és automatizálási eszközök használatát –, tartalmát és feltételeit. A tagállamok a hatóságok említett megállapodásokban való részvétele részleteinek meghatározása során feltételeket szabhatnak az illetékes hatóságok vagy a CSIRT-ek által rendelkezésre bocsátott információkra vonatkozóan. A tagállamok segítséget nyújtanak az említett megállapodások alkalmazásához az 7. cikk (2) bekezdésének g) pontjában említett szakpolitikájukkal összhangban.

(4) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek az említett megállapodások megkötésekor értesítsék az illetékes hatóságokat a (2) bekezdésben említett kiberbiztonsági információmegosztási megállapodásokban való részvételükről, vagy adott esetben az említett megállapodások felmondásáról, a felmondás hatálybalépésekor.

(5) Az ENISA bevált gyakorlatok megosztásával és útmutatás nyújtásával segítséget nyújt a (2) bekezdésben említett kiberbiztonsági információmegosztási megállapodások létrehozásához.

30. cikk

A releváns információk önkéntes bejelentése

(1) A tagállamok biztosítják, hogy a 23. cikkben előírt értesítési kötelezettségen túlmenően a CSIRT-ekhez vagy adott esetben az illetékes hatóságokhoz önkéntes alapon be lehessen nyújtani bejelentéseket az alábbiak által:

a) alapvető és fontos szervezetek az események, a kiberfenyegetések és a majdnem bekövetkezett események tekintetében;

b) az a) pontban említettektől eltérő szervezetek – függetlenül attól, hogy ezen irányelv hatálya alá tartoznak-e – a jelentős események, a kiberfenyegetések és a majdnem bekövetkezett események tekintetében.

(2) A tagállamok az e cikk (1) bekezdésében említett bejelentéseket a 23. cikkben megállapított eljárásnak megfelelően dolgozzák fel. A tagállamok előnyben részesíthetik a kötelező bejelentések feldolgozását az önkéntes bejelentésekkel szemben.

Szükség esetén a CSIRT-ek és adott esetben az illetékes hatóságok átadják az egyedüli kapcsolattartó pontoknak az e cikk alapján kapott bejelentésekre vonatkozó információkat, biztosítva ugyanakkor a bejelentő szervezet által nyújtott információk bizalmas kezelését és megfelelő védelmét. A bűncselekmények megelőzésének, kivizsgálásának, felderítésének és büntetőeljárás alá vonásának sérelme nélkül, az önkéntes adatszolgáltatás nem eredményezhet a bejelentő szervezetre nézve olyan további kötelezettségeket, amelyek nem vonatkoztak volna rá, ha nem nyújtja be a bejelentést.

VII. FEJEZET

FELÜGYELET ÉS VÉGREHAJTÁS

31. cikk

A felügyelet és a végrehajtás általános szempontjai

(1) A tagállamok biztosítják, hogy az illetékes hatóságaik ténylegesen felügyeljék és megtegyék az ezen irányelvnek való megfelelés biztosításához szükséges intézkedéseket.

(2) A tagállamok engedélyezhetik az illetékes hatóságaik számára, hogy rangsorolják a felügyeleti feladatokat. Az ilyen rangsorolásnak kockázatalapú megközelítésen kell alapulnia. Ennek érdekében a 32. és 33. cikkben előírt felügyeleti feladataik ellátása keretében az illetékes hatóságok kialakíthatnak olyan felügyeleti módszereket, amelyek lehetővé teszik e feladatok kockázatalapú megközelítés alapján történő rangsorolását.

(3) Az illetékes hatóságok szorosan együttműködnek az (EU) 2016/679 rendelet szerinti felügyeleti hatóságokkal a személyes adatok megsértését eredményező események kezelése során, a felügyeleti hatóságok említett rendelet szerinti illetékességének és feladatainak sérelme nélkül.

(4) A nemzeti jogszabályi és intézményi keretek sérelme nélkül, a tagállamok biztosítják, hogy a közigazgatási szervek ezen irányelvnek való megfelelésének felügyelete és az ezen irányelv megsértésére tekintettel előírt végrehajtási intézkedések során az illetékes hatóságok rendelkezzenek az ahhoz szükséges megfelelő hatáskörökkel, hogy a felügyelet hatálya alá vont közigazgatási szervekkel szemben működési szempontból függetlenül végezhessék el ezen feladataikat. A tagállamok a nemzeti jogszabályi és intézményi keretekkel összhangban határozhatnak megfelelő, arányos és hatékony felügyeleti és végrehajtási intézkedések előírásáról e szervezetekkel szemben.

32. cikk

Az alapvető szervezetekre vonatkozó felügyeleti és végrehajtási intézkedések

(1) A tagállamok biztosítják, hogy az alapvető szervezetekre az ezen irányelvben megállapított kötelezettségek tekintetében előírt felügyeleti vagy végrehajtási intézkedések hatékonyak, arányosak és visszatartó erejűek legyenek, figyelembe véve az egyes konkrét esetek körülményeit.

(2) A tagállamok biztosítják, hogy az illetékes hatóságok az alapvető szervezetekkel kapcsolatos felügyeleti feladataik ellátása során hatáskörrel rendelkezzenek arra, hogy ezeknél a szervezeteknél elvégezzék legalább az alábbiakat:

a) képzett szakemberek által végrehajtott helyszíni ellenőrzések és távoli felügyeleti intézkedések, ideértve a véletlenszerű ellenőrzéseket is;

b) egy független szerv vagy illetékes hatóság által végzett, rendszeres és célzott biztonsági ellenőrzések;

c) eseti ellenőrzések, többek között ha azt jelentős esemény vagy ezen irányelvnek az alapvető szervezet általi megsértése indokolja;

d) objektív, megkülönböztetéstől mentes, méltányos és átlátható kockázatértékelési kritériumokon alapuló biztonsági vizsgálatok, amennyiben szükséges, az érintett szervezet együttműködésével;

e) az érintett szervezet által elfogadott kiberbiztonsági kockázatkezelési intézkedések –többek között a dokumentált kiberbiztonsági szabályzatok – értékeléséhez, valamint az információk illetékes hatóságok részére való, a 27. cikk alapján történő bejelentésére vonatkozó kötelezettség betartásának értékeléséhez szükséges tájékoztatás kérése;

f) a felügyeleti feladataik ellátásához szükséges adatokhoz, dokumentumokhoz és információkhoz való hozzáférés iránti kérelmek;

g) a kiberbiztonsági szabályzatok végrehajtására vonatkozó bizonyítékok, például a minősített ellenőr által végzett biztonsági ellenőrzések eredményei és a vonatkozó mögöttes bizonyítékok iránti kérelmek.

Az első albekezdés b) pontjában említett célzott biztonsági ellenőrzéseknek az illetékes hatóság vagy az ellenőrzött szervezet által végzett kockázatértékeléseken vagy más rendelkezésre álló, kockázattal kapcsolatos információkon kell alapulniuk.

A célzott biztonsági ellenőrzések eredményeit az illetékes hatóság rendelkezésére kell bocsátani. A független szerv által végzett ilyen célzott biztonsági ellenőrzés költségeit az ellenőrzött szervezet fizeti, kivéve azokban a kellően indokolt esetekben, amikor az illetékes hatóság másként határoz.

(3) A (2) bekezdés e), f) vagy g) pontja szerinti hatásköreik gyakorlása során az illetékes hatóságok közlik a megkeresés célját és meghatározzák a kért információkat.

(4) A tagállamok biztosítják, hogy az illetékes hatóságaik az alapvető szervezetekkel kapcsolatos végrehajtási hatásköreik gyakorlása során hatáskörrel rendelkezzenek legalább az alábbiakra:

a) figyelmeztetés kiadása ezen irányelv érintett szervezetek általi megsértéséről;

b) kötelező erejű utasítások – többek között az események megelőzéséhez vagy orvoslásához szükséges intézkedésekre, azok végrehajtási határidejére és a végrehajtással kapcsolatos adatszolgáltatásra vonatkozóan – vagy végzés elfogadása, amely előírja az érintett szervezetek számára, hogy orvosolják a feltárt hiányosságokat vagy ezen irányelv megsértését;

c) az érintett szervezetek kötelezése arra, hogy szüntessék meg az ezen irányelvet sértő magatartást, és tartózkodjanak a magatartás ismételt elkövetésétől;

d) az érintett szervezetek kötelezése arra, hogy meghatározott módon és határidőn belül biztosítsák, hogy kiberbiztonsági kockázatkezelési intézkedéseik megfeleljenek a 21. cikknek, és meghatározott módon és határidőn belül eleget tegyenek a 23. cikkben megállapított jelentéstételi kötelezettségeiknek;

e) az érintett szervezetek kötelezése arra, hogy azon természetes vagy jogi személyeket, akik vagy amelyek tekintetében szolgáltatásokat nyújtanak vagy tevékenységeket végeznek, és akiket vagy amelyeket egy jelentős kiberfenyegetés potenciálisan érinthet, tájékoztassák a fenyegetés jellegéről, valamint minden lehetséges védelmi vagy helyreállítási intézkedésről, amelyet e természetes vagy jogi személyek megtehetnek a fenyegetés elhárítására;

f) az érintett szervezetek kötelezése arra, hogy észszerű határidőn belül hajtsák végre a biztonsági ellenőrzés eredményeként adott ajánlásokat;

g) egy jól meghatározott feladatokkal ellátott ellenőrző tisztviselő kinevezése egy meghatározott időtartamra az érintett szervezetek 21. és 23. cikkben előírt kötelezettségei teljesítésének felügyeletére;

h) az érintett szervezetek kötelezése arra, hogy ezen irányelv megsértésének szempontjait meghatározott módon hozzák nyilvánosságra;

i) a 34. cikk szerinti közigazgatási bírság kiszabása vagy annak kérése az illetékes szervektől vagy bíróságoktól a nemzeti joggal összhangban, az e bekezdés a)–h) pontjában említett intézkedések mellett.

(5) Ha a (4) bekezdés a)–d) és f) pontja alapján elfogadott végrehajtási intézkedések eredménytelenek, a tagállamok biztosítják, hogy az illetékes hatóságaik jogosultak legyenek határidőt tűzni, amelyen belül az alapvető szervezet köteles a hiányosságok orvoslásához vagy az említett hatóságok követelményeinek való megfeleléshez szükséges intézkedések meghozatalára. Ha a kért intézkedést a kitűzött határidőn belül nem hozzák meg, a tagállamok biztosítják, hogy az illetékes hatóságaik hatáskörrel rendelkezzenek a következőkre:

a) a tanúsítás vagy az engedély ideiglenes felfüggesztése az alapvető szervezet által nyújtott releváns szolgáltatások vagy tevékenységek egészére vagy egy részére vonatkozóan, vagy a nemzeti joggal összhangban egy tanúsító vagy engedélyező szervezet, illetve egy bíróság erre való felkérése;

b) az érintett szervek, bíróságok felkérése arra, hogy a nemzeti joggal összhangban ideiglenesen tiltsák meg az alapvető szervezet vezérigazgatói vagy jogi képviseleti szintű vezetői feladatainak ellátásáért felelős bármely természetes személy számára, hogy az adott szervezetben vezetői feladatokat lásson el.

Az e bekezdés szerint kiszabott ideiglenes felfüggesztéseket vagy tiltásokat csak addig kell alkalmazni, amíg az érintett szervezet megteszi a szükséges intézkedéseket a hiányosságok orvoslására, vagy eleget tesz az illetékes hatóság azon követelményeinek, amelyek tekintetében az említett végrehajtási intézkedéseket alkalmazták. Az ilyen ideiglenes felfüggesztések vagy tiltások kiszabására megfelelő eljárási biztosítékok vonatkoznak, az uniós jog általános elveivel és a Chartával összhangban, ideértve a hatékony jogorvoslathoz és a tisztességes eljáráshoz való jogot, az ártatlanság vélelmét és a védelemhez való jogot.

Az e bekezdésben előírt végrehajtási intézkedések nem alkalmazhatók az ezen irányelv hatálya alá tartozó közigazgatási szervekre.

(6) A tagállamok biztosítják, hogy az alapvető szervezetért felelős vagy annak jogi képviseletében – képviseleti joga, a nevében történő döntéshozatal vagy az irányítás gyakorlásának joga alapján – eljáró természetes személy hatáskörrel rendelkezzen az ezen irányelvnek való megfelelés biztosítására. A tagállamok biztosítják, hogy e természetes személyek felelősségre vonhatók az ezen irányelvnek való megfelelés biztosítását szolgáló kötelezettségeik megsértéséért.

A közigazgatási szervek tekintetében e bekezdés nem érinti azon nemzeti jogot, amely a köztisztviselők és a megválasztott vagy kinevezett tisztviselők jogi felelősségét szabályozza.

(7) A (4) vagy (5) bekezdésben említett végrehajtási intézkedések bármelyikének meghozatala esetén az illetékes hatóságoknak tiszteletben kell tartaniuk a védelemhez való jogot, és figyelembe kell venniük a konkrét eset körülményeit, és legalább kellően figyelembe kell venniük az alábbiakat:

a) a jogsértés súlya és a megsértett rendelkezések jelentősége, azzal hogy többek között a következők minden esetben súlyos jogsértésnek minősülnek:

   i. ismételt jogsértések;

   ii. jelentős események bejelentésének vagy orvoslásának elmaradása;

   iii. a hiányosságok orvoslásának elmaradása az illetékes hatóságok kötelező erejű utasításait követően;

   iv. a jogsértés megállapítását követően az illetékes hatóság által elrendelt ellenőrzések vagy ellenőrzési tevékenységek akadályozása;

   v. hamis vagy súlyosan pontatlan információk közlése a 21. és 23. cikkben megállapított kiberbiztonsági kockázatkezelési intézkedésekkel vagy jelentéstételi kötelezettségekkel kapcsolatban;

b) a jogsértés időtartama;

c) az érintett szervezet által korábban elkövetett releváns jogsértések;

d) az okozott bármely vagyoni vagy nem vagyoni kár, beleértve bármely pénzügyi vagy gazdasági veszteséget, az egyéb szolgáltatásokra gyakorolt hatásokat és az érintett felhasználók számát;

e) a jogsértés elkövetőjének bármely szándékossága vagy gondatlansága;

f) a szervezet által a vagyoni vagy nem vagyoni kár megelőzésére vagy mérséklésére tett bármely intézkedések;

g) a jóváhagyott magatartási kódexek vagy jóváhagyott tanúsítási mechanizmusok betartása;

h) a felelősnek tartott természetes vagy jogi személyek illetékes hatóságokkal való együttműködésének szintje.

(8) Az illetékes hatóságok részletesen indokolják végrehajtási intézkedéseiket. Az ilyen intézkedések elfogadása előtt az illetékes hatóságok értesítik az érintett szervezeteket előzetes megállapításaikról. Emellett észszerű időt kell biztosítaniuk az említett szervezetek számára észrevételeik benyújtására, kivéve azokat a kellően indokolt eseteket, amikor az események megelőzésére vagy az azokra való reagálásra irányuló azonnali intézkedések máskülönben akadályokba ütköznének.

(9) A tagállamok biztosítják, hogy az ezen irányelv szerinti illetékes hatóságaik tájékoztassák az (EU) 2022/2557 irányelv szerinti, ugyanazon tagállambeli érintett illetékes hatóságokat arról, amikor gyakorolják azon felügyeleti és végrehajtási hatásköreiket, amelyek célja az (EU) 2022/2557 irányelv szerint kritikus szervezetként azonosított szervezet által ezen irányelvnek való megfelelés biztosítása. Adott esetben az (EU) 2022/2557 irányelv szerinti illetékes hatóságok előírhatják az ezen irányelv szerinti illetékes hatóságok számára, hogy gyakorolják felügyeleti és végrehajtási hatásköreiket az ezen irányelv hatálya alá tartozó, az (EU) 2022/2557 irányelv értelmében kritikus szervezetként azonosított szervezet tekintetében.

(10) A tagállamok biztosítják, hogy az ezen irányelv szerinti illetékes hatóságaik együttműködjenek az érintett tagállamnak az (EU) 2022/2554 rendelet szerinti illetékes hatóságaival. A tagállamok biztosítják különösen, hogy az ezen irányelv szerinti illetékes hatóságaik tájékoztassák az (EU) 2022/2554 rendelet 32. cikkének (1) bekezdése szerint létrehozott felvigyázási fórumot arról, amikor gyakorolják azon felügyeleti és végrehajtási hatásköreiket, amelyek célja annak biztosítása, hogy az ezen irányelv hatálya alá tartozó, az (EU) 2022/2554 rendelet 31. cikke szerint kritikus harmadik fél IKT-szolgáltatónak kijelölt alapvető szervezetek megfeleljenek ezen irányelvnek.

33. cikk

A fontos szervezetekre vonatkozó felügyeleti és végrehajtási intézkedések

(1) Ha bizonyítékokat, jelzést vagy információt kapnak arról, hogy egy fontos szervezet vélhetően nem felel meg ezen irányelvnek és különösen a 21. és 23. cikkének, a tagállamok biztosítják, hogy az illetékes hatóságok szükség esetén utólagos felügyeleti intézkedések révén intézkedjenek. A tagállamok biztosítják, hogy ezek az intézkedések hatékonyak, arányosak és visszatartó erejűek legyenek, figyelembe véve az egyes konkrét esetek körülményeit.

(2) A tagállamok biztosítják, hogy az illetékes hatóságok a fontos szervezetekkel kapcsolatos felügyeleti feladataik ellátása során hatáskörrel rendelkezzenek arra, hogy ezeknél a szervezeteknél elvégezzék legalább az alábbiakat:

a) képzett szakemberek által végrehajtott helyszíni ellenőrzések és távoli, utólagos felügyeleti intézkedések;

b) egy független szerv vagy illetékes hatóság által végzett célzott biztonsági ellenőrzések;

c) objektív, megkülönböztetéstől mentes, méltányos és átlátható kockázatértékelési kritériumokon alapuló biztonsági vizsgálatok, amennyiben szükséges, az érintett szervezet együttműködésével;

d) az érintett szervezet által elfogadott kiberbiztonsági kockázatkezelési intézkedések –többek között a dokumentált kiberbiztonsági szabályzatok – értékeléséhez, valamint az információk illetékes hatóságok részére való, a 27. cikk alapján történő bejelentésére vonatkozó kötelezettség betartásának értékeléséhez szükséges tájékoztatás kérése;

e) a felügyeleti feladataik ellátásához szükséges adatokhoz, dokumentumokhoz és információkhoz való hozzáférés iránti kérelmek;

f) a kiberbiztonsági szabályzatok végrehajtására vonatkozó bizonyítékok, például a minősített ellenőr által végzett biztonsági ellenőrzések eredményei és a vonatkozó mögöttes bizonyítékok iránti kérelmek.

Az első albekezdés b) pontjában említett célzott biztonsági ellenőrzéseknek az illetékes hatóság vagy az ellenőrzött szervezet által végzett kockázatértékeléseken vagy más rendelkezésre álló, kockázattal kapcsolatos információkon kell alapulniuk.

A célzott biztonsági ellenőrzések eredményeit az illetékes hatóság rendelkezésére kell bocsátani. A független szerv által végzett ilyen célzott biztonsági ellenőrzés költségeit az ellenőrzött szervezet fizeti, kivéve azokban a kellően indokolt esetekben, amikor az illetékes hatóság másként határoz.

(3) Hatásköreik (2) bekezdés d), e) vagy f) pontja szerinti gyakorlása során az illetékes hatóságok közlik a megkeresés célját és meghatározzák a kért tájékoztatást.

(4) A tagállamok biztosítják, hogy az illetékes hatóságok a fontos szervezetekkel kapcsolatos végrehajtási hatásköreik gyakorlása során hatáskörrel rendelkezzenek legalább az alábbiakra:

a) figyelmeztetés kiadása ezen irányelv érintett szervezetek általi megsértéséről;

b) kötelező erejű utasítások vagy végzés elfogadása, amelyek előírják az érintett szervezetek számára, hogy orvosolják a feltárt hiányosságokat vagy ezen irányelv megsértését;

c) az érintett szervezetek kötelezése arra, hogy szüntessék meg az ezen irányelvet sértő magatartást, és tartózkodjanak a magatartás ismételt elkövetésétől;

d) az érintett szervezetek kötelezése arra, hogy meghatározott módon és határidőn belül biztosítsák, hogy kiberbiztonsági kockázatkezelési intézkedéseik megfeleljenek a 21. cikknek, és meghatározott módon és határidőn belül eleget tegyenek a 23. cikkben megállapított jelentéstételi kötelezettségeiknek;

e) az érintett szervezetek kötelezése arra, hogy azon természetes vagy jogi személyeket, akik vagy amelyek tekintetében szolgáltatásokat nyújtanak vagy tevékenységeket végeznek, és akiket vagy amelyeket egy jelentős kiberfenyegetés potenciálisan érinthet, tájékoztassák a fenyegetés jellegéről, valamint minden lehetséges védelmi vagy helyreállítási intézkedésről, amelyet e természetes vagy jogi személyek megtehetnek a fenyegetés elhárítására;

f) az érintett szervezetek kötelezése arra, hogy észszerű határidőn belül hajtsák végre a biztonsági ellenőrzés eredményeként adott ajánlásokat;

g) az érintett szervezetek kötelezése arra, hogy ezen irányelv megsértésének szempontjait meghatározott módon hozzák nyilvánosságra;

h) a 34. cikk szerinti közigazgatási bírság kiszabása vagy annak kérése az illetékes szervektől vagy bíróságoktól a nemzeti joggal összhangban, az e bekezdés a)–g) pontjában említett intézkedések mellett.

(5) A 32. cikk (6), (7) és (8) bekezdését értelemszerűen alkalmazni kell az e cikkben a fontos szervezetekre vonatkozóan előírt felügyeleti és végrehajtási intézkedésekre is.

(6) A tagállamok biztosítják, hogy az ezen irányelv szerinti illetékes hatóságaik együttműködjenek az érintett tagállamnak az (EU) 2022/2554 rendelet szerinti illetékes hatóságaival. A tagállamok biztosítják különösen, hogy az ezen irányelv szerinti illetékes hatóságaik tájékoztassák az (EU) 2022/2554 rendelet 32. cikkének (1) bekezdése szerint létrehozott felvigyázási fórumot arról, amikor gyakorolják azon felügyeleti és végrehajtási hatásköreiket, amelyek célja annak biztosítása, hogy az ezen irányelv hatálya alá tartozó, az (EU) 2022/2554 rendelet 31. cikke szerint kritikus harmadik fél IKT-szolgáltatónak kijelölt fontos szervezetek megfeleljenek ezen irányelvnek.

34. cikk

Közigazgatási bírság alapvető és fontos szervezetekre történő kiszabásának általános feltételei

(1) A tagállamok biztosítják, hogy az ezen irányelv megsértésére tekintettel az alapvető és fontos szervezetekre e cikk szerint kiszabott közigazgatási bírságok hatékonyak, arányosak és visszatartó erejűek legyenek, figyelembe véve az egyes konkrét esetek körülményeit.

(2) A közigazgatási bírságot a 32. cikk (4) bekezdésének a)–h) pontjában, a 32. cikk (5) bekezdésében és a 33. cikk (4) bekezdésének a)–g) pontjában említett intézkedések mellett kell kiszabni.

(3) Az egyes esetekben a közigazgatási bírság kiszabásának és annak összegének eldöntésekor kellő figyelmet kell fordítani legalább a 32. cikk (7) bekezdésében előírt elemekre.

(4) A tagállamok biztosítják, hogy az alapvető szervezeteket – amennyiben megsértik a 21. vagy a 23. cikket – e cikk (2) és (3) bekezdésével összhangban legalább 10 000 000 EUR vagy, ha ez magasabb, legalább azon vállalkozás előző pénzügyi évi globális éves forgalma teljes összege 2%-ának megfelelő maximális összegű közigazgatási bírsággal sújtsák, amelyhez az alapvető szervezet tartozik.

(5) A tagállamok biztosítják, hogy a fontos szervezeteket – amennyiben megsértik a 21. vagy a 23. cikket – e cikk (2) és (3) bekezdésével összhangban legalább 7 000 000 EUR vagy, ha ez magasabb, legalább azon vállalkozás előző pénzügyi évi globális éves forgalma teljes összege 1,4%-ának megfelelő maximális összegű közigazgatási bírsággal sújtsák, amelyhez a fontos szervezet tartozik.

(6) A tagállamok rendelkezhetnek időszakos kényszerítő bírság kiszabásának hatásköréről annak érdekében, hogy egy alapvető vagy fontos szervezetet az illetékes hatóság korábbi határozatával összhangban ezen irányelv megsértésének megszüntetésére kényszerítsenek.

(7) Az illetékes hatóságok 32. és 33. cikk szerinti hatáskörének sérelme nélkül minden tagállam meghatározhat arra vonatkozó szabályokat, hogy közigazgatási bírság kiszabható-e és milyen mértékben a közigazgatási szervekre.

(8) Ha a tagállam jogrendszere nem rendelkezik közigazgatási bírságokról, az adott tagállam biztosítja, hogy e cikket oly módon alkalmazzák, hogy a bírságot az illetékes hatóság kezdeményezésére az illetékes nemzeti bíróság rója ki, ugyanakkor biztosítva e jogorvoslatok hatékonyságát és az illetékes hatóságok által kiszabott közigazgatási bírságokéval egyenértékű hatását. A kiszabott bírságoknak minden esetben hatékonynak, arányosnak és visszatartó erejűnek kell lenniük. A tagállamok 2024. október 17-ig értesítik a Bizottságot az e bekezdés alapján elfogadott jogszabályokról, valamint haladéktalanul értesítik a Bizottságot az ezeket érintő későbbi módosító jogszabályokról vagy módosításokról.

35. cikk

A személyes adatok megsértésével járó jogsértések

(1) Ha az illetékes hatóságoknak a felügyelet vagy a végrehajtás során a tudomásukra jut, hogy az ezen irányelv 21. és 23. cikkében megállapított kötelezettségeknek egy alapvető vagy fontos szervezet általi megsértése személyes adatok megsértésével járhat az (EU) 2016/679 rendelet 4. cikkének (12) bekezdésében meghatározottak szerint, amelyet az említett rendelet 33. cikke alapján be kell jelenteni, indokolatlan késedelem nélkül tájékoztatniuk kell az említett rendelet 55. vagy 56. cikkében említett felügyeleti hatóságokat.

(2) Amennyiben az (EU) 2016/679 rendelet 55. vagy 56. cikkében említett felügyeleti hatóságok az említett rendelet 58. cikke (2) bekezdésének i) pontja alapján közigazgatási bírságot szabnak ki, az illetékes hatóságok nem szabhatnak ki ezen irányelv 34. cikke szerinti közigazgatási bírságot az e cikk (1) bekezdésében említett olyan jogsértésért, amely ugyanazon magatartásból ered, mint amely az (EU) 2016/679 rendelet 58. cikke (2) bekezdésének i) pontja szerinti közigazgatási bírság tárgyát képezte. Az illetékes hatóságok azonban előírhatják az ezen irányelv 32. cikke (4) bekezdésének a)–h) pontjában, 32. cikkének (5) bekezdésében és 33. cikke (4) bekezdésének a)–g) pontjában előírt végrehajtási intézkedéseket.

(3) Ha az (EU) 2016/679 rendelet alapján illetékes felügyeleti hatóság az illetékes hatóság tagállamától eltérő tagállamban található, az illetékes hatóság tájékoztatja a saját tagállamában található felügyeleti hatóságot a személyes adatok (1) bekezdésben említett potenciális megsértéséről.

36. cikk

Szankciók

A tagállamok megállapítják az ezen irányelv alapján elfogadott nemzeti rendelkezések megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és meghoznak minden szükséges intézkedést ezek végrehajtására. Az előírt szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük. A tagállamok e szabályokról és intézkedésekről 2025. január 17-ig értesítik a Bizottságot, és haladéktalanul tájékoztatják a Bizottságot az e szabályokat és intézkedéseket érintő minden későbbi módosításról.

37. cikk

Kölcsönös segítségnyújtás

(1) Ha egy szervezet egynél több tagállamban nyújt szolgáltatásokat, vagy egy vagy több tagállamban nyújt szolgáltatásokat, és hálózati és információs rendszerei egy vagy több másik tagállamban találhatók, az érintett tagállamok illetékes hatóságai szükség szerint együttműködnek és segítik egymást. Ez az együttműködés magában foglalja legalább a következőket:

a) az egyik tagállamban felügyeleti vagy végrehajtási intézkedéseket alkalmazó illetékes hatóságok az egyedüli kapcsolattartó ponton keresztül tájékoztatják a többi érintett tagállam illetékes hatóságait és konzultálnak velük a megtett felügyeleti és végrehajtási intézkedésekről;

b) az illetékes hatóság felkérhet egy másik illetékes hatóságot felügyeleti vagy végrehajtási intézkedések megtételére;

c) az illetékes hatóság egy másik illetékes hatóságtól származó indokolt kérelem kézhezvétele után – a saját erőforrásaihoz mérten arányos módon – kölcsönös segítséget nyújt a másik illetékes hatóság számára annak érdekében, hogy a felügyeleti vagy végrehajtási intézkedéseket hatékonyan, eredményesen és következetesen lehessen végrehajtani.

Az első albekezdés c) pontjában említett kölcsönös segítségnyújtás kiterjedhet az információkérésekre és a felügyeleti intézkedésekre, beleértve a helyszíni ellenőrzések, a távoli felügyelet vagy a célzott biztonsági ellenőrzések elvégzésére irányuló megkereséseket is. Az az illetékes hatóság, amelyhez segítségnyújtás iránti megkeresést intéztek, nem utasíthatja el a megkeresést, kivéve, ha megállapítást nyer, hogy nem rendelkezik hatáskörrel a kért segítség nyújtására, a kért segítség nem arányos az illetékes hatóság felügyeleti feladataival, vagy a megkeresés olyan információra vonatkozik, vagy olyan tevékenységeket foglal magában, amelyek közlése vagy végrehajtása ellentétes lenne az adott tagállam nemzetbiztonságának, közbiztonságának vagy védelmének alapvető érdekeivel. A megkeresés elutasítása előtt az illetékes hatóság konzultál a többi érintett illetékes hatósággal, valamint az érintett tagállamok egyikének kérésére a Bizottsággal és az ENISA-val.

(2) Adott esetben és közös megegyezéssel különböző tagállamok illetékes hatóságai közös felügyeleti intézkedéseket végezhetnek.

VIII. FEJEZET

FELHATALMAZASON ALAPULO ES VEGREHAJTASI JOGI AKTUSOK

38. cikk

A felhatalmazás gyakorlása

(1) A felhatalmazáson alapuló jogi aktusok elfogadására vonatkozóan a Bizottság részére adott felhatalmazás feltételeit ez a cikk határozza meg.

(2) A Bizottságnak a 24. cikk (2) bekezdésében említett, felhatalmazáson alapuló jogi aktus elfogadására vonatkozó felhatalmazása ötéves időtartamra szól, 2023. január 16-tól kezdődő hatállyal.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 24. cikk (2) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. Ez a határozat az *Európai Unió Hivatalos Lapjában* való közzétételét követő napon vagy a határozatban meghatározott későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

(4) A felhatalmazáson alapuló jogi aktus elfogadása előtt a Bizottság a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban megállapított elvekkel összhangban konzultál az egyes tagállamok által kijelölt szakértőkkel.

(5) A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul és egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.

(6) A 24. cikk (2) bekezdése értelmében elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha az Európai Parlamentnek és a Tanácsnak a jogi aktusról való értesítését követő két hónapon belül sem az Európai Parlament, sem a Tanács nem emelt ellene kifogást, illetve ha az említett időtartam lejártát megelőzően mind az Európai Parlament, mind a Tanács arról tájékoztatta a Bizottságot, hogy nem fog kifogást emelni. Az Európai Parlament vagy a Tanács kezdeményezésére ez az időtartam két hónappal meghosszabbodik.

39. cikk

A bizottsági eljárás

(1) A Bizottságot egy bizottság segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottságnak minősül.

(2) Az e bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 5. cikkét kell alkalmazni.

(3) Ha a bizottság véleményét írásbeli eljárás útján kell beszerezni, ezt az eljárást eredmény hiányában meg kell szüntetni, ha a vélemény benyújtására előírt határidőn belül a bizottság elnöke így dönt, vagy a bizottság egyik tagja kéri.

IX. FEJEZET

ZARO RENDELKEZESEK

40. cikk

Felülvizsgálat

A Bizottság 2027. október 17-ig, majd azt követően 36 havonta felülvizsgálja ezen irányelv működését, és jelentést nyújt be az Európai Parlamentnek és a Tanácsnak. A jelentés különösen azt értékeli, hogy az érintett szervezetek mérete, és az I. és II. mellékletben említett ágazatok, alágazatok, valamint szervezettípusok mennyire relevánsak a gazdaság és a társadalom működése szempontjából a kiberbiztonság tekintetében. Ennek érdekében a stratégiai és operatív együttműködés további előmozdítása céljából a Bizottság figyelembe veszi az együttműködési csoport és a CSIRT-hálózat stratégiai és operatív szinten szerzett tapasztalatokról szóló jelentéseit. A jelentéshez szükség esetén jogalkotási javaslatot kell mellékelni.

41. cikk

Átültetés

(1) A tagállamok 2024. október 17-ig elfogadják és kihirdetik azokat a rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek megfeleljenek. Erről haladéktalanul tájékoztatják a Bizottságot.

Ezeket a rendelkezésket 2024. október 18-tól alkalmazzák.

(2) Amikor a tagállamok elfogadják az (1) bekezdésben említett rendelkezéseket, azokban hivatkozni kell erre az irányelvre, vagy azokhoz hivatalos kihirdetésük alkalmával ilyen hivatkozást kell fűzni. A hivatkozás módját a tagállamok határozzák meg.

42. cikk

A 910/2014/EU rendelet módosításai

A 910/2014/EU rendelet 19. cikkét 2024. október 18-i hatállyal el kell hagyni.

43.cikk

Az (EU) 2018/1972 irányelv módosítása

Az (EU) 2018/1972 irányelv 40. és 41. cikkét 2024. október 18-i hatállyal el kell hagyni.

44. cikk

Hatályon kívül helyezés

Az (EU) 2016/1148 irányelv 2024. október 18-i hatállyal hatályát veszti.

A hatályon kívül helyezett irányelvre történő hivatkozásokat ezen irányelvre való hivatkozásnak kell tekinteni és a III. mellékletben szereplő megfelelési táblázattal összhangban kell értelmezni.

45. cikk

Hatálybalépés

Ez az irányelv az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

46. cikk

Címzettek

Ennek az irányelvnek a tagállamok a címzettjei.

Kelt Strasbourgban, 2022. december 14-én.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*
R. METSOLA	M. BEK

I. MELLÉKLET

A KIEMELTEN KRITIKUS ÁGAZATOK

Ágazat	Alágazat	Szervezet típusa
1. Energia	a) Villamos energia	– Az (EU) 2019/944 európai parlamenti és tanácsi irányelv ([1]) 2. cikkének 57. pontjában meghatározott villamosenergia-ipari vállalkozások, amelyek az említett irányelv 2. cikkének 12. pontjában meghatározott „ellátás” funkciót végzik
		– Az (EU) 2019/944 irányelv 2. cikkének 29. pontjában meghatározott elosztórendszer-üzemeltetők
		– Az (EU) 2019/944 irányelv 2. cikkének 35. pontjában meghatározott átvitelirendszer-üzemeltetők
		– Az (EU) 2019/944 irányelv 2. cikkének 38. pontjában meghatározott termelők
		– Az (EU) 2019/943 európai parlamenti és tanácsi rendelet ([2]) 2. cikkének 8. pontjában meghatározott kijelölt villamosenergiapiac-üzemeltetők – Az (EU) 2019/943 rendelet 2. cikkének 25. pontjában meghatározott, az (EU) 2019/944 irányelv 2. cikkének 18., 20. és 59. pontjában említett aggregálást, keresletoldali választ vagy energiatárolási szolgáltatást nyújtó piaci szereplők – Az elektromos töltőpont kezeléséért és üzemeltetéséért felelős jogalanyok, akik – többek között egy mobilitási szolgáltató nevében és megbízásából – elektromos töltési szolgáltatást nyújtanak végfelhasználók számára
	b) Távfűtés és -hűtés	– Az (EU) 2018/2001 európai parlamenti és tanácsi irányelv ([3]) 2. cikkének 19. pontjában meghatározott távfűtés vagy távhűtés üzemeltetői
	c) Olaj	– Az olajszállító csővezetékek üzemeltetői
		– Olajtermelő, finomító és kezelő létesítmények, tárolók üzemeltetői és szállításirendszer-üzemeltetők
		– A 2009/119/EK tanácsi irányelv ([4]) 2. cikkének f) pontjában meghatározott központi készletezőszervek
	d) Gáz	– A 2009/73/EK európai parlamenti és tanácsi irányelv ([5]) 2. cikkének 8. pontjában meghatározott ellátó vállalkozások
		– A 2009/73/EK irányelv 2. cikkének 6. pontjában meghatározott elosztórendszer-üzemeltetők
		– A 2009/73/EK irányelv 2. cikkének 4. pontjában meghatározott szállításirendszer-üzemeltetők
		– A 2009/73/EK irányelv 2. cikkének 10. pontjában meghatározott tárolásirendszer-üzemeltetők
		– A 2009/73/EK irányelv 2. cikkének 12. pontjában meghatározott LNG-létesítmény rendszerüzemeltetők
		– A 2009/73/EK irányelv 2. cikkének 1. pontjában meghatározott földgázipari vállalkozások
		– A földgázfinomító és -kezelő létesítmények üzemeltetői
	e) Hidrogén	– A hidrogéntermelés, -tárolás és -szállítás üzemeltetői

Ágazat	Alágazat	Szervezet típusa
2. Szállítás	a) Légi	– A 300/2008/EK rendelet 3. cikkének 4. pontjában említett – üzleti célra igénybe vett – légi fuvarozók
		– A 2009/12/EK európai parlamenti és tanácsi irányelv ([6]) 2. cikkének 2. pontjában meghatározott repülőtér-irányító szervezetek, az említett irányelv 2. cikkének 1. pontjában meghatározott repülőterek, a törzshálózathoz tartozó, az 1315/2013/EU európai parlamenti és tanácsi rendelet ([7]) II. mellékletének 2. szakaszában felsorolt repülőtereket is beleértve, valamint a repülőtereken található kapcsolódó létesítményeket üzemeltető szervezetek
		– Az 549/2004/EK európai parlamenti és tanácsi rendelet ([8]) 2. cikkének 1. pontjában meghatározott légiforgalmi irányító (ATC) szolgálatot ellátó forgalomirányítási üzemeltetők
	b) Vasúti	– A 2012/34/EU európai parlamenti és tanácsi irányelv ([9]) 3. cikkének 2. pontjában meghatározott pályahálózat-működtetők
		– A 2012/34/EU irányelv 3. cikkének 1. pontjában meghatározott vállalkozó vasútitársaságok, a kiszolgáló létesítményeknek az említett irányelv 3. cikkének 12. pontjában meghatározott üzemeltetőit is beleértve
	c) Vízi	– A 725/2004/EK európai parlamenti és tanácsi rendelet ([10]) I. mellékletében foglalt tengeri szállítás tekintetében meghatározott azon vállalkozások, amelyek belvízi, tengeri és part menti vízi személyszállítással, illetve vízi árufuvarozással foglalkoznak, ide nem értve azonban az e vállalkozások által üzemeltetett egyes hajókat
		– A 2005/65/EK európai parlamenti és tanácsi irányelv ([11]) 3. cikkének 1. pontjában meghatározott kikötőket irányító szervezetek, a 725/2004/EK rendelet 2. cikkének 11. pontjában meghatározott kikötőlétesítményeiket is beleértve, valamint a kikötőkben található létesítményeket és berendezéseket üzemeltető szervezetek
		– A 2002/59/EK európai parlamenti és tanácsi irányelv ([12]) 3. cikkének o) pontjában meghatározott hajóforgalmi szolgálatok (VTS) üzemeltetői
	d) Közúti	– Az (EU) 2015/962 felhatalmazáson alapuló bizottsági rendelet ([13]) 2. cikkének 12. pontjában meghatározott, a forgalomirányításért felelős közúti hatóságok, azon közigazgatási szervek kivételével, amelyek általános tevékenységének nem alapvető része a forgalomszervezés vagy az intelligens közlekedési rendszerek üzemeltetése
		– A 2010/40/EU európai parlamenti és tanácsi irányelv ([14]) 4. cikkének 1. pontjában meghatározott intelligens közlekedési rendszerek üzemeltetői
3. Banki szolgáltatások		Az 575/2013/EU európai parlamenti és tanácsi rendelet ([15]) 4. cikkének 1. pontjában meghatározott hitelintézetek
4. Pénzügyi piaci infrastruktúrák		– A 2014/65/EU európai parlamenti és tanácsi irányelv ([16]) 4. cikkének 24. pontjában meghatározott kereskedési helyszínek működtetői
		– A 648/2012/EU európai parlamenti és tanácsi rendelet ([17]) 2. cikkének 1. pontjában meghatározott központi szerződő felek

Ágazat	Alágazat	Szervezet típusa
5. Egészségügy		– A 2011/24/EU európai parlamenti és tanácsi irányelv ([18]) 3. cikkének g) pontjában meghatározott egészségügyi szolgáltatók
		– Az (EU) 2022/2371 európai parlamenti és tanácsi rendelet ([19]) 15. cikkében említett uniós referencialaboratóriumok
		– A 2001/83/EK európai parlamenti és tanácsi irányelv ([20]) 1. cikkének 2. pontjában említett gyógyszerek kutatásával és fejlesztésével foglalkozó szervezetek – A NACE Rev. 2. C nemzetgazdasági ágának 21. ágazatában említett gyógyszeralapanyagokat és gyógyszerkészítményeket gyártó szervezetek – Az (EU) 2022/123 európai parlamenti és tanácsi rendelet ([21]) 22. cikkének értelmében vett népegészségügyi szükséghelyzetben kritikus fontosságú orvostechnikai eszközöket (a népegészségügyi szükséghelyzet kritikus fontosságú eszközeinek jegyzéke) gyártó szervezetek
6. Ivóvíz		Az (EU) 2020/2184 európai parlamenti és tanácsi irányelv ([22]) 2. cikke 1. pontjának a) alpontjában meghatározott, emberi fogyasztásra szánt víz szolgáltatói és elosztói, azokat az elosztókat kivéve, akik számára az emberi fogyasztásra szánt víz elosztása más áruk és termékek forgalmazásából álló általános tevékenységüknek nem alapvető része
7. Szennyvíz		A 91/271/EGK tanácsi irányelv ([23]) 2. cikkének 1, 2. és 3. pontjában meghatározott települési szennyvíz, háztartási szennyvíz, vagy ipari szennyvíz összegyűjtését, ártalmatlanítását vagy kezelését végző vállalkozások, azokat a vállalkozásokat kivéve, amelyek általános tevékenységének nem alapvető része a települési szennyvíz, háztartási szennyvíz vagy ipari szennyvíz összegyűjtése, ártalmatlanítása és kezelése
8. Digitális infrastruktúra		– Internetes exchange pont szolgáltatók
		– DNS-szolgáltatók, a gyökérnév-szerverek üzemeltetőit kivéve
		– Legfelső szintű doménnév-nyilvántartók
		– Felhőszolgáltatók
		– Adatközpont-szolgáltatók
		– Tartalomszolgáltató hálózati szolgáltatók
		– Bizalmi szolgáltatók
		– Nyilvános elektronikus hírközlési hálózatok szolgáltatói
		– Nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók
9. IKT-szolgáltatások irányítása (vállalkozások között)		– Irányított szolgáltatók – Irányított biztonsági szolgáltatók

Ágazat	Alágazat	Szervezet típusa
10. Közigazgatás		– A tagállam által a nemzeti joggal összhangban meghatározott, a központi kormányzathoz tartozó közigazgatási szervek
		– A tagállam által a nemzeti joggal összhangban meghatározott regionális szintű közigazgatási szervek
11. Világűr		A tagállamok vagy magánfelek tulajdonában, kezelésében és üzemeltetésében lévő azon földi infrastruktúra üzemeltetői, amelyek támogatják az űralapú szolgáltatások nyújtását, kivéve a nyilvános elektronikus hírközlő hálózatok szolgáltatóit

([1]) Az Európai Parlament és a Tanács (EU) 2019/944 irányelve (2019. június 5.) a villamos energia belső piacára vonatkozó közös szabályokról és a 2012/27/EU irányelv módosításáról (HL L 158., 2019.6.14., 125. o.).

([2]) Az Európai Parlament és a Tanács (EU) 2019/943 rendelete (2019. június 5.) a villamos energia belső piacáról (HL L 158., 2019.6.14., 54. o.).

([3]) Az Európai Parlament és a Tanács (EU) 2018/2001 irányelve (2018. december 11.) a megújuló energiaforrásokból előállított energia használatának előmozdításáról (HL L 328., 2018.12.21., 82. o.).

([4]) A Tanács 2009/119/EK irányelve (2009. szeptember 14.) a tagállamok minimális kőolaj- és/vagy kőolajtermék-készletezési kötelezettségéről (HL L 265., 2009.10.9., 9. o.).

([5]) Az Európai Parlament és a Tanács 2009/73/EK irányelve (2009. július 13.) a földgáz belső piacára vonatkozó közös szabályokról és a 2003/55/EK irányelv hatályon kívül helyezéséről (HL L 211., 2009.8.14., 94. o.).

([6]) Az Európai Parlament és a Tanács 2009/12/EK irányelve (2009. március 11.) a repülőtéri díjakról (HL L 70., 2009.3.14., 11. o.).

([7]) Az Európai Parlament és a Tanács 1315/2013/EU rendelete (2013. december 11.) a transzeurópai közlekedési hálózat fejlesztésére vonatkozó uniós iránymutatásokról és a 661/2010/EU határozat hatályon kívül helyezéséről (HL L 348., 2013.12.20., 1. o.).

([8]) Az Európai Parlament és a Tanács 549/2004/EK rendelete (2004. március 10.) az egységes európai égbolt létrehozására vonatkozó keret megállapításáról (keretrendelet) (HL L 96., 2004.3.31., 1. o.; magyar nyelvű különkiadás, 7. fejezet, 8. kötet, 23. o.).

([9]) Az Európai Parlament és a Tanács 2012/34/EU irányelve (2012. november 21.) az egységes európai vasúti térség létrehozásáról (HL L 343., 2012.12.14., 32. o.).

([10]) Az Európai Parlament és a Tanács 725/2004/EK rendelete (2004. március 31.) a hajók és kikötői létesítmények biztonságának fokozásáról (HL L 129., 2004.4.29., 6. o.).

([11]) Az Európai Parlament és a Tanács 2005/65/EK irányelve (2005. október 26.) a kikötővédelem fokozásáról (HL L 310., 2005.11.25., 28. o.).

([12]) Az Európai Parlament és a Tanács 2002/59/EK irányelve (2002. június 27.) a közösségi hajóforgalomra vonatkozó megfigyelő és információs rendszer létrehozásáról és a 93/75/EGK irányelv hatályon kívül helyezéséről (HL L 208., 2002.8.5., 10. o.).

([13]) A Bizottság (EU) 2015/962 felhatalmazáson alapuló rendelete (2014. december 18.) a 2010/40/EU európai parlamenti és tanácsi irányelvnek az EU egészére kiterjedő valós idejű forgalmi információs szolgáltatások nyújtása tekintetében történő kiegészítéséről (HL L 157., 2015.6.23., 21. o.).

([14]) Az Európai Parlament és a Tanács 2010/40/EU irányelve (2010. július 7.) az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről (HL L 207., 2010.8.6., 1. o.).

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

([16]) Az Európai Parlament és a Tanács 2014/65/EU irányelve (2014. május 15.) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról (HL L 173., 2014.6.12., 349. o.).

([17]) 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.).

([18]) Az Európai Parlament és a Tanács 2011/24/EU irányelve (2011. március 9.) a határon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről (HL L 88., 2011.4.4., 45. o.).

([19]) Az Európai Parlament és a Tanács (EU) 2022/2371 rendelete (2022. november 23.) a határokon át terjedő súlyos egészségügyi veszélyekről és az 1082/2013/EU határozat hatályon kívül helyezéséről (HL L 314., 2022.12.6., 26. o.).

([20]) Az Európai Parlament és a Tanács 2001/83/EK irányelve (2001. november 6.) az emberi felhasználásra szánt gyógyszerek közösségi kódexéről (HL L 311., 2001.11.28., 67. o.).

([21]) Az Európai Parlament és a Tanács (EU) 2022/123 rendelete (2022. január 25.) az Európai Gyógyszerügynökség által a gyógyszerek és orvostechnikai eszközök tekintetében a válsághelyzetekre való felkészültség és a válságkezelés terén betöltött szerep megerősítéséről (HL L 20., 2022.1.31., 1. o.).

([22]) Az Európai Parlament és a Tanács (EU) 2020/2184 irányelve (2020. december 16.) az emberi fogyasztásra szánt víz minőségéről (HL L 435., 2020.12.23., 1. o.).

([23]) A Tanács 91/271/EGK irányelve (1991. május 21.) a települési szennyvíz kezeléséről (HL L 135., 1991.5.30., 40. o.).

II. MELLÉKLET

EGYÉB KRITIKUS ÁGAZATOK

Ágazat	Alágazat	Szervezet típusa
1. Postai és futárszolgáltatások		A 97/67/EK irányelv 2. cikkének 1a. pontjában meghatározott postai szolgáltatók, beleértve a futárszolgáltatókat
2. Hulladékgazdálkodás		A 2008/98/EK európai parlamenti és tanácsi irányelv ([1]) 3. cikkének 9. pontjában meghatározott hulladékgazdálkodással foglalkozó vállalkozások, kivéve azokat a vállalkozásokat, amelyeknek nem a hulladékgazdálkodás a fő gazdasági tevékenységük
3. Vegyszerek gyártása, előállítása és forgalmazása		Az 1907/2006/EK európai parlamenti és tanácsi rendelet ([2]) 3. cikkének 9. és 14. pontjában említettek szerint anyagok gyártását, illetve anyagok vagy keverékek forgalmazását végző vállalkozások, továbbá az említett rendelet 3. cikkének 3. pontjában meghatározott árucikkeket ilyen anyagokból vagy keverékekből előállító vállalkozások
4. Élelmiszer-termelés, -feldolgozás és -forgalmazás		A 178/2002/EK európai parlamenti és tanácsi rendelet ([3]) 3. cikkének 2. pontjában meghatározott élelmiszer-vállalkozások, amelyek nagykereskedelemmel, ipari termeléssel és feldolgozással foglalkoznak
5. Gyártás	a) Orvostechnikai eszközök és in vitro diagnosztikai orvostechnikai eszközök gyártása	Az (EU) 2017/745 európai parlamenti és tanácsi rendelet ([4]) 2. cikkének 1. pontjában meghatározott orvostechnikai eszközöket, valamint az (EU) 2017/746 európai parlamenti és tanácsi rendelet ([5]) 2. cikkének 2. pontjában meghatározott in vitro diagnosztikai orvostechnikai eszközöket gyártó szervezetek, kivéve az e rendelet 1. melléklete 5. pontjának ötödik franciabekezdésében említett orvostechnikai eszközöket gyártó szervezeteket
	b) Számítógépek, elektronikai és optikai termékek gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 26. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
	c) Villamos berendezések gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 27. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
	d) Máshova nem sorolt gépek és gépi berendezések gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 28. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
	e) Gépjárművek, pótkocsik és félpótkocsik gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 29. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
	f) Egyéb szállítóeszközök gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 30. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások

Ágazat	Alágazat	Szervezet típusa
6. Digitális szolgáltatók		– Online piacterek szolgáltatói
		– Online keresőmotorok szolgáltatói
		– A közösségimédia-szolgáltatási platform szolgáltatói
7. Kutatás		Kutatóhelyek

([1]) Az Európai Parlament és a Tanács 2008/98/EK irányelve (2008. november 19.) a hulladékokról és egyes irányelvek hatályon kívül helyezéséről (HL L 312., 2008.11.22., 3. o.).

([2]) Az Európai Parlament és a Tanács 1907/2006/EK rendelete (2006. december 18.) a vegyi anyagok regisztrálásáról, értékeléséről, engedélyezéséről és korlátozásáról (REACH), az Európai Vegyianyag-ügynökség létrehozásáról, az 1999/45/EK irányelv módosításáról, valamint a 793/93/EGK tanácsi rendelet, az 1488/94/EK bizottsági rendelet, a 76/769/EGK tanácsi irányelv, a 91/155/EGK, a 93/67/EGK, a 93/105/EK és a 2000/21/EK bizottsági irányelv hatályon kívül helyezéséről (HL L 396., 2006.12.30., 1. o.).

([3]) Az Európai Parlament és a Tanács 178/2002/EK rendelete (2002. január 28.) az élelmiszerjog általános elveiről és követelményeiről, az Európai Élelmiszerbiztonsági Hatóság létrehozásáról és az élelmiszerbiztonságra vonatkozó eljárások megállapításáról (HL L 31., 2002.2.1., 1. o.).

([4]) Az Európai Parlament és a Tanács (EU) 2017/745 rendelete (2017. április 5.) az orvostechnikai eszközökről, a 2001/83/EK irányelv, a 178/2002/EK rendelet és az 1223/2009/EK rendelet módosításáról, valamint a 90/385/EGK és a 93/42/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 117., 2017.5.5., 1. o.).

([5]) Az Európai Parlament és a Tanács (EU) 2017/746 rendelete (2017. április 5.) az in vitro diagnosztikai orvostechnikai eszközökről, valamint a 98/79/EK irányelv és a 2010/227/EU bizottsági határozat hatályon kívül helyezéséről (HL L 117., 2017.5.5., 176. o.).

III. MELLÉKLET

MEGFELELÉSI TÁBLÁZAT

Az (EU) 2016/1148 irányelv	Ez az irányelv
1. cikk, (1) bekezdés	1. cikk, (1) bekezdés
1. cikk, (2) bekezdés	1. cikk, (2) bekezdés
1. cikk, (3) bekezdés	–
1. cikk, (4) bekezdés	2. cikk, (12) bekezdés
1. cikk, (5) bekezdés	2. cikk, (13) bekezdés
1. cikk, (6) bekezdés	2. cikk, (6) és (11) bekezdés
1. cikk, (7) bekezdés	4. cikk
2. cikk	2. cikk, (14) bekezdés
3. cikk	5. cikk
4. cikk	6. cikk
5. cikk	–
6. cikk	–
7. cikk, (1) bekezdés	7. cikk, (1) és (2) bekezdés
7. cikk, (2) bekezdés	7. cikk, (4) bekezdés
7. cikk, (3) bekezdés	7. cikk, (3) bekezdés
8. cikk, (1)–(5) bekezdés	8. cikk, (1)–(5) bekezdés
8. cikk, (6) bekezdés	13. cikk, (4) bekezdés
8. cikk, (7) bekezdés	8. cikk, (6) bekezdés
9. cikk, (1), (2) és (3) bekezdés	10. cikk, (1), (2) és (3) bekezdés
9. cikk, (4) bekezdés	10. cikk, (9) bekezdés
9. cikk, (5) bekezdés	10. cikk, (10) bekezdés
10. cikk, (1), (2) és (3) bekezdés, első albekezdés	13. cikk, (1), (2) és (3) bekezdés
10. cikk (3) bekezdés, második albekezdés	23. cikk (9) bekezdés
11. cikk, (1) bekezdés	14. cikk, (1) és (2) bekezdés
11. cikk, (2) bekezdés	14. cikk, (3) bekezdés
11. cikk, (3) bekezdés	14. cikk, (4) bekezdés, első albekezdés, a)–q) pont és s) pont és (7) bekezdés
11. cikk, (4) bekezdés	14. cikk, (4) bekezdés, első albekezdés, r) pont és második albekezdés
11. cikk, (5) bekezdés	14. cikk, (8) bekezdés
12. cikk, (1)–(5) bekezdés	15. cikk, (1)–(5) bekezdés
13. cikk	17. cikk
14. cikk, (1) és (2) bekezdés	21. cikk, (1)–(4) bekezdés
14. cikk, (3) bekezdés	23. cikk, (1) bekezdés
14. cikk, (4) bekezdés	23. cikk, (3) bekezdés
14. cikk, (5) bekezdés	23. cikk, (5), (6) és (8) bekezdés

Az (EU) 2016/1148 irányelv	Ez az irányelv
14. cikk, (6) bekezdés	23. cikk, (7) bekezdés
14. cikk, (7) bekezdés	23. cikk, (11) bekezdés
15. cikk, (1) bekezdés	31. cikk, (1) bekezdés
15. cikk, (2) bekezdés, első albekezdés, a) pont	32. cikk, (2) bekezdés, e) pont
15. cikk, (2) bekezdés, első albekezdés, b) pont	32. cikk, (2) bekezdés, g) pont
15. cikk, (2) bekezdés, második albekezdés	32. cikk, (3) bekezdés
15. cikk, (3) bekezdés	32. cikk, (4) bekezdés, b) pont
15. cikk, (4) bekezdés	31. cikk, (3) bekezdés
16. cikk, (1) és (2) bekezdés	21. cikk, (1)–(4) bekezdés
16. cikk, (3) bekezdés	23. cikk, (1) bekezdés
16. cikk, (4) bekezdés	23. cikk, (3) bekezdés
16. cikk, (5) bekezdés	–
16. cikk, (6) bekezdés	23. cikk, (6) bekezdés
16. cikk, (7) bekezdés	23. cikk, (7) bekezdés
16. cikk, (8) és (9) bekezdés	21. cikk, (5) bekezdés és 23. cikk (11) bekezdés
16. cikk, (10) bekezdés	–
16. cikk, (11) bekezdés	2. cikk, (1), (2) és (3) bekezdés
17. cikk, (1) bekezdés	33. cikk, (1) bekezdés
17. cikk, (2) bekezdés, a) pont	32. cikk, (2) bekezdés, e) pont
17. cikk, (2) bekezdés, b) pont	32. cikk, (4) bekezdés, b) pont
17. cikk, (3) bekezdés	37. cikk, (1) bekezdés, a) és b) pont
18. cikk, (1) bekezdés	26. cikk, (1) bekezdés, b) pont és (2) bekezdés
18. cikk, (2) bekezdés	26. cikk, (3) bekezdés
18. cikk, (3) bekezdés	26. cikk, (4) bekezdés
19. cikk	25. cikk
20. cikk	30. cikk
21. cikk	36. cikk
22. cikk	39. cikk
23. cikk	40. cikk
24. cikk	–
25. cikk	41. cikk
26. cikk	45. cikk
27. cikk	46. cikk
I. melléklet, 1. pont	11. cikk, (1) bekezdés
I. melléklet, 2. pont, a) pont, i–iv. alpont	11. cikk, (2) bekezdés, a–d) pont

Az (EU) 2016/1148 irányelv	Ez az irányelv
I. melléklet, 2. pont, a) pont, v. alpont	11. cikk, (2) bekezdés, f) pont
I. melléklet, 2. pont, b) pont	11. cikk, (4) bekezdés
I. melléklet, 2. pont, c) pont, i. és ii. alpont	11. cikk, (5) bekezdés, a) pont
II. melléklet	I. melléklet
III. melléklet, 1. és 2. pont	II. melléklet, 6. pont
III. melléklet, 3. pont	I. melléklet, 8. pont

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2556 IRÁNYELVE

(2022. december 14.)

a pénzügyi ágazat digitális működési rezilienciája tekintetében a 2009/65/EK, a 2009/138/EK, a 2011/61/EU, a 2013/36/EU, a 2014/59/EU, a 2014/65/EU, az (EU) 2015/2366 és az (EU) 2016/2341 irányelv módosításáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 53. cikke (1) bekezdésére és 114. cikkére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Központi Bank véleményére ([1]),

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére ([2]),

rendes jogalkotási eljárás keretében ([3]),

mivel:

(1) Az Uniónak megfelelően és átfogóan kell kezelnie azon valamennyi pénzügyi szervezetet érintő digitális kockázatokat, amelyek a pénzügyi szolgáltatások nyújtása és igénybevétele során az információs és kommunikációs technológiák (IKT) fokozott használatából erednek, hozzájárulva ezáltal a digitális pénzügyi szolgáltatásokban rejlő potenciál megvalósításához az innováció ösztönzése és a verseny előmozdítása tekintetében egy biztonságos digitális környezetben.

(2) A pénzügyi szervezetek nagymértékben támaszkodnak digitális technológiák használatára mindennapi üzleti tevékenységük során. Rendkívül fontos ezért a digitális műveleteik IKT-kockázattal szembeni működési rezilienciájának biztosítása. Ez az igény még inkább sürgetővé vált az áttörést hozó technológiáknak, különösen az érték vagy a jogok digitális megjelenítőinek elektronikusan – megosztott főkönyvi vagy hasonló technológia felhasználásával – történő átruházását és tárolását lehetővé tevő technológiáknak (kriptoeszközök), valamint az említett eszközökhöz kapcsolódó szolgáltatásoknak a piacon történő növekedése miatt.

([1]) HL C 343., 2021.8.26., 1. o.
([2]) HL C 155., 2021.4.30., 38. o.
([3]) Az Európai Parlament 2022. november 10-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2022. november 28-i határozata.

(3) Uniós szinten a pénzügyi ágazatban fennálló IKT-kockázat kezelésével kapcsolatos követelményekről jelenleg a 2009/65/EK ([4]), a 2009/138/EK ([5]), a 2011/61/EU ([6]), a 2013/36/EU ([7]), a 2014/59/EU ([8]), a 2014/65/EU ([9]), az (EU) 2015/2366 ([10]) és az (EU) 2016/2341 ([11]) európai parlamenti és tanácsi irányelv rendelkezik. Az említett követelmények sokfélék, és alkalmanként hiányosak. Egyes esetekben az IKT-kockázatot a működési kockázat részeként, csak implicit módon kezelik, más esetekben pedig egyáltalán nem kezelik.

Az említett kérdéseket orvosolja az (EU) 2022/2554 európai parlamenti és tanácsi rendelet ([12]) elfogadása. Az említett irányelveket ezért az említett rendelettel való összhang biztosítása érdekében módosítani kell. Ez az irányelv egy sor olyan módosítást foganatosít, amelyek szükségesek a jogi egyértelműség és következetesség megteremtéséhez az említett irányelvekkel összhangban engedélyezett és felügyelt pénzügyi szervezetek általi olyan különböző, digitális működési rezilienciára vonatkozó követelmények alkalmazásával kapcsolatban, amelyek tevékenységeik folytatásához és szolgáltatásaik nyújtásához szükségesek, ezáltal garantálva a belső piac zavartalan működését. Szükséges az említett követelmények piaci fejleményekkel kapcsolatos megfelelőségének biztosítása, ösztönözve ugyanakkor az arányosságot – a megfelelési költségek csökkentése céljából – különösen a pénzügyi szervezetek mérete és a rájuk vonatkozó egyedi szabályozási rendszerek tekintetében.

(4) A banki szolgáltatások területén a 2013/36/EU irányelv jelenleg csak általános belső irányítási szabályokat, valamint a vészhelyzeti és üzletmenet-folytonossági tervekre vonatkozó követelményeket magukban foglaló, működési kockázatra vonatkozó rendelkezéseket határoz meg, amelyek implicit módon az IKT-kockázat kezelése alapjául szolgálnak. Az IKT-kockázat kifejezett és egyértelmű kezelése érdekében azonban a vészhelyzeti és üzletmenet-folytonossági tervekre vonatkozó követelményeket módosítani kell, hogy azok az IKT-kockázatra vonatkozóan is kiterjedjenek az üzletmenet-folytonossági, valamint a reagálási és helyreállítási tervekre, az (EU) 2022/2554 rendeletben meghatározott követelményekkel összhangban. Továbbá, az IKT-kockázat – a működési kockázat részeként – csak implicit módon szerepel az illetékes hatóságok által végzett felügyeleti felülvizsgálati és értékelési eljárásban (SREP), és értékelésének kritériumai jelenleg az 1093/2010/EU európai parlamenti és tanácsi rendelettel ([13]) létrehozott európai felügyeleti hatóság (Európai Bankhatóság, EBH) által kiadott, az „Iránymutatások a felügyeleti felülvizsgálati és értékelési eljárás (SREP) során végzendő IKT-kockázat értékeléséhez” című

([4]) Az Európai Parlament és a Tanács 2009/65/EK irányelve (2009. július 13.) az átruházható értékpapírokkal foglalkozó kollektív befektetési vállalkozásokra (ÁÉKBV) vonatkozó törvényi, rendeleti és közigazgatási rendelkezések összehangolásáról (HL L 302., 2009.11.17., 32. o.).

([5]) Az Európai Parlament és a Tanács 2009/138/EK irányelve (2009. november 25.) a biztosítási és viszontbiztosítási üzleti tevékenység megkezdéséről és gyakorlásáról (Szolvencia II) (HL L 335., 2009.12.17., 1. o.).

([6]) Az Európai Parlament és a Tanács 2011/61/EU irányelve (2011. június 8.) az alternatívbefektetésialap-kezelőkről, valamint a 2003/41/EK és a 2009/65/EK irányelv, továbbá az 1060/2009/EK és az 1095/2010/EU rendelet módosításáról (HL L 174., 2011.7.1., 1. o.).

([7]) Az Európai Parlament és a Tanács 2013/36/EU irányelve (2013. június 26.) a hitelintézetek tevékenységéhez való hozzáférésről és a hitelintézetek prudenciális felügyeletéről, a 2002/87/EK irányelv módosításáról, a 2006/48/EK és a 2006/49/EK irányelv hatályon kívül helyezéséről (HL L 176., 2013.6.27., 338. o.).

([8]) Az Európai Parlament és a Tanács 2014/59/EU irányelve (2014. május 15.) a hitelintézetek és befektetési vállalkozások helyreállítását és szanálását célzó keretrendszer létrehozásáról és a 82/891/EGK tanácsi irányelv, a 2001/24/EK, 2002/47/EK, 2004/25/EK, 2005/56/EK, 2007/36/EK, 2011/35/EU, 2012/30/EU és 2013/36/EU irányelv, valamint az 1093/2010/EU és a 648/2012/EU európai parlamenti és tanácsi rendelet módosításáról (HL L 173., 2014.6.12., 190. o.).

([9]) Az Európai Parlament és a Tanács 2014/65/EU irányelve (2014. május 15.) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról (HL L 173., 2014.6.12., 349. o.).

([10]) 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 az 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről (HL L 337., 2015.12.23., 35. o.).

([11]) Az Európai Parlament és a Tanács (EU) 2016/2341 irányelve (2016. december 14.) a foglalkoztatói nyugellátást szolgáltató intézmények tevékenységéről és felügyeletéről (HL L 354., 2016.12.23., 37. o.).

([12]) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (lásd e Hivatalos Lap 1. oldalát).

([13]) 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.).

dokumentumban vannak meghatározva. A jogi egyértelműség és annak biztosítása érdekében, hogy a bankfelügyeletek a digitális működési rezilienciára vonatkozó új kerettel összhangban hatékonyan azonosítsák az IKT-kockázatot, és nyomon kövessék annak a pénzügyi szervezetek által történő kezelését, a SREP hatályát is módosítani kell, hogy az kifejezetten utaljon az (EU) 2022/2554 rendeletben meghatározott követelményekre, valamint lefedje különösen a jelentős IKT-vonatkozású eseményjelentések által és a pénzügyi szervezetek által az említett rendelettel összhangban végzett, a digitális működési rezilienciára vonatkozó tesztelés eredményei által feltárt kockázatokat.

(5) A digitális működési reziliencia alapvető fontosságú egy pénzügyi szervezet kritikus funkcióinak és fő üzletágainak a szanálása esetén történő megőrzéséhez, és ezáltal a reálgazdaságban és a pénzügyi rendszerben való zavarok elkerüléséhez. A jelentős működési zavart okozó események akadályozhatják egy pénzügyi szervezet további működésre való képességét, és veszélyeztethetik a szanálási célkitűzéseket. Bizonyos, az IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodások alapvető fontosságúak a működés folytonosságának biztosításához és szanálás esetén a szükséges adatok biztosításához. A működési rezilienciára vonatkozó uniós keret célkitűzéseivel való összehangolása érdekében a 2014/59/EU irányelvet megfelelően módosítani kell annak biztosítása céljából, hogy a működési rezilienciára vonatkozó információkat figyelembe vegyék a szanálási tervezéssel és a pénzügyi szervezetek szanálhatóságának értékelésével összefüggésben.

(6) A 2014/65/EU irányelv azon befektetési vállalkozások és kereskedési helyszínek számára ír elő szigorúbb IKT-kockázati szabályokat, amelyek algoritmikus kereskedéssel foglalkoznak. Kevésbé részletes követelmények alkalmazandók az adatszolgáltatókra és a kereskedési adattárakra. Úgyszintén, a 2014/65/EU irányelv csak korlátozott utalásokat tartalmaz az adatfeldolgozó rendszerekre vonatkozó ellenőrzési és biztonsági eljárásokra, valamint az üzleti szolgáltatások folyamatosságának és szabályszerűségének biztosítását szolgáló megfelelő rendszerek, erőforrások és eljárások használatára. Továbbá, az említett irányelvet össze kell hangolni az (EU) 2022/2554 rendelettel a befektetési szolgáltatások nyújtása és a befektetési tevékenységek végzése során a folyamatosság és a szabályszerűség, a működési reziliencia, a kereskedési rendszerek kapacitása, valamint az üzletmenet-folytonossági mechanizmusok és a kockázatkezelés hatékonysága tekintetében.

(7) Az (EU) 2015/2366 irányelv egyedi szabályokat határoz meg az IKT-vel kapcsolatos biztonsági ellenőrzési és kockázatmérséklési elemekre vonatkozóan a pénzforgalmi szolgáltatások nyújtásához szükséges engedély megszerzése céljából. Az említett engedélyezési szabályokat az (EU) 2022/2554 rendelettel való összehangolásuk érdekében módosítani kell. Továbbá, az adminisztratív terhek csökkentése, valamint az összetettség és a párhuzamos adatszolgáltatási követelmények elkerülése érdekében az említett irányelvben foglalt eseményjelentési szabályok alkalmazását az említett irányelv által szabályozott és egyúttal az (EU) 2022/2554 rendelet hatálya alá is tartozó pénzforgalmi szolgáltatók számára meg kell szüntetni, ezáltal lehetővé téve, hogy az említett pénzforgalmi szolgáltatók valamennyi pénzforgalmi-vonatkozású működési vagy biztonsági esemény tekintetében egyetlen, teljes mértékben harmonizált eseményjelentési mechanizmus előnyét élvezzék, függetlenül attól, hogy az ilyen események IKT-vonatkozásúak-e.

(8) A 2009/138/EK és az (EU) 2016/2341 irányelv részben beépíti az IKT-kockázatot az irányításra és a kockázatkezelésre vonatkozó általános rendelkezéseibe, bizonyos követelmények részletes meghatározását pedig felhatalmazáson alapuló jogi aktusokra hagyja, az IKT-kockázatra való külön hivatkozásokkal vagy anélkül. Hasonlóképpen, csak nagyon általános szabályok vonatkoznak a 2011/61/EU irányelv hatálya alá tartozó alternatív-befektetésialap-kezelőkre és a 2009/65/EK irányelv hatálya alá tartozó alapkezelő társaságokra. Az említett irányelveket ezért össze kell hangolni az (EU) 2022/2554 rendeletben az IKT-rendszerek és -eszközök kezelése tekintetében megállapított követelményekkel.

(9) Számos esetben az illetékes európai felügyeleti hatóság által kidolgozott szabályozástechnikai standardtervezetek és végrehajtás-technikai standardtervezetek alapján elfogadott felhatalmazáson alapuló és végrehajtási jogi aktusokban már meghatároztak további IKT kockázati követelményeket. Mivel az (EU) 2022/2554 rendelet rendelkezései képezik ezentúl a pénzügyi ágazatban az IKT-kockázatra vonatkozó jogi keretet, a 2009/65/EK, a 2009/138/EK, a 2011/61/EU és a 2014/65/EU irányelvben foglalt, felhatalmazáson alapuló és végrehajtási jogi aktusok elfogadására vonatkozó egyes felhatalmazásokat módosítani kell, hogy az IKT-kockázatra vonatkozó rendelkezések kikerüljenek az említett felhatalmazások hatálya alól.

(10) A pénzügyi ágazat digitális működési rezilienciájára vonatkozó új keret következetes végrehajtásának biztosítása érdekében a tagállamoknak az ezen irányelvet átültető nemzeti jogi rendelkezéseket az (EU) 2022/2554 rendelet alkalmazásának kezdőnapjától kell alkalmazniuk.

(11) A 2009/65/EK, a 2009/138/EK, a 2011/61/EU, a 2013/36/EU, a 2014/59/EU, a 2014/65/EU, az (EU) 2015/2366 és az (EU) 2016/2341 irányelvet az Európai Unió működéséről szóló szerződés (EUMSZ) 53. cikkének (1) bekezdése vagy 114. cikke vagy mindkettő alapján fogadták el. Az ezen irányelvben foglalt módosításokat egyetlen jogi aktusba foglalták a módosítások tárgya és célkitűzései közötti összekapcsoltság miatt. Következésképpen ezen irányelvet együttesen az EUMSZ 53. cikkének (1) bekezdése és 114. cikke alapján kell elfogadni.

(12) Mivel ezen irányelv céljait a tagállamok nem tudják kielégítően megvalósítani, mert azok már irányelvekben foglalt követelmények harmonizációjához vezetnek, az Unió szintjén azonban az intézkedés terjedelme és hatásai miatt e célok jobban megvalósíthatók, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritás elvével összhangban. Az arányosságnak az említett cikkben foglalt elvével összhangban ez az irányelv nem lépi túl az e célok eléréséhez szükséges mértéket.

(13) A tagállamoknak és a Bizottságnak a magyarázó dokumentumokról szóló, 2011. szeptember 28-i együttes politikai nyilatkozatával ([14]) összhangban a tagállamok vállalták, hogy az átültető intézkedéseikről szóló értesítéshez indokolt esetben egy vagy több olyan dokumentumot mellékelnek, amely megmagyarázza az irányelv elemei és az azt átültető nemzeti jogi eszközök megfelelő részei közötti kapcsolatot. Ezen irányelv tekintetében a jogalkotó úgy ítéli meg, hogy ilyen dokumentumok átadása indokolt,

ELFOGADTA EZT AZ IRÁNYELVET:

1. cikk

A 2009/65/EK irányelv módosításai

A 2009/65/EK irányelv 12. cikke a következőképpen módosul:

1. Az (1) bekezdés második albekezdése a) pontjának helyébe a következő szöveg lép:

„a) rendelkezzen szilárd és megalapozott igazgatási és számviteli eljárásokkal, az elektronikus adatfeldolgozásra vonatkozó ellenőrzési és biztonsági eljárásokkal – többek között az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek (*) megfelelően létrehozott és kezelt hálózati és információs rendszerek tekintetében –, valamint megfelelő belső ellenőrzési mechanizmusokkal, amelyek magukban foglalják különösen az alkalmazottai által lebonyolított személyes tranzakciókra vagy a sajátszámlás befektetések céljából vásárolt pénzügyi eszközökbe történt befektetések birtoklására vagy kezelésére vonatkozó szabályokat, és biztosítják legalább minden egyes, az ÁÉKBV-t érintő tranzakciók eredetének, az azokban részt vevő feleknek, az ügylet jellegének, időpontjának és helyének az utólagos visszakeresését és ellenőrzését, valamint azt, hogy az ÁÉKBV-nek az alapkezelő társaságok kezelésében levő eszközeit a mindenkori működési szabályokkal vagy létesítő okiratokkal és hatályos jogi rendelkezésekkel összhangban fektessék be;

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27., 1. o.).”

2. A (3) bekezdés helyébe a következő szöveg lép:

„(3) A 116. cikk sérelme nélkül a Bizottság – a 112a. cikkel összhangban felhatalmazáson alapuló jogi aktusok révén – intézkedéseket fogad el a következők meghatározása céljából:

a) az (1) bekezdés második albekezdésének a) pontjában említett – a hálózati és információs rendszerekre vonatkozó eljárásoktól és szabályoktól eltérő – eljárások és szabályok;

b) az (1) bekezdés második albekezdésének b) pontjában említett, az összeférhetetlenség minimalizálására irányuló szerkezeti és szervezeti követelmények.”

([14]) HL C 369., 2011.12.17., 14. o.

2. cikk

A 2009/138/EK irányelv módosításai

A 2009/138/EK irányelv a következőképpen módosul:

1. A 41. cikk (4) bekezdésének helyébe a következő szöveg lép:

„(4) A biztosító vagy viszontbiztosító észszerű lépéseket tesz a tevékenységei végzése során a folyamatosság és szabályszerűség biztosítása érdekében, beleértve vészhelyzeti tervek kidolgozását. E célból a vállalkozások megfelelő és arányos rendszereket, erőforrásokat és eljárásokat alkalmaznak, és így különösen hálózati és információs rendszereket hoznak létre és kezelnek, az (EU) 2022/2554 európai parlamenti és tanácsi rendelettel (*) összhangban.

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27.,1. o.).”

2. Az 50. cikk (1) bekezdése a) és b) pontjának helyébe a következő szöveg lép:

„a) a 41., a 44., a 46. és a 47. cikkben említett rendszereknek – az információs és kommunikációs technológiai kockázat kezelésére vonatkozó elemektől eltérő – elemei, különösen a 44. cikk (2) bekezdésében felsorolt területek;

b) a 44., a 46., a 47. és a 48. cikkben említett – az információs és kommunikációs technológiai kockázat kezeléséhez kapcsolódó feladatköröktől eltérő – feladatkörök.”

3. cikk

A 2011/61/EU irányelv módosítása

A 2011/61/EU irányelv 18. cikkének helyébe a következő szöveg lép:

„*18. cikk*

Általános elvek

(1) A tagállamok előírják, hogy az ABAK-ok mindig az ABA-k helyes kezeléséhez szükséges, megfelelő és célszerű emberi és technikai erőforrást alkalmazzanak.

Így különösen, az ABAK letelepedése szerinti tagállam hatáskörrel rendelkező hatóságai, figyelembe véve az ABAK kezelésében lévő ABA-k jellegét is, előírják, hogy az ABAK rendelkezzen megbízható igazgatási és számviteli eljárásokkal, az elektronikus adatfeldolgozásra vonatkozó ellenőrzési és biztonsági eljárásokkal – többek között az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek (*) megfelelően létrehozott és kezelt hálózati és információs rendszerek tekintetében –, valamint megfelelő belső ellenőrzési mechanizmusokkal, beleértve különösen az alkalmazottai által lebonyolított személyes ügyletekre vagy a sajátszámlás befektetések birtoklására és kezelésére vonatkozó szabályokat, amelyek biztosítják legalább az ABA-k részvételével vagy közreműködésével lebonyolított ügyletek eredetének, az azokban részt vevő feleknek, az ügylet jellegének, időpontjának és helyének utólagos visszakereshetőségét és ellenőrizhetőségét, valamint azt, hogy az ABA-knak az ABAK kezelésében levő eszközeit az ABA-k alapszabályával vagy létesítő okiratával és a hatályos jogi rendelkezésekkel összhangban fektessék be.

(2) A Bizottság az 56. cikkel összhangban, valamint az 57. és az 58. cikk feltételeinek megfelelően, felhatalmazáson alapuló jogi aktusok révén intézkedéseket fogad el, amelyekben meghatározza az e cikk (1) bekezdésében említett – a hálózati és információs rendszerekre vonatkozó eljárásoktól és szabályoktól eltérő – eljárásokat és szabályokat.

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27., 1. o.).”

4. cikk

A 2013/36/EU irányelv módosításai

A 2013/36/EU irányelv a következőképpen módosul:

1. A 65. cikk (3) bekezdése a) pontja vi. alpontjának helyébe a következő szöveg lép:

„vi. olyan harmadik felek, amelyekhez az i–iv. pontban említett szervezetek funkciókat vagy tevékenységeket szerveztek ki, beleértve az (EU) 2022/2554 európai parlamenti és tanácsi rendelet (*) V. fejezetében említett, harmadik fél IKT-szolgáltatókat is;

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27., 1. o.).”

2. A 74. cikk (1) bekezdése első albekezdésének helyébe a következő szöveg lép:

„Az intézményeknek olyan megbízható irányítási rendszerrel kell rendelkezniük, amely magában foglalja az áttekinthető szervezeti felépítést, az egymástól jól elhatárolt, átlátható és következetes felelősségi köröket, a fennálló vagy esetlegesen felmerülő kockázatok azonosítására, kezelésére, nyomon követésére és bejelentésére szolgáló hatékony eljárásokat, a megfelelő belső ellenőrzési mechanizmusokat – beleértve a megbízható adminisztratív és számviteli eljárásokat is –, az (EU) 2022/2554 rendeletnek megfelelően létrehozott és kezelt hálózati és információs rendszereket, valamint a hatékony és eredményes kockázatkezeléssel összhangban álló, azt előmozdító javadalmazási szabályokat és gyakorlatokat.”

3. A 85. cikk (2) bekezdésének helyébe a következő szöveg lép:

„(2) Az illetékes hatóságok biztosítják, hogy az intézmények megfelelő vészhelyzeti és üzletmenet-folytonossági politikákkal és tervekkel rendelkezzenek – beleértve az általuk információközlésre használt technológia tekintetében az IKT-vonatkozású üzletmenet-folytonossági politikákat és terveket, valamint az IKT-vonatkozású reagálási és helyreállítási terveket is –, továbbá, hogy az említett tervek létrehozására, kezelésére és tesztelésére az (EU) 2022/2554 rendelet 11. cikkének megfelelően kerüljön sor, annak lehetővé tétele érdekében, hogy az intézmények tovább működjenek az üzletmenetben okozott súlyos zavar esetén, és mérsékeljék az ilyen zavar következtében felmerülő veszteségeket.”

4. A 97. cikk (1) bekezdése a következő ponttal egészül ki:

„d) a digitális működési reziliencia tesztelése által az (EU) 2022/2554 rendelet IV. fejezetével összhangban feltárt kockázatokat.”

5. cikk

A 2014/59/EU irányelv módosításai

A 2014/59/EU irányelv a következőképpen módosul:

1. A 10. cikk a következőképpen módosul:

a) a (7) bekezdés c) pontjának helyébe a következő szöveg lép:

„c) annak bemutatása, hogy a kritikus funkciók és a fő üzletágak hogyan különíthetők el a szükséges mértékben jogilag és gazdaságilag más funkcióktól annak érdekében, hogy az intézmény csődje esetén a folytonosság és a digitális működési reziliencia biztosítható legyen;”

b) a (7) bekezdés q) pontjának helyébe a következő szöveg lép:

„q) az intézmény működési eljárásai folyamatos működésének fenntartását szolgáló alapvető fontosságú műveletek és rendszerek leírása, beleértve az (EU) 2022/2554 európai parlamenti és tanácsi rendeletben (*) említett hálózati és információs rendszereket is;

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27., 1. o.).”;

c) a (9) bekezdés a következő albekezdéssel egészül ki:

„Az EBH-nak az 1093/2010/EU rendelet 10. cikkével összhangban felül kell vizsgálnia, és adott esetben aktualizálnia kell a szabályozástechnikai standardokat, többek között az (EU) 2022/2554 rendelet II. fejezete rendelkezéseinek figyelembevétele érdekében."

2. A melléklet a következőképpen módosul:

a) az A. szakasz (16) pontjának helyébe a következő szöveg lép:

„(16) az intézmény működési folyamatai – többek között az (EU) 2022/2554 rendeletnek megfelelően létrehozott és kezelt hálózati és információs rendszerek – folyamatos működésének fenntartásához szükséges szabályok és intézkedések;"

b) a B. szakasz a következőképpen módosul:

i. a (14) pont helyébe a következő szöveg lép:

„(14) a (13) pontban meghatározott rendszerek tulajdonosainak, a rendszerekhez kapcsolódó, szolgáltatási szintre vonatkozó megállapodásoknak, valamint bármely szoftvernek és rendszereknek vagy engedélyeknek az azonosítása – beleértve a jogi személyeihez, kritikus működési folyamataihoz és fő üzletágaihoz való hozzárendelést is –, valamint az (EU) 2022/2554 rendelet 3. cikkének 23. pontjában meghatározott kritikus harmadik fél IKT-szolgáltatók azonosítása;"

ii. a szöveg a következő ponttal egészül ki:

„(14a) az intézmény digitális működési rezilienciájának az (EU) 2022/2554 rendelet szerinti tesztelésének eredményei;"

c) a C. szakasz a következőképpen módosul:

i. a (4) pont helyébe a következő szöveg lép:

„(4) az, hogy az intézmény által fenntartott szolgáltatási megállapodások – beleértve az IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokat is – mennyire szilárdak és érvényesíthetők teljes körűen az intézmény szanálása esetén;"

ii. a szöveg a következő ponttal egészül ki:

„(4a) az intézmény kritikus funkcióit és fő üzletágait támogató hálózati és információs rendszerek digitális működési rezilienciája, figyelembe véve a jelentős IKT-vonatkozású eseményjelentéseket és a digitális működési reziliencia (EU) 2022/2554 rendelet szerinti tesztelésének eredményeit;".

6. cikk

A 2014/65/EU irányelv módosításai

A 2014/65/EU irányelv a következőképpen módosul:

1. A 16. cikk a következőképpen módosul:

a) a (4) bekezdés helyébe a következő szöveg lép:

„(4) A befektetési vállalkozás észszerű lépéseket tesz a befektetési szolgáltatások és tevékenységek végzése során a folyamatosság és szabályszerűség biztosítása érdekében. A befektetési vállalkozás e célból megfelelő és arányos rendszereket – beleértve az (EU) 2022/2554 európai parlamenti és tanácsi rendelet (*) 7. cikkének megfelelően létrehozott és kezelt információs és kommunikációs technológiai (IKT) rendszereket –, valamint megfelelő és arányos erőforrásokat és eljárásokat alkalmaz.

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27., 1. o.).";

b) az (5) bekezdés második és harmadik albekezdésének helyébe a következő szöveg lép:

„A befektetési vállalkozás megalapozott igazgatási és számviteli eljárásokkal, belső ellenőrzési mechanizmusokkal és hatékony kockázatértékelési eljárásokkal rendelkezik.

Az illetékes hatóságok azon képességének sérelme nélkül, hogy ezen irányelvvel és a 600/2014/EU rendelettel összhangban hozzáférést kérjenek a kommunikációhoz, a befektetési vállalkozás megbízható biztonsági mechanizmusokkal rendelkezik, hogy – az (EU) 2022/2554 európai parlamenti és tanácsi rendeletben meghatározott követelményekkel összhangban – biztosítsa az információtovábbítási eszközök biztonságát és hitelesítését, minimalizálja az adatsérülés és a jogosulatlan hozzáférés kockázatát, és megelőzze az információk kiszivárgását, ezáltal mindenkor fenntartva az adatok bizalmas jellegét.”

2. A 17. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) Az algoritmikus kereskedéssel foglalkozó befektetési vállalkozás az általa működtetett üzleti tevékenységnek megfelelő, hatékony rendszerekkel és kockázat-ellenőrzési mechanizmusokkal rendelkezik annak biztosítására, hogy kereskedési rendszerei – az (EU) 2022/2554 rendelet II. fejezetében meghatározott követelményekkel összhangban – reziliensek legyenek, és elegendő kapacitással rendelkezzenek, megfelelő kereskedési küszöbértékek és limitek hatálya alá tartozzanak, és megakadályozzák a hibás megbízások kiküldését vagy a rendszerek egyéb, potenciálisan rendellenes piaci helyzetet eredményező vagy ilyen helyzet kialakulását elősegítő működését.

Az ilyen vállalkozás hatékony rendszerekkel és kockázat-ellenőrzési mechanizmusokkal rendelkezik annak biztosítására is, hogy a kereskedési rendszerek ne legyenek felhasználhatók semmiféle olyan célra, amely ellentétes az 596/2014/EU rendelettel vagy azon kereskedési helyszín szabályaival, amelyhez kapcsolódik.

A befektetési vállalkozás olyan, hatékony üzletmenet-folytonossági mechanizmusokkal rendelkezik, amelyek alkalmasak a kereskedési rendszereiben fellépő bármely hiba kezelésére, beleértve az (EU) 2022/2554 rendelet 11. cikkével összhangban létrehozott IKT-vonatkozású üzletmenet-folytonossági politikát és terveket, valamint IKT-vonatkozású reagálási és helyreállítási terveket is, továbbá biztosítja rendszereinek teljes körű tesztelését és megfelelő nyomon követését annak biztosítása érdekében, hogy azok megfeleljenek az e bekezdésben meghatározott általános követelményeknek és az (EU) 2022/2554 rendelet II. és IV. fejezetében meghatározott bármely egyedi követelménynek.”;

b) a (7) bekezdés a) pontjának helyébe a következő szöveg lép:

„a) a különböző befektetési szolgáltatásokat nyújtó, befektetési tevékenységeket folytató, kiegészítő szolgáltatásokat nyújtó, vagy ezek különböző kombinációival foglalkozó befektetési vállalkozásokra vonatkozóan az (1)–(6) bekezdésben előírt – az IKT-kockázatkezeléshez kapcsolódóaktól eltérő – szervezeti követelmények részletei, amelyek keretében az (5) bekezdésben meghatározott szervezeti követelményekkel kapcsolatos előírásoknak oly módon kell egyedi követelményeket meghatározniuk a közvetlen piaci hozzáférés és a szponzorált hozzáférés vonatkozásában, hogy az biztosítsa, hogy a szponzorált hozzáférésre vonatkozó ellenőrzési mechanizmusok legalább egyenértékűek legyenek a közvetlen hozzáférésre vonatkozóakkal;”.

3. A 47. cikk (1) bekezdése a következőképpen módosul:

a) a b) pont helyébe a következő szöveg lép:

„b) legyen megfelelően felszerelt azon kockázatok kezelésére, amelyeknek ki van téve – beleértve az IKT-kockázatnak az (EU) 2022/2554 rendelet II. fejezetének megfelelő kezelését is –, hogy megfelelő megállapodásokat és rendszereket hozzon létre a működését veszélyeztető lényeges kockázatok azonosítására, és hatékony intézkedéseket hozzon az említett kockázatok csökkentésére;”

b) a c) pontot el kell hagyni.

4. A 48. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) A tagállamok előírják a szabályozott piac számára, hogy az (EU) 2022/2554 rendelet II. fejezetében meghatározott követelményekkel összhangban alakítsa ki és tartsa fenn a működési rezilienciáját annak biztosítására, hogy kereskedési rendszerei reziliensek legyenek, elegendő kapacitással rendelkezzenek csúcsterhelés esetén a megbízások és üzenetek volumenének kezelésére, képesek legyenek szabályos kereskedést biztosítani jelentős piaci stresszhelyzetben, teljes körű tesztelésen essenek át az ilyen feltételek teljesülésének biztosítása érdekében, továbbá hatékony üzletmenet-folytonossági mechanizmusokkal rendelkezzenek – beleértve az (EU) 2022/2554 rendelet 11. cikkével összhangban létrehozott IKT-vonatkozású üzletmenet-folytonossági politikát és terveket, valamint IKT-vonatkozású reagálási és helyreállítási terveket – a szolgáltatásai folyamatosságának biztosítása érdekében, ha a kereskedési rendszereiben meghibásodás következik be.”;

b) a (6) bekezdés helyébe a következő szöveg lép:

„(6) A tagállamok előírják a szabályozott piac számára, hogy hatékony rendszerei, eljárásai és mechanizmusai legyenek – ideértve a tagok vagy résztvevők arra való felszólítását, hogy végezzék el az algoritmusok megfelelő tesztelését, és biztosítsanak környezetet az ilyen tesztelés megkönnyítéséhez az (EU) 2022/2554 rendelet II. és IV. fejezetében meghatározott követelményekkel összhangban – annak biztosítására, hogy az algoritmikus kereskedési rendszerek ne hozhassanak létre rendellenes kereskedési feltételeket a piacon, és ne járulhassanak hozzá ilyenek kialakulásához, továbbá hogy kezelje az ilyen algoritmikus kereskedési rendszerekből mégis felmerülő rendellenes kereskedési feltételeket, ideértve az olyan rendszereket, amelyek lehetővé teszik a nem végrehajtott megbízások arányának korlátozását a rendszerbe egy tag vagy résztvevő által bevihető ügyleti megbízásokhoz képest, a megbízások áramlásának lelassítását, ha fennáll a rendszere határkapacitása elérésének kockázata, valamint a piacon végrehajtható legkisebb árlépésköz korlátozását és betartatását.”;

c) a (12) bekezdés a következőképpen módosul:

i. az a) pont helyébe a következő szöveg lép:

„a) a szabályozott piacok kereskedési rendszerei rezilienciájának és megfelelő kapacitásának biztosítására vonatkozó követelmények, a digitális működési rezilienciával kapcsolatos követelmények kivételével;”;

ii. a g) pont helyébe a következő szöveg lép:

„g) az algoritmusok megfelelő tesztelésének – kivéve a digitális működési reziliencia tesztelését – biztosítására vonatkozó követelmények annak biztosítása érdekében, hogy az algoritmikus kereskedési rendszerek – ideértve a nagysebességű algoritmikus kereskedési rendszereket – ne hozhassanak létre rendellenes kereskedési feltételeket a piacon, vagy ne járulhassanak hozzá ilyenek kialakulásához.”

7. cikk

Az (EU) 2015/2366 irányelv módosításai

Az (EU) 2015/2366 irányelv a következőképpen módosul:

1. A 3. cikk j) pontjának helyébe a következő szöveg lép:

„j) olyan technikai szolgáltatók által nyújtott szolgáltatások, amelyek támogatják a fizetési szolgáltatások nyújtását anélkül, hogy bármikor is birtokolnák a továbbítandó pénzeszközöket, ideértve az adatok feldolgozását és tárolását, a bizalmi és adatvédelmi szolgáltatásokat, az adat- és entitáshitelesítést, az információs és kommunikációs technológia (IKT) és a kommunikációs hálózat biztosítását, fizetési szolgáltatásokhoz használt terminálok és eszközök biztosítását és karbantartását, kivéve a megbízásos online átutalásokat és a számlainformációk összesítését;”.

2. Az 5. cikk (1) bekezdése a következőképpen módosul:

a) az első albekezdés a következőképpen módosul:

i. az e) pont helyébe a következő szöveg lép:

„e) a kérelmező irányítási rendszereinek és belső ellenőrzési mechanizmusainak leírása – beleértve az adminisztratív, kockázatkezelési és számviteli eljárásokat, valamint az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek (*) megfelelően az IKT-szolgáltatások igénybevételére irányuló megállapodásokat is –, amely bemutatja, hogy az említett irányítási rendszerek és belső ellenőrzési mechanizmusok arányosak, helyénvalóak, megbízhatóak és megfelelőek;

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27., 1. o.).”;

ii. az f) pont helyébe a következő szöveg lép:

„f) a biztonsági események és a biztonsággal kapcsolatos ügyfélpanaszok nyomon követésére, kezelésére és utókövetésére szolgáló eljárások leírása, ideértve az eseményjelentési mechanizmust is, amely figyelembe veszi a pénzforgalmi intézményeknek az (EU) 2022/2554 rendelet III. fejezetében megállapított értesítési kötelezettségeit;”

iii. a h) pont helyébe a következő szöveg lép:

„h) az üzletmenet-folytonossági mechanizmusok leírása, amely magában foglalja a kritikus műveletek, a hatékony IKT-vonatkozású üzletmenet-folytonossági politika és tervek, valamint IKT-vonatkozású reagálási és helyreállítási tervek, továbbá az ilyen tervek megfelelőségének és hatékonyságának rendszeres tesztelésére és felülvizsgálatára szolgáló, az (EU) 2022/2554 rendeletnek megfelelő eljárás egyértelmű azonosítását;"

b) a harmadik albekezdés helyébe a következő szöveg lép:

„Az első albekezdés j) pontjában említett biztonsági ellenőrzési és kockázatmérséklési intézkedéseknek be kell mutatniuk, hogyan biztosítják a magas szintű digitális működési rezilienciát az (EU) 2022/2554 rendelet II. fejezetével összhangban, különösen a műszaki biztonsággal és adatvédelemmel kapcsolatban, ideértve a kérelmező által vagy a kérelmező működésének egy részét vagy egészét kiszervezett tevékenységként végző vállalkozások által alkalmazott szoftvereket és IKT-rendszereket. Az említett intézkedéseknek magukban kell foglalniuk az ezen irányelv 95. cikkének (1) bekezdésében meghatározott biztonsági intézkedéseket is. Az említett intézkedéseknek – a foganatosításukkor – figyelembe kell venniük az EBH biztonsági intézkedésekről szóló, ezen irányelv 95. cikkének (3) bekezdésében említett iránymutatásait."

3. A 19. cikk (6) bekezdése második albekezdésének helyébe a következő szöveg lép:

„Fontos működtetési feladatok, többek között IKT-rendszerek kiszervezésére nem kerülhet sor oly módon, hogy az lényegesen csorbítsa a pénzforgalmi intézmény belső ellenőrzésének minőségét, valamint az illetékes hatóságok azon képességét, hogy monitorozzák és nyomon kövessék, hogy a pénzforgalmi intézmény eleget tesz-e az ezen irányelvben megállapított valamennyi kötelezettségnek."

4. A 95. cikk (1) bekezdése a következő albekezdéssel egészül ki:

„Az első albekezdés nem érinti az (EU) 2022/2554 rendelet II. fejezetének alkalmazását a következők tekintetében:

a) az ezen irányelv 1. cikke (1) bekezdésének a), b) és d) pontjában említett pénzforgalmi szolgáltatók;

b) az ezen irányelv 33. cikkének (1) bekezdésében említett számlainformációkat összesítő szolgáltatók;

c) az ezen irányelv 32. cikkének (1) bekezdése alapján mentesített pénzforgalmi intézmények; és

d) a 2009/110/EK irányelv 9. cikkének (1) bekezdésében említett, alkalmazás alóli mellőzést élvező elektronikuspénz-kibocsátó intézmények."

5. A 96. cikk a következő bekezdéssel egészül ki:

„(7) A tagállamok biztosítják, hogy e cikk (1)–(5) bekezdése nem alkalmazandó a következőkre:

a) az ezen irányelv 1. cikke (1) bekezdésének a), b) és d) pontjában említett pénzforgalmi szolgáltatók;

b) az ezen irányelv 33. cikkének (1) bekezdésében említett számlainformációkat összesítő szolgáltatók;

c) az ezen irányelv 32. cikkének (1) bekezdése alapján mentesített pénzforgalmi intézmények; és

d) a 2009/110/EK irányelv 9. cikkének (1) bekezdésében említett, alkalmazás alóli mellőzést élvező elektronikuspénz-kibocsátó intézmények."

6. A 98. cikk (5) bekezdésének helyébe a következő szöveg lép:

„(5) Az EBH-nak az 1093/2010/EU rendelet 10. cikkével összhangban rendszeresen felül kell vizsgálnia, és adott esetben aktualizálnia kell a szabályozástechnikai standardokat többek között annak érdekében, hogy figyelembe vegye az innovációt és a technológiai fejleményeket, valamint az (EU) 2022/2554 rendelet II. fejezetének rendelkezéseit."

8. cikk

Az (EU) 2016/2341 irányelv módosítása

Az (EU) 2016/2341 irányelv 21. cikke (5) bekezdésének helyébe a következő szöveg lép:

„(5) A tagállamok biztosítják, hogy a foglalkoztatói nyugellátást szolgáltató intézmények észszerű lépéseket tegyenek a tevékenységeik végzése során a folyamatosság és szabályszerűség biztosítása érdekében, beleértve

vészhelyzeti tervek kidolgozását. E célból a foglalkoztatói nyugellátást szolgáltató intézmények megfelelő és arányos rendszereket, erőforrásokat és eljárásokat alkalmaznak, és így különösen – adott esetben – hálózati és információs rendszereket hoznak létre és kezelnek az (EU) 2022/2554 európai parlamenti és tanácsi rendelettel (*) összhangban.

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (HL L 333.., 2022.12.27., 1. o.)."

9. cikk

Átültetés

(1) A tagállamok legkésőbb 2025. január 17-ig elfogadják és kihirdetik azokat a rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek megfeleljenek. Erről haladéktalanul tájékoztatják a Bizottságot.

A tagállamok ezeket a rendelkezéseket 2025. január 17-től alkalmazzák.

Amikor a tagállamok elfogadják ezeket a rendelkezéseket, azokban hivatkozni kell erre az irányelvre, vagy azokhoz hivatalos kihirdetésük alkalmával ilyen hivatkozást kell fűzni. A hivatkozás módját a tagállamok határozzák meg.

(2) A tagállamok közlik a Bizottsággal nemzeti joguk azon főbb rendelkezéseinek szövegét, amelyeket az ezen irányelv által szabályozott területen fogadnak el.

10. cikk

Hatálybalépés

Ez az irányelv az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

11. cikk

Címzettek

Ennek az irányelvnek a tagállamok a címzettjei.

Kelt Strasbourgban, 2022. december 14-én.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*
R. METSOLA	M. BEK

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2557 IRÁNYELVE

(2022. december 14.)

a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről

(EGT-vonatkozású szöveg)

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 114. cikkére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére ([1]),

tekintettel a Régiók Bizottságának véleményére ([2]),

rendes jogalkotási eljárás keretében ([3]),

mivel:

(1) Alapvető szolgáltatásokat nyújtó szervezetekként a kritikus szervezetek nélkülözhetetlen szerepet töltenek be a belső piacon az alapvetően fontos társadalmi funkciók vagy gazdasági tevékenységek fenntartásában, egy olyan uniós gazdaságban, amelynek ágazatai egyre nagyobb mértékben függenek egymástól. Ezért alapvető fontosságú egy olyan uniós keret kidolgozása, amely mind a belső piacon működő kritikus szervezetek rezilienciájának fokozását célozza harmonizált minimumszabályok meghatározásával, mind pedig koherens és célzott támogatási és felügyeleti intézkedésekkel hivatott segíteni e szervezeteket.

(2) A 2008/114/EK tanácsi irányelv ([4]) rendelkezik az energia- és a közlekedési ágazatban működő azon európai kritikus infrastruktúra kijelölésére szolgáló eljárásról, amelyek zavarának vagy megrongálódásának jelentős határokon átnyúló hatása lehet legalább két tagállamban. Az említett irányelv kizárólag az ilyen infrastruktúra védelmére összpontosít. A 2008/114/EK irányelv 2019-ben elvégzett értékelése azonban azt állapította meg, hogy a kritikus infrastruktúra használatával végzett műveletek egyre inkább összekapcsolódó és határokon átnyúló jellege miatt a kizárólag az egyes eszközökre vonatkozó védelmi intézkedések nem elegendőek a zavarok megelőzéséhez. Ezért változtatni kell a megközelítésen, és a kockázatok megfelelőbb figyelembevételének biztosítására kell összpontosítani, valamint arra, hogy a belső piac működése szempontjából alapvető szolgáltatásokat nyújtó kritikus szervezetek szerepe és feladatai jobban meg legyenek határozva és koherensek legyenek, valamint hogy uniós

([1]) HL C 286., 2021.7.16., 170. o.
([2]) HL C 440., 2021.10.29., 99. o.
([3]) Az Európai Parlament 2022. november 22-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2022. december 8-i határozata.
([4]) A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (HL L 345., 2008.12.23., 75. o.).

szabályok elfogadására kerüljön sor a kritikus szervezetek rezilienciájának fokozása érdekében. A kritikus szervezeteknek képeseknek kell lenniük fokozni az arra irányuló képességüket, hogy az alapvető szolgáltatások nyújtásában zavarokat előidézni képes eseményeket megelőzzék, azokkal szemben védekezzenek, azokra reagáljanak, azoknak ellenálljanak, azokat enyhítsék, tompítsák, azokhoz alkalmazkodjanak és azokból helyreálljanak.

(3) Noha több uniós szintű intézkedés, így például a kritikus infrastruktúrák védelmére vonatkozó európai program, valamint nemzeti szintű intézkedés célja támogatni az Unión belüli kritikus infrastruktúra védelmét, további intézkedéseket kell hozni annak érdekében, hogy az ilyen infrastruktúrát üzemeltető szervezeteket jobban felvértezzék a működésüket érintő azon kockázatok kezelésére, amelyek zavart idézhetnek elő az alapvető szolgáltatások nyújtásában. Többet kell tenni annak érdekében is, hogy az ilyen szervezeteket felvértezzék, mert dinamikusan változó a fenyegetettségi helyzet, amely magában foglal változó hibrid és terrorista fenyegetéseket, valamint az infrastruktúra és az ágazatok közötti növekvő kölcsönös függőségeket.. Ezen túlmenően a természeti katasztrófák és az éghajlatváltozás miatt megnövekedett a fizikai kockázat, az éghajlatváltozás ugyanis fokozza a szélsőséges időjárási események előfordulásának gyakoriságát és nagyságrendjét, és hosszú távú változásokat idéz elő az átlagos éghajlati viszonyokban, amelyek csökkenthetik bizonyos infrastruktúratípusok kapacitását, hatékonyságát és élettartamát, amennyiben nem kerülnek bevezetésre az éghajlatváltozáshoz való alkalmazkodást célzó intézkedések. Ezen kívül, a belső piacot a kritikus szervezetek azonosítását illetően fragmentáció jellemzi, mert a releváns ágazatokat és szervezeti kategóriákat nem minden tagállamban ismerik el következetesen kritikusként. Ezen irányelvnek ezért magas szintű harmonizációt kell megvalósítania a hatálya alá tartozó ágazatok és szervezeti kategóriák tekintetében.

(4) Míg egyes gazdasági ágazatokat – így például az energia- és a közlekedési ágazatot – már ágazatspecifikus uniós jogi aktusok szabályoznak, az említett jogi aktusok olyan rendelkezéseket tartalmaznak, amelyek az ezen ágazatokban működő szervezetek rezilienciájának csupán bizonyos aspektusaira vonatkoznak. A belső piac megfelelő működése szempontjából kritikus szervezetek rezilienciájának átfogó kezelése érdekében ez az irányelv olyan átfogó keretet hoz létre, amely figyelmet fordít a kritikus szervezetek valamennyi – akár természeti vagy ember okozta, véletlen vagy szándékos – veszéllyel szembeni rezilienciájára.

(5) Az infrastruktúra és az ágazatok közötti növekvő kölcsönös függőségek annak eredményeként alakulnak ki, hogy egyre inkább határokon átívelő és egymástól kölcsönösen függő, Unió-szerte a kulcsfontosságú infrastruktúrát használó szolgáltatási hálózatok jönnek létre az energia, a közlekedés, a banki szolgáltatások, az ivóvíz, a szennyvíz, az élelmiszer-termelés, -feldolgozás és -forgalmazás, az egészségügy, a világűr, a pénzügyi piaci infrastruktúra és a digitális infrastruktúra ágazatában, valamint a közigazgatási ágazat bizonyos aspektusaiban. A világűrágazat – a vagy a tagállamok által vagy a magánfelek által tulajdonolt, irányított és üzemeltetett földi infrastruktúrától függő bizonyos szolgáltatások nyújtása tekintetében – ezen irányelv hatálya alá tartozik; következésképpen az Unió űrprogramja részeként az Unió által vagy az Unió nevében tulajdonolt, irányított vagy üzemeltetett infrastruktúra nem tartozik ezen irányelv hatálya alá.

Az energiaágazatban, különösen (a villamosenergia-ellátás tekintetében) a villamosenergia-termelési és -átviteli módszerek vonatkozásában a villamosenergia-termelés adott esetben magában foglalhatja az atomerőművek villamosenergia-átvitelre szolgáló részeit, de kizárja a szerződések és az uniós jog hatálya alá tartozó, kifejezetten nukleáris elemeket, beleértve az Uniónak a nukleáris energiára vonatkozó releváns jogi aktusait. Az élelmiszer-ágazatbeli kritikus szervezetek azonosítására szolgáló eljárásnak megfelelően tükröznie kell a belső piac jellegét az említett ágazatban, valamint az élelmiszerjog és az élelmiszer-biztonság általános elveire és követelményeire vonatkozó kiterjedt uniós szabályokat. Ezért az arányos megközelítés biztosítása, valamint az említett szervezetek nemzeti szinten betöltött szerepének és jelentőségének megfelelő tükrözése érdekében a kritikus szervezeteket csak a kizárólag logisztikával és nagykereskedelmi forgalmazással, valamint nagyléptékű ipari termeléssel és feldolgozással foglalkozó, a nemzeti szinten jelentős piaci részesedéssel rendelkező élelmiszeripari vállalkozások közül kell beazonosítani, függetlenül attól, hogy nyereségorientáltak-e vagy sem, és hogy állami vagy magánvállalkozásokról van-e szó. Az említett kölcsönös függőségek azt jelentik, hogy az alapvető szolgáltatások bármely megzavarása, még ha az kezdetben csak egy szervezetre vagy ágazatra korlátozódik is, szélesebb körű továbbgyűrűző hatásokkal járhat, potenciálisan messzire nyúló és hosszú távú negatív hatást eredményezve a szolgáltatások nyújtására az egész belső piacon. Az olyan jelentős válságok, mint a Covid19-világjárvány, rámutattak az egyre inkább egymásra utalt társadalmaink sebezhetőségére a nagy hatású, csekély valószínűségű kockázatokkal szemben.

(6) Egyre gyakrabban fordul elő, hogy a nemzeti jog alapján eltérő követelmények vonatkoznak az alapvető szolgáltatások nyújtásában részt vevő szervezetekre. Az a tény, hogy egyes tagállamokban kevésbé szigorú biztonsági követelmények vonatkoznak az említett szervezetekre, nemcsak a reziliencia eltérő szintjeihez vezet, hanem Unió-szerte negatívan hathat az alapvetően fontos társadalmi funkciók vagy gazdasági tevékenységek fenntartására is, és a belső piac megfelelő működésével szembeni akadályokhoz vezet. A befektetők és a vállalkozások az olyan kritikus szervezetekre tudnak támaszkodni, és azokban tudnak megbízni, amelyek reziliensek, továbbá a megbízhatóság és a bizalom a jól működő belső piac sarokkövei. Hasonló típusú szervezetek egyes tagállamokban kritikusnak minősülnek, másokban viszont nem, és különböző tagállamokban eltérő követelmények vonatkoznak a kritikusnak minősített szervezetekre. Ez további és szükségtelen adminisztratív terhet ró a határokon átnyúlóan működő vállalatokra, különösen a szigorúbb követelményekkel rendelkező tagállamokban aktív vállalatokra. Az uniós keretnek ezért olyan hatása is volna, hogy Unió-szerte egyenlő versenyfeltételeket teremt a kritikus szervezetek számára.

(7) Harmonizált minimumszabályokat kell megállapítani az alapvető belső piaci szolgáltatások nyújtásának biztosítása, a kritikus szervezetek rezilienciájának fokozása, valamint az illetékes hatóságok közötti, határokon átnyúló együttműködés javítása érdekében. Fontos, hogy az említett szabályok a kialakításuk és végrehajtásuk tekintetében időtállók legyenek, miközben lehetővé teszik a szükséges rugalmasságot. Alapvető fontosságú javítani a kritikus szervezetek azon képességét is, hogy a különféle kockázatok ellenére alapvető szolgáltatásokat nyújtsanak.

(8) A magas szintű reziliencia elérése érdekében a tagállamoknak azonosítaniuk kell azon kritikus szervezeteket, amelyekre különleges követelmények és felügyelet fog vonatkozni, és amelyek – valamennyi releváns kockázat tekintetében – különös támogatást és iránymutatást fognak kapni.

(9) Tekintve a kiberbiztonság jelentőségét a kritikus szervezetek rezilienciája szempontjából, valamint a következetesség érdekében lehetőség szerint koherens megközelítést kell biztosítani ezen irányelv és az (EU) 2022/2555 európai parlamenti és tanácsi irányelv ([5]) között. Szem előtt tartva a kiberkockázatok nagyobb gyakoriságát és sajátos jellemzőit, az (EU) 2022/2555 irányelv a szervezetek széles köre számára átfogó követelményeket szab meg kiberbiztonságuk biztosítása érdekében. Tekintve, hogy az (EU) 2022/2555 említett irányelv kellő mértékben foglalkozik a kiberbiztonsággal, az említett irányelv hatálya alá tartozó kérdéseket ki kell zárni ezen irányelv hatálya alól, a digitálisinfrastruktúra-ágazatban működő szervezetekre vonatkozó különös szabályozás sérelme nélkül.

(10) Amennyiben ágazatspecifikus uniós jogi aktusok rendelkezései előírják a kritikus szervezetek számára, hogy hozzanak intézkedéseket rezilienciájuk fokozása érdekében, és amennyiben az említett követelményeket a tagállamok legalább egyenértékűnek ismerik el az ezen irányelvben meghatározott megfelelő kötelezettségekkel, az átfedések és a szükségtelen terhek elkerülése érdekében ezen irányelv releváns rendelkezéseit nem kell alkalmazni. Ebben az esetben az ilyen uniós jogi aktusok releváns rendelkezéseit kell alkalmazni. Amennyiben ezen irányelv releváns rendelkezései nem alkalmazandók, a felügyeletre és a jogérvényesítésre vonatkozó, ezen irányelvben megállapított rendelkezések sem alkalmazandók.

(11) Ezen irányelv nem érinti a tagállamok és hatóságaik hatásköreit az igazgatási autonómia tekintetében, vagy a nemzetbiztonság és védelem megőrzésére vonatkozó felelősségét, vagy az egyéb alapvető állami funkciók védelmére vonatkozó hatáskörüket, különösen a közbiztonságra, a területi integritásra és a közrend fenntartására vonatkozóan. A közigazgatási szervezetek ezen irányelv hatálya alóli kizárását olyan szervezetekre kell alkalmazni, amelyek tevékenységeiket túlnyomórészt a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés területén – beleértve a bűncselekményekre irányuló nyomozást, felderítést és vádeljárás lefolytatását is – végzik. Azon közigazgatási szervezeteknek azonban, amelyek tevékenységei csak marginálisan kapcsolódnak az említett területekhez, ezen irányelv hatálya alá kell tartozniuk. Ezen irányelv alkalmazásában a szabályozási hatáskörrel rendelkező szervezetek nem tekintendők a bűnüldözés területén tevékenységeket folytató szervezetnek, és ezért nincsenek az említett alapon kizárva ezen irányelv hatálya alól. Azon közigazgatási szervezetek, amelyeket valamely nemzetközi megállapodásnak megfelelően egy harmadik országgal közösen hoznak létre, ki vannak zárva ezen irányelv hatálya alól. Ezen irányelv nem alkalmazandó a tagállamok harmadik országokban működő diplomáciai és konzuli képviseleteire.

([5]) Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (lásd e Hivatalos Lap 80. oldalát).

Egyes kritikus szervezetek a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés területén folytatnak tevékenységeket, beleértve a bűncselekményekre irányuló nyomozást, felderítést és vádeljárás lefolytatását is, vagy kizárólag olyan közigazgatási szervezetek számára nyújtanak szolgáltatásokat, amelyek tevékenységüket túlnyomórészt az említett területeken végzik. Tekintettel a tagállamoknak a nemzetbiztonság és védelem megőrzésére irányuló felelősségére, a tagállamok dönthetnek úgy, hogy a kritikus szervezetekre vonatkozó, ezen irányelvben megállapított kötelezettségek részben vagy egészben nem alkalmazandók az említett kritikus szervezetekre, ha az általuk nyújtott szolgáltatások vagy az általuk végzett tevékenységek túlnyomórészt a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés területéhez kapcsolódnak, beleértve a bűncselekményekre irányuló nyomozást, felderítést és vádeljárás lefolytatását is. Azon kritikus szervezeteknek, amelyek szolgáltatásai vagy tevékenységei csak marginálisan kapcsolódnak az említett területekhez, ezen irányelv hatálya alá kell tartozniuk. Egyetlen tagállamot sem lehet arra kötelezni, hogy olyan információkat szolgáltasson, amelyek közlése ellentétes lenne nemzetbiztonságának alapvető érdekeivel. Relevanciával bírnak a minősített adatok védelmére vonatkozó uniós vagy nemzeti szabályok, valamint a titoktartási megállapodások.

(12) Annak érdekében, hogy ne veszélyeztessék a nemzetbiztonságot vagy a kritikus szervezetek biztonságát és kereskedelmi érdekeit, az érzékeny információkhoz való hozzáférést, azok cseréjét és kezelését gondosan kell végezni, továbbá különös figyelemmel a felhasznált továbbítási csatornákra és tárolási kapacitásokra.

(13) A kritikus szervezetek rezilienciájára vonatkozó átfogó megközelítés biztosítása céljából mindegyik tagállamnak rendelkeznie kell a kritikus szervezetek rezilienciájának erősítését célzó stratégiával (a továbbiakban: a stratégia). A stratégiának meg kell határoznia a stratégiai célkitűzéseket és a végrehajtandó szakpolitikai intézkedéseket. A koherencia és a hatékonyság érdekében a stratégiát úgy kell kialakítani, hogy gördülékenyen integrálja a meglévő szakpolitikákat, ahol lehetséges, építve a releváns, meglévő nemzeti és ágazati stratégiákra, tervekre vagy hasonló dokumentumokra. Az átfogó megközelítés elérése érdekében a tagállamoknak biztosítaniuk kell, hogy a stratégiájuk szakpolitikai keretet biztosítson az ezen irányelv szerinti illetékes hatóságok és az (EU) 2022/2555 irányelv szerinti illetékes hatóságok közötti fokozott koordinációhoz, a kiberbiztonsági kockázatokra, a kiberfenyegetésekre és kiberjellegű eseményekre, valamint a nem kiberjellegű kockázatokra, fenyegetésekre és eseményekre vonatkozó információmegosztással és a felügyeleti feladatok ellátásával összefüggésben. A stratégiájuk bevezetésekor a tagállamoknak kellően figyelembe kell venniük a kritikus szervezetekkel szembeni fenyegetések hibrid jellegét.

(14) A tagállamoknak továbbítaniuk kell a Bizottság részére a stratégiájukat és annak jelentősen aktualizált változatait, különösen annak lehetővé tétele érdekében, hogy a Bizottság értékelje ezen irányelv helyes alkalmazását a kritikus szervezetek rezilienciájával kapcsolatos nemzeti szintű szakpolitikai megközelítéseket illetően. A stratégiák szükség esetén minősített információként is továbbíthatók. A Bizottságnak összefoglaló jelentést kell készítenie a tagállamok által továbbított stratégiákról, hogy alapul szolgáljon a kritikus szervezetek rezilienciájával foglalkozó csoport keretében a legjobb gyakorlatok és a közös érdekű kérdések azonosítása céljából folytatott megbeszélésekhez. Az összefoglaló jelentésben foglalt aggregált információk érzékeny jellege miatt – függetlenül attól, hogy azok minősített adatok-e vagy sem – a Bizottságnak az összefoglaló jelentést a kritikus szervezetek, a tagállamok és az Unió biztonsága tekintetében a megfelelő szintű tudatossággal kell kezelnie. Az összefoglaló jelentést és a stratégiákat meg kell őrizni a jogellenes vagy rosszindulatú cselekményekkel szemben, és azokat csak az arra felhatalmazott személyek számára szabad hozzáférhetővé tenni ezen irányelv célkitűzéseinek teljesítése érdekében. A stratégiák és azok jelentősen aktualizált változatai továbbításának segítenie kell a Bizottságot annak megértésében is, hogy milyen fejlemények történtek a kritikus szervezetek rezilienciájával kapcsolatos megközelítések terén, és hozzá kell járulnia ezen irányelv hatásának és hozzáadott értékének monitorozásához, amit a Bizottságnak időszakosan felül kell vizsgálnia.

(15) A kritikus szervezetek azonosítására és rezilienciájának biztosítására irányuló tagállami intézkedéseknek kockázatalapú megközelítést kell követniük, amely az alapvető fontosságú társadalmi funkciók vagy gazdasági tevékenységek ellátása szempontjából leginkább releváns szervezetekre koncentrál. Az ilyen célzott megközelítés biztosítása érdekében egy összehangolt kereten belül minden egyes tagállamnak el kell végeznie az olyan releváns természeti és ember okozta kockázatok értékelését – ideértve a több ágazatot érintő, illetve a határokon átnyúló jellegű kockázatokat is –, amelyek hatással lehetnek az alapvető szolgáltatások nyújtására, beleértve a baleseteket, a természeti katasztrófákat, a népegészségügyi szükséghelyzeteket, így például a világjárványokat és a hibrid fenyegetéseket vagy egyéb ellenséges fenyegetéseket, ideértve a terrorista bűncselekményeket, a bűncselekményi célú beszivárgást és a szabotázst (a továbbiakban: tagállami kockázatértékelés). A tagállami kockázatértékelések elvégzésekor a tagállamoknak szem előtt kell tartaniuk a más uniós jogi aktusok alapján elvégzett egyéb általános vagy ágazatspecifikus kockázatértékeléseket, és figyelembe kell venniük annak mértékét, amennyire az ágazatok egymástól függenek, ideértve a más tagállamokbeli és a harmadik országbeli ágazatoktól is. A tagállami kockázatértékelés eredményét fel kell használni a kritikus szervezetek azonosítása céljából, és arra, hogy segítsen az

említett szervezeteknek a reziliencia-követelményeik teljesítésében. Ezen irányelv csak a tagállamokra és az Unión belül működő kritikus szervezetekre alkalmazandó. Mindazonáltal, adott esetben és az alkalmazandó jogi eszközökkel összhangban fel lehetne használni a harmadik országok – különösen az Unió közvetlen szomszédságában fekvő országok – javára azon szakértelmet és tudást, amelyet az illetékes hatóságok különösen a kockázatértékelések révén generálnak, és amelyet a Bizottság különösen a különböző támogatási és együttműködési formák révén generál, beépítve azokat a rezilienciával kapcsolatos meglévő együttműködésbe.

(16) Annak biztosítása érdekében, hogy ezen irányelv reziliencia-követelményei valamennyi releváns szervezetre vonatkozzanak, és csökkenjenek az e tekintetben mutatkozó eltérések, fontos olyan harmonizált szabályokat megállapítani, amelyek Unió-szerte lehetővé teszik a kritikus szervezetek következetes azonosítását, egyúttal lehetővé teszik a tagállamok számára, hogy megfelelően tükrözzék az említett szervezetek nemzeti szinten betöltött szerepét és jelentőségét. Az ezen irányelvben meghatározott kritériumok alkalmazása során minden egyes tagállamnak azonosítania kell azon szervezeteket, amelyek egy vagy több alapvető szolgáltatást nyújtanak, valamint amelyek a területén működnek és ott kritikus infrastruktúrával rendelkeznek. Úgy tekintendő, hogy egy szervezet azon tagállam területén működik, amelyben a szóban forgó alapvető szolgáltatáshoz vagy szolgáltatásokhoz szükséges tevékenységeket végez, és amelyben az említett szervezetnek az említett szolgáltatás vagy szolgáltatások nyújtásához használt kritikus infrastruktúrája található. Amennyiben egy tagállamban egyik szervezet sem felel meg az említett kritériumoknak, az említett tagállam nem kötelezhető arra, hogy kritikus szervezetet azonosítson a vonatkozó ágazatban vagy alágazatban. Az eredményesség, a hatékonyság, a következetesség és a jogbiztonság érdekében megfelelő szabályokat kell meghatározni a szervezetek arról való értesítésére vonatkozóan, hogy kritikus szervezetként azonosították őket.

(17) A tagállamoknak az ezen irányelv célkitűzéseit teljesítő módon be kell nyújtaniuk a Bizottság részére az alapvető szolgáltatások jegyzékét, a mellékletben meghatározott egyes ágazatok és alágazatok, valamint az egyes szervezetek által nyújtott alapvető szolgáltatás vagy szolgáltatások tekintetében azonosított kritikus szervezetek számát, valamint – ha alkalmazandó – a küszöbértékeket. Lehetővé kell tenni a küszöbérték közlését önmagában vagy aggregált formában, ami azt jelenti, hogy az adatokat lehet földrajzi terület, év, ágazat vagy alágazat szerint, illetve egyéb módon átlagolni, és azok információt tartalmazhatnak a megadott mutatók köréről.

(18) Kritériumokat kell megállapítani egy esemény által keltett zavaró hatás jelentőségének meghatározásához. Az említett kritériumoknak az (EU) 2016/1148 európai parlamenti és tanácsi irányelvben ([6]) meghatározott kritériumokra kell épülniük annak érdekében, hogy ki lehessen aknázni az említett irányelvben meghatározott, alapvető szolgáltatásokat üzemeltetők azonosítására tett tagállami erőfeszítéseket és az e tekintetben szerzett tapasztalatokat. Az olyan jelentős válságok, mint például a Covid19-világjárvány, megmutatták, hogy fontos biztosítani az ellátási lánc biztonságát, és rávilágítottak arra, hogy annak megzavarása miként jár negatív gazdasági és társadalmi hatással számos ágazatban és a határokon átnyúlóan. Ezért a tagállamoknak a lehetőségekhez mérten figyelembe kell venniük az ellátási láncra gyakorolt hatásokat is, amikor meghatározzák, hogy egyéb ágazatok és alágazatok milyen mértékben függenek egy kritikus szervezet által nyújtott alapvető szolgáltatástól.

(19) Az alkalmazandó uniós és nemzeti joggal, többek között az Unióba irányuló közvetlen külföldi befektetések átvilágítási keretét létrehozó (EU) 2019/452 európai parlamenti és tanácsi rendelettel ([7]) összhangban figyelembe kell venni az Unión belüli kritikus infrastruktúra külföldi tulajdonba kerülése által jelentett potenciális veszélyt, mivel a szolgáltatások, a gazdaság, valamint az uniós polgárok szabad mozgása és biztonsága függ a kritikus infrastruktúra megfelelő működésétől.

(20) Az (EU) 2022/2555 irányelv előírja a digitálisinfrastruktúra-ágazathoz tartozó azon szervezetek számára, amelyek ezen irányelv alapján kritikus szervezetként azonosíthatóak, hogy hozzanak megfelelő és arányos technikai, operatív és szervezeti intézkedéseket a hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése, valamint a jelentős eseményekre és kiberfenyegetésekre vonatkozó értesítés érdekében. Mivel a hálózati és információs rendszerek biztonságát érintő fenyegetések eredete különböző lehet, az (EU) 2022/2555 irányelv minden veszélyre kiterjedő megközelítést alkalmaz, amelybe beletartozik a hálózati és információs rendszereknek, valamint az említett rendszerek fizikai alkotóelemeinek és környezetének a rezilienciája is.

([6]) 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.).

([7]) Az Európai Parlament és a Tanács (EU) 2019/452 rendelete (2019. március 19.) az Unióba irányuló közvetlen külföldi befektetések átvilágítási keretének létrehozásáról (HL L 79. I., 2019.3.21., 1. o.).

Tekintve, hogy az (EU) 2022/2555 irányelvben e tekintetben megállapított követelmények legalább egyenértékűek az ezen irányelvben megállapított megfelelő kötelezettségekkel, az átfedések és a szükségtelen terhek elkerülése érdekében az ezen irányelv 11. cikkében, valamint III., IV. és VI. fejezetében megállapított kötelezettségek nem alkalmazhatók a digitálisinfrastruktúra-ágazathoz tartozó szervezetekre. Figyelembe véve azonban a digitálisinfrastruktúra-ágazathoz tartozó szervezetek által nyújtott szolgáltatások fontosságát a valamennyi egyéb ágazathoz tartozó, kritikus szervezetek számára, a tagállamoknak – az ezen irányelvben előírt kritériumok alapján és eljárást alkalmazva – kritikus szervezetekként kell azonosítaniuk a digitálisinfrastruktúra-ágazathoz tartozó szervezeteket. Következésképpen alkalmazni kell az ezen irányelv II. fejezetében meghatározott stratégiákat, tagállami kockázatértékeléseket és támogatási intézkedéseket. A tagállamok számára lehetővé kell tenni, hogy nemzeti jogi rendelkezéseket fogadjanak el vagy tartsanak fenn az említett kritikus szervezetek magasabb szintű rezilienciájának elérése érdekében, feltéve, hogy az említett rendelkezések összhangban vannak az alkalmazandó uniós joggal.

(21) A pénzügyi szolgáltatásokra vonatkozó uniós jog átfogó követelményeket állapít meg a pénzügyi szervezetek tekintetében az őket érintő valamennyi kockázat, köztük a működési kockázatok kezelése, és az üzletmenet-folytonosság biztosítása érdekében. Az ilyen jog körébe tartozik a 648/2012/EU ([8]), az 575/2013/EU ([9]) és a 600/2014/EU ([10]) európai parlamenti és tanácsi rendelet, valamint a 2013/36/EU ([11]) és a 2014/65/EU ([12]) európai parlamenti és tanácsi irányelv. Az említett jogi keret kiegészül az (EU) 2022/2554 európai parlamenti és tanácsi rendelettel ([13]), amely az információs és kommunikációs technológiai (IKT) kockázatok kezelését célzó, a pénzügyi szervezetekre alkalmazandó követelményeket állapít meg, ideértve a fizikai IKT-infrastruktúra védelmére vonatkozóan is. Mivel az említett szervezetek rezilienciája ezért átfogóan szabályozott, az átfedések és a szükségtelen terhek elkerülése érdekében ezen irányelv 11. cikke, valamint III., IV. és VI. fejezete az említett szervezetekre nem alkalmazandó.

Figyelembe véve azonban a pénzügyi ágazatban működő szervezetek által nyújtott szolgáltatások fontosságát a valamennyi egyéb ágazathoz tartozó, kritikus szervezetek számára, a tagállamoknak – az ezen irányelvben előírt kritériumok alapján és eljárást alkalmazva – kritikus szervezetekként kell azonosítaniuk a pénzügyi ágazatban működő szervezeteket. Következésképpen alkalmazni kell az ezen irányelv II. fejezetében meghatározott stratégiákat, a tagállami kockázatértékeléseket és támogatási intézkedéseket. A tagállamok számára lehetővé kell tenni, hogy nemzeti jogi rendelkezéseket fogadjanak el vagy tartsanak fenn az említett kritikus szervezetek magasabb szintű rezilienciájának elérése érdekében, feltéve, hogy az említett rendelkezések összhangban vannak az alkalmazandó uniós joggal.

(22) A tagállamoknak illetékes hatóságokat kell kijelölniük vagy létrehozniuk az ezen irányelvben foglalt szabályok alkalmazásának felügyeletére és szükség esetén érvényesítésére, valamint biztosítaniuk kell, hogy az említett hatóságok megfelelő felhatalmazással és forrásokkal rendelkezzenek. A nemzeti kormányzási struktúrák közötti különbségek fényében, a meglévő ágazati intézkedések vagy az uniós felügyeleti és szabályozó szervek megóvása érdekében, és az átfedések elkerülése érdekében a tagállamok számára lehetővé kell tenni, hogy egynél több illetékes hatóságot jelöljenek ki vagy hozzanak létre. Amennyiben a tagállamok egynél több illetékes hatóságot jelölnek ki vagy hoznak létre, világosan körül kell határolniuk az érintett hatóságok vonatkozó feladatait, és biztosítaniuk kell, hogy zökkenőmentesen és hatékonyan működjenek együtt. Valamennyi illetékes hatóságnak általánosabban véve együtt kell működnie más releváns hatóságokkal, uniós és nemzeti szinten egyaránt.

([8]) 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.).

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

([10]) Az Európai Parlament és a Tanács 600/2014/EU rendelete (2014. május 15.) a pénzügyi eszközök piacairól és a 648/2012/EU rendelet módosításáról (HL L 173., 2014.6.12., 84. o.).

([11]) 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.).

([12]) Az Európai Parlament és a Tanács 2014/65/EU irányelve (2014. május 15.) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról (HL L 173., 2014.6.12., 349. o.).

([13]) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) 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 (lásd e Hivatalos Lap 1. oldalát).

(23) A határokon átnyúló együttműködés és kommunikáció elősegítése, valamint ezen irányelv eredményes végrehajtása érdekében minden egyes tagállamnak – az ágazatspecifikus uniós jogi aktusok követelményeinek sérelme nélkül – ki kell jelölnie egy, a kritikus szervezetek rezilienciájával kapcsolatos kérdések koordinálásáért és az uniós szintű, határokon átnyúló együttműködésért felelős egyedüli kapcsolattartó pontot (a továbbiakban: egyedüli kapcsolattartó pont) adott esetben valamely illetékes hatóságon belül. Mindegyik egyedüli kapcsolattartó pontnak kapcsolatot kell fenntartania, és adott esetben koordinálnia kell a kommunikációt a tagállamának illetékes hatóságaival, a többi tagállam egyedüli kapcsolattartó pontjával és a kritikus szervezetek rezilienciájával foglalkozó csoporttal.

(24) Az ezen irányelv szerinti illetékes hatóságoknak és az (EU) 2022/2555 irányelv szerinti illetékes hatóságoknak együtt kell működniük és információkat kell cserélniük a kritikus szervezeteket érintő kiberbiztonsági kockázatokkal, kiberfenyegetésekkel és kiberjellegű eseményekkel, valamint a nem kiberjellegű kockázatokkal, fenyegetésekkel és eseményekkel kapcsolatban, továbbá az ezen irányelv szerinti illetékes hatóságok és az (EU) 2022/2555 irányelv szerinti illetékes hatóságok által hozott releváns intézkedésekkel kapcsolatban. Fontos, hogy a tagállamok biztosítsák az ezen irányelvben és az (EU) 2022/2555 irányelvben előírt követelmények kiegészítő módon történő végrehajtását, és azt, hogy a kritikus szervezetekre ne háruljanak azon túlmenő adminisztratív terhek, mint ami szükséges az ezen irányelv és az említett irányelv célkitűzéseinek eléréséhez.

(25) A tagállamoknak támogatniuk kell a kritikus szervezeteket – ideértve azokat is, amelyek kis- és középvállalkozásoknak minősülnek – rezilienciájuknak az ezen irányelvben megállapított tagállami kötelezettségeknek megfelelő megerősítésében, a kritikus szervezeteknek az ilyen megfelelés biztosítására irányuló saját jogi felelősségének sérelme nélkül, és ennek során meg kell előzniük a túlzott adminisztratív terheket. A tagállamok így különösen iránymutatásokat és módszereket dolgozhatnak ki, támogathatják a kritikus szervezetek rezilienciájának tesztelését szolgáló gyakorlatok szervezését, valamint tanácsadást és képzést biztosíthatnak a kritikus szervezetek személyzete számára. Amennyiben szükséges és azt közérdekű célkitűzések indokolják, a tagállamok pénzügyi forrásokat biztosíthatnak, és elő kell segíteniük a kritikus szervezetek közötti önkéntes információmegosztást és a bevált gyakorlatok cseréjét, az Európai Unió működéséről szóló szerződésben (EUMSZ) megállapított versenyszabályok alkalmazásának sérelme nélkül.

(26) A tagállamok által azonosított, kritikus szervezetek rezilienciájának fokozása és az említett kritikus szervezetekre nehezedő adminisztratív terhek csökkentése céljából az illetékes hatóságoknak adott esetben konzultálniuk kell egymással annak biztosítása céljából, hogy ezen irányelvet következetes módon alkalmazzák. Az említett konzultációkat bármely érdekelt illetékes hatóság kérésére meg kell indítani, és azoknak egy konvergáló megközelítés biztosítására kell összpontosítaniuk az egymással összekapcsolt azon kritikus szervezetek vonatkozásában, amelyek két vagy több tagállam között fizikailag összekötött kritikus infrastruktúrát használnak, amelyek ugyanazon csoportokhoz vagy vállalati struktúrákhoz tartoznak, vagy amelyeket egy tagállamban azonosítottak, és amelyek más tagállamok számára vagy más tagállamokban nyújtanak alapvető szolgáltatásokat.

(27) Amennyiben az uniós vagy a nemzeti jog rendelkezései előírják a kritikus szervezetek számára, hogy értékeljék az ezen irányelv céljából releváns kockázatokat, és hozzanak intézkedéseket saját rezilienciájuk biztosítása érdekében, az említett követelményeket megfelelően figyelembe kell venni a kritikus szervezetek ezen irányelvnek való megfelelése felügyeletének céljából.

(28) A kritikus szervezeteknek átfogó ismeretekkel kell rendelkezniük az őket érintő releváns kockázatokról, és kötelezettséggel arra, hogy elemezzék az említett kockázatokat. E célból kockázatértékeléseket kell végezniük, valahányszor szükséges a sajátos körülményeikre és az említett kockázatok alakulására tekintettel, és egyébként négyévente, valamennyi olyan releváns kockázat értékelése érdekében, amely akadályozhatja az alapvető szolgáltatásaik nyújtását (a továbbiakban: kritikus szervezet általi kockázatértékelés). Amennyiben a kritikus szervezetek más jogi aktusokban megállapított kötelezettségek alapján egyéb olyan kockázatértékeléseket végeztek, vagy olyan dokumentumokat készítettek, amelyek a kritikus szervezetek általi kockázatértékelés szempontjából relevánsak, képesnek kell lenniük arra, hogy az említett értékeléseket és dokumentumokat felhasználják a kritikus szervezet általi kockázatértékelésre vonatkozóan ezen irányelvben meghatározott követelményeknek való megfelelés érdekében. Lehetővé kell tenni valamely illetékes hatóság számára, hogy kijelentse, egy kritikus szervezet által végzett meglévő kockázatértékelés, amely kitér a releváns kockázatokra és a függőség releváns mértékére, részben vagy egészben megfelel az ezen irányelvben megállapított kötelezettségeknek.

(29) A kritikus szervezeteknek megfelelő és az őket érintő kockázatokkal arányos technikai, biztonsági és szervezeti intézkedéseket kell hozniuk, hogy megelőzzenek valamely eseményt, védekezzenek azzal szemben, reagáljanak arra, ellenálljanak annak, enyhítsék, tompítsák azt, alkalmazkodjanak ahhoz, és abból helyreálljanak. Míg a kritikus szervezeteknek ezen irányelvvel összhangban kell meghozniuk az említett intézkedéseket, az ilyen intézkedések részleteinek és mértékének megfelelő és arányos módon tükrözniük kell az egyes kritikus szervezetek által a kritikus szervezet általi kockázatértékelés részeként azonosított különböző kockázatokat és az ilyen szervezet sajátosságait. A koherens uniós megközelítés előmozdítása érdekében a Bizottságnak – a kritikus szervezetek rezilienciájával foglalkozó csoporttal folytatott konzultációt követően – nem kötelező erejű iránymutatásokat kell elfogadnia az említett technikai, biztonsági és szervezeti intézkedések további pontosítása érdekében. A tagállamoknak biztosítaniuk kell, hogy mindegyik kritikus szervezet kijelöljön egy összekötő tisztviselőt vagy egy ezzel egyenértékű személyt kapcsolattartó pontként az illetékes hatóságok felé.

(30) A hatékonyság és az elszámoltathatóság érdekében a kritikus szervezeteknek – a rezilienciatervben vagy a rezilienciatervvel egyenértékű dokumentumban, illetve dokumentumokban azonosított kockázatok figyelembevételével – a hatékonysági és elszámoltathatósági célok elégséges eléréséhez szükséges részletességgel ismertetniük kell az általuk hozott intézkedéseket, és a gyakorlatban is alkalmazniuk kell az említett tervet. Amennyiben a kritikus szervezet már hozott technikai, biztonsági és szervezeti intézkedéseket, valamint az ezen irányelv szerinti reziliencia-fokozó intézkedések szempontjából releváns egyéb jogi aktusok alapján készített dokumentumokat, az átfedések elkerülése érdekében lehetővé kell tenni számára, hogy alkalmazza az említett intézkedéseket és dokumentumokat az ezen irányelv szerinti reziliencia-intézkedések tekintetében fennálló követelmények teljesítéséhez. Az átfedések elkerülése érdekében lehetővé kell tenni az illetékes hatóság számára, hogy kijelentse, egy kritikus szervezet által hozott olyan meglévő reziliencia-intézkedések, amelyek kitérnek a technikai, biztonsági és szervezeti intézkedések meghozatalára vonatkozó, ezen irányelv szerinti kötelezettségére, részben vagy egészben megfelelnek ezen irányelv követelményeinek.

(31) A 725/2004/EK ([14]) és a 300/2008/EK európai parlamenti és tanácsi rendelet ([15]), valamint a 2005/65/EK európai parlamenti és tanácsi irányelv ([16]) a légi közlekedési és a tengeri szállítási ágazatban működő szervezetekre vonatkozó követelményeket állapít meg a jogellenes cselekmények által okozott események megelőzése, valamint az ilyen események következményeinek való ellenállás és azok enyhítése érdekében. Bár a kezelt kockázatok és a meghozandó intézkedések típusai tekintetében az ezen irányelv alapján előírt intézkedések szélesebb körűek, az említett ágazatokban tevékenykedő kritikus szervezetek reziliencia-tervében vagy azzal egyenértékű dokumentumaiban tükröződniük kell az említett egyéb uniós jogi aktusok alapján hozott intézkedéseknek. A kritikus szervezeteknek figyelembe kell venniük a 2008/96/EK európai parlamenti és tanácsi irányelvet ([17]) is, amely egy hálózati szintű közúti felmérést vezet be a balesetek kockázatának feltérképezése érdekében, valamint egy célzott közúti közlekedésbiztonsági felülvizsgálatot a balesetek és sérülések kockázatát fokozó veszélyes körülmények, hibák és problémák azonosítása érdekében, amely meglévő utak vagy útszakaszok helyszíni bejárásain alapul. A kritikus szervezetek védelmének és rezilienciájának biztosítása kiemelkedő fontosságú a vasúti ágazat számára, és az ezen irányelv szerinti reziliencia-intézkedések végrehajtásakor a kritikus szervezeteket arra kell ösztönözni, hogy vegyék figyelembe az ágazati munkafolyamatok keretében kidolgozott, nem kötelező erejű iránymutatásokat és a bevált gyakorlatokat tartalmazó dokumentumokat, így például a 2018/C 232/03 bizottsági határozattal ([18]) létrehozott Európai Uniós Vasúti Utasbiztonsági Platformot.

(32) Növekvő aggodalomra ad okot annak kockázata, hogy a kritikus szervezetek alkalmazottai vagy vállalkozóik sérelem- és károkozás céljából visszaélnek például a kritikus szervezeten belüli hozzáférési jogaikkal. A tagállamoknak ezért pontosan meg kell határozniuk azon feltételeket, amelyek mellett a kritikus szervezetek számára megengedett, hogy – kellően indokolt esetekben és a tagállami kockázatértékelések figyelembevételével – kérelmezzék a személyzetük meghatározott kategóriáiba tartozó személyek háttérellenőrzését. Biztosítani kell, hogy a releváns hatóságok észszerű határidőn belül értékeljék az ilyen kérelmeket, és azokat a nemzeti jogszabályokkal és eljárásokkal, valamint a releváns és alkalmazandó, többek között a személyes adatok védelmére vonatkozó uniós joggal összhangban dolgozzák fel. Azon személy személyazonosságának megerősítése érdekében, aki háttérellenőrzésen esik át, helyénvaló, hogy a tagállamok az alkalmazandó joggal összhangban előírják a személyazonosság igazolását, így például útlevéllel, nemzeti személyazonosító igazolvánnyal vagy digitális személyazonosító formában.

([14]) Az Európai Parlament és a Tanács 725/2004/EK rendelete (2004. március 31.) a hajók és kikötőlétesítmények védelmének fokozásáról (HL L 129., 2004.4.29., 6. o.).

([15]) Az Európai Parlament és a Tanács 300/2008/EK rendelete (2008. március 11.) a polgári légi közlekedés védelmének közös szabályairól és a 2320/2002/EK rendelet hatályon kívül helyezéséről (HL L 97., 2008.4.9., 72. o.).

([16]) Az Európai Parlament és a Tanács 2005/65/EK irányelve (2005. október 26.) a kikötővédelem fokozásáról (HL L 310., 2005.11.25., 28. o.).

([17]) Az Európai Parlament és a Tanács 2008/96/EK irányelve (2008. november 19.) a közúti infrastruktúra közlekedésbiztonsági kezeléséről (HL L 319., 2008.11.29., 59. o.).

([18]) A Bizottság határozata (2018. június 29.) az Európai Uniós Vasúti Utasbiztonsági Platform létrehozásáról (2018/C 232/03, HL C 232., 2018.7.3., 10. o.).

A háttérellenőrzéseknek ki kell terjedniük az érintett személyre vonatkozó bűnügyi nyilvántartások ellenőrzésére is. A tagállamoknak a 2009/315/IB tanácsi kerethatározatban ([19]), valamint – adott esetben és amennyiben alkalmazandó – az (EU) 2019/816 európai parlamenti és tanácsi rendeletben ([20]) meghatározott eljárásoknak megfelelően az Európai Bűnügyi Nyilvántartási Információs Rendszert (ECRIS) kell igénybe venniük abból a célból, hogy beszerezzék a más tagállamok által fenntartott bűnügyi nyilvántartásokból származó információkat. A tagállamok – adott esetben és amennyiben alkalmazandó – támaszkodhatnak az (EU) 2018/1862 európai parlamenti és tanácsi rendelettel ([21]) létrehozott Schengeni Információs Rendszer második generációjára (SIS II), hírszerzési adatokra és bármely egyéb, rendelkezésre álló objektív információra, amely szükséges lehet annak megállapításához, hogy az érintett személy alkalmas-e arra, hogy azon pozícióban dolgozzon, amellyel kapcsolatban a kritikus szervezet háttérellenőrzést kért.

(33) Ki kell alakítani a bizonyos eseményekről szóló értesítést szolgáló mechanizmust annak lehetővé tétele érdekében, hogy az illetékes hatóságok gyorsan és megfelelően reagáljanak az eseményekre, továbbá hogy átfogó képpel rendelkezzenek azon események hatásairól, jellegéről, okáról és lehetséges következményeiről, amelyekkel a kritikus szervezetek szembesülnek. A kritikus szervezeteknek indokolatlan késedelem nélkül értesíteniük kell az illetékes hatóságokat azon eseményekről, amelyek jelentősen megzavarják, vagy alkalmasak lehetnek arra, hogy jelentős megzavarják az alapvető szolgáltatások nyújtását. A kritikus szervezeteknek legkésőbb 24 órán belül be kell nyújtaniuk a kezdeti értesítést azt követően, hogy tudomást szereztek egy eseményről, kivéve, ha ezt operatív okokból nem képesek megtenni. A kezdeti értesítésnek csak azon információkat kell tartalmaznia, amelyek feltétlenül szükségesek ahhoz, hogy az illetékes hatóság tudomást szerezzen az eseményről, és lehetővé teszik a kritikus szervezet számára, hogy szükség esetén segítséget kérjen. Egy ilyen értesítésnek lehetőség szerint meg kell jelölnie az esemény feltételezett okát. A tagállamoknak biztosítaniuk kell, hogy a kezdeti értesítés benyújtására vonatkozó követelmény ne vonja el a kritikus szervezet erőforrásait az esemény kezelésével kapcsolatos tevékenységektől, amelyeket prioritásként kell kezelni. A kezdeti értesítést az eseményt követő legkésőbb egy hónappal adott esetben részletes jelentésnek kell követnie. A részletes jelentésnek ki kell egészítenie a kezdeti értesítést, és teljesebb áttekintést kell nyújtania az eseményről.

(34) A szabványosításnak elsősorban piacvezérelt folyamatnak kell maradnia. Előfordulhatnak azonban még olyan helyzetek, amelyekben helyénvaló előírni a meghatározott szabványoknak való megfelelést. A tagállamoknak – amikor az hasznosnak bizonyul – ösztönözniük kell a kritikus szervezetekre alkalmazandó biztonsági és reziliencia-intézkedések szempontjából releváns, európai és nemzetközi szabványok és technikai előírások alkalmazását.

(35) Bár a kritikus szervezetek általában egyre szorosabban összekapcsolt szolgáltatásnyújtási és infrastrukturális hálózat részeként működnek, valamint gyakran egynél több tagállamban nyújtanak alapvető szolgáltatásokat, az említett kritikus szervezetek némelyike különös jelentőséggel bír az Unió és annak belső piaca tekintetében, mivel hat vagy több tagállam számára, illetve tagállamban nyújtanak alapvető szolgáltatásokat, és ezért uniós szintű egyedi támogatásban részesülhetnek. Szabályokat kell ezért megállapítani az ilyen különös európai jelentőségű kritikus szervezetek tekintetében a tanácsadó missziókra vonatkozóan. Az említett szabályok nem érintik az ezen irányelvben meghatározott, felügyeletre és jogérvényesítésre vonatkozó szabályokat.

(36) A Bizottság, vagy egy vagy több olyan tagállam indokolással ellátott megkeresése alapján, amely számára vagy amelyben az alapvető szolgáltatást nyújtják, amennyiben további információra van szükség ahhoz, hogy tanácsot lehessen adni egy kritikus szervezetnek az ezen irányelv alapján fennálló kötelezettségeinek teljesítéséhez vagy ahhoz, hogy értékelni lehessen, hogy egy különös európai jelentőségű, kritikus szervezet megfelel-e az említett kötelezettségeknek, azon tagállamnak, amely kritikus szervezetként azonosított egy különös európai jelentőségű kritikus szervezetet, a Bizottság rendelkezésére kell bocsátania bizonyos információkat az ezen irányelvben foglaltaknak megfelelően. A Bizottság számára lehetővé kell tenni, hogy – azon tagállammal egyetértésben, amely kritikus szervezetként azonosította a különös európai jelentőségű kritikus szervezetet – tanácsadó missziót szervezzen a szóban forgó szervezet által foganatosított intézkedések értékelésére. Az ilyen tanácsadó missziók megfelelő végrehajtásának biztosítása érdekében kiegészítő szabályokat kell megállapítani, különösen a tanácsadó missziók megszervezésére és lebonyolítására, a megteendő utánkövetési tevékenységekre és az érintett különös

([19]) A Tanács 2009/315/IB kerethatározata (2009. február 26.) a bűnügyi nyilvántartásból származó információk tagállamok közötti cseréjének megszervezéséről és azok tartalmáról (HL L 93., 2009.4.7., 23. o.).

([20]) Az Európai Parlament és a Tanács (EU) 2019/816 rendelete (2019. április 17.) az Európai Bűnügyi Nyilvántartási Információs Rendszer kiegészítése érdekében a harmadik országbeli állampolgárokkal és a hontalan személyekkel szemben hozott ítéletekre vonatkozó információval rendelkező tagállamok azonosítására szolgáló központosított rendszer (ECRIS-TCN) létrehozásáról, valamint az (EU) 2018/1726 rendelet módosításáról (HL L 135., 2019.5.22., 1. o.).

([21]) Az Európai Parlament és a Tanács (EU) 2018/1862 rendelete (2018. november 28.) a rendőrségi együttműködés és a büntetőügyekben folytatott igazságügyi együttműködés terén a Schengeni Információs Rendszer (SIS) létrehozásáról, működéséről és használatáról, a 2007/533/IB tanácsi határozat módosításáról és hatályon kívül helyezéséről, valamint az 1986/2006/EK európai parlamenti és tanácsi rendelet és a 2010/261/EU bizottsági határozat hatályon kívül helyezéséről (HL L 312., 2018.12.7., 56. o.).

európai jelentőségű kritikus szervezetek kötelezettségeire vonatkozóan. A tanácsadó missziókat – nem érintve azt, hogy a misszió lebonyolításának helye szerinti tagállamnak és a kritikus szervezetnek meg kell felelnie az ezen irányelvben megállapított szabályoknak – az említett tagállam jogának részletes szabályai – például a releváns helyiségekhez vagy dokumentumokhoz való hozzáférés megszerzéséhez teljesítendő pontos feltételekre és a bírósági jogorvoslatra vonatkozó szabályok – szerint kell lebonyolítani. Az ilyen tanácsadó missziókhoz szükséges különleges szakértelmet adott esetben az 1313/2013/EU európai parlamenti és tanácsi határozattal ([22]) létrehozott Veszélyhelyzet-reagálási Koordinációs Központon keresztül lehet igényelni.

(37) A Bizottság támogatása, valamint az ezen irányelvvel kapcsolatos kérdésekre vonatkozóan a tagállamok közötti együttműködés és többek között a legjobb gyakorlatokra vonatkozó információcsere elősegítése érdekében létre kell hozni a kritikus szervezetek rezilienciájával foglalkozó csoportot. A tagállamoknak törekedniük kell annak biztosítására, hogy az illetékes hatóságaik kijelölt képviselői hatékonyan és eredményesen működjenek együtt a kritikus szervezetek rezilienciájával foglalkozó csoportban, többek között azáltal, hogy adott esetben biztonsági tanúsítvánnyal rendelkező képviselőket jelölnek ki. A kritikus szervezetek rezilienciájával foglalkozó csoportnak a lehető leghamarabb meg kell kezdenie feladatainak ellátását annak érdekében, hogy további eszközöket biztosítson az ezen irányelv átültetési időszaka alatti megfelelő együttműködéshez. A kritikus szervezetek rezilienciájával foglalkozó csoportnak kapcsolatot kell fenntartania egyéb releváns ágazatspecifikus szakértői munkacsoportokkal.

(38) A kritikus szervezetek rezilienciájával foglalkozó csoportnak együtt kell működnie az (EU) 2022/2555 irányelv alapján létrehozott együttműködési csoporttal a kritikus szervezetek kiber- és nemkiber-rezilienciájára vonatkozó átfogó keret támogatása céljából. A kritikus szervezetek rezilienciájával foglalkozó csoportnak és az (EU) 2022/2555 irányelv alapján létrehozott együttműködési csoportnak rendszeres párbeszédet kell folytatnia az ezen irányelv szerinti és az (EU) 2022/2555 irányelv szerinti illetékes hatóságok közötti együttműködés előmozdítása és az információcsere elősegítése érdekében, különösen a mindkét csoport számára relevanciával bíró témákról.

(39) Ezen irányelv célkitűzéseinek elérése érdekében, valamint a tagállamok és a kritikus szervezetek azon jogi felelősségének sérelme nélkül, hogy biztosítsák az ezen irányelvben megállapított kötelezettségeiknek való megfelelést, a Bizottságnak az általa szükségesnek tartott esetekben támogatnia kell az illetékes hatóságokat és a kritikus szervezeteket a vonatkozó kötelezettségeiknek való megfelelés elősegítése céljából. A tagállamoknak és a kritikus szervezeteknek az ezen irányelv szerinti kötelezettségek végrehajtásához való támogatásnyújtás során a Bizottságnak a meglévő struktúrákra és eszközökre – így például az 1313/2013/EU határozattal létrehozott uniós polgári védelmi mechanizmus és a kritikus infrastruktúrák védelmével foglalkozó európai referenciahálózat keretében rendelkezésre állókra – kell támaszkodnia. A Bizottságnak emellett tájékoztatnia kell a tagállamokat az uniós szinten – így például az (EU) 2021/1149 európai parlamenti és tanácsi rendelettel ([23]) létrehozott Belső Biztonsági Alap, az (EU) 2021/695 európai parlamenti és tanácsi rendelettel ([24]) létrehozott Horizont Európa vagy a kritikus szervezetek rezilienciája tekintetében releváns egyéb eszközök keretében – rendelkezésre álló erőforrásokról.

(40) A tagállamoknak biztosítaniuk kell, hogy illetékes hatóságaik bizonyos konkrét hatáskörökkel rendelkezzenek ezen irányelvnek a kritikus szervezetek tekintetében történő megfelelő alkalmazására és érvényesítésére, amennyiben az említett szervezetek az ezen irányelvben meghatározottak szerint a joghatóságuk alá tartoznak. Az említett hatáskörök magukban foglalják különösen a következőket: ellenőrzések és auditok lefolytatására vonatkozó hatáskör, felügyeleti hatáskör, hatáskör annak előírására, hogy a kritikus szervezetek biztosítsanak tájékoztatást és bizonyítékot a kötelezettségeik teljesítése érdekében hozott intézkedések kapcsán, valamint szükség esetén hatáskör a beazonosított jogsértések orvoslását célzó határozatok kibocsátására. Az ilyen határozatok kibocsátásakor a tagállamok által előírt intézkedések nem léphetik túl az érintett kritikus szervezet megfelelésének biztosításához szükséges és arányos mértéket, figyelembe véve különösen a jogsértés súlyosságát és az érintett kritikus szervezet gazdasági képességét. Általánosabban véve, az Európai Unió Alapjogi Chartájával összhangban az említett

([22]) Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról (HL L 347., 2013.12.20., 924. o.).

([23]) Az Európai Parlament és a Tanács (EU) 2021/1149 rendelete (2021. július 7.) a Belső Biztonsági Alap létrehozásáról (HL L 251., 2021.7.15., 94. o.).

([24]) Az Európai Parlament és a Tanács (EU) 2021/695 rendelete (2021. április 28.) a Horizont Európa kutatási és innovációs keretprogram létrehozásáról, valamint részvételi és terjesztési szabályainak megállapításáról, továbbá az 1290/2013/EU és az 1291/2013/EU rendelet hatályon kívül helyezéséről (HL L 170., 2021.5.12., 1. o.).

hatásköröket a nemzeti jogban pontosan meghatározandó megfelelő és hatékony biztosítékoknak kell kísérniük. Az ezen irányelv szerinti illetékes hatóságok számára lehetővé kell tenni, hogy – annak értékelése során, hogy valamely kritikus szervezet megfelel-e az ezen irányelvben megállapított kötelezettségeinek – felkérhessék az (EU) 2022/2555 irányelv szerinti illetékes hatóságokat arra, hogy gyakorolják felügyeleti és jogérvényesítési hatáskörüket valamely olyan, az említett irányelv szerinti szervezet tekintetében, amelyet ezen irányelv alapján kritikus szervezetként azonosítottak. Az ezen irányelv szerinti illetékes hatóságoknak és az (EU) 2022/2555 irányelv szerinti illetékes hatóságoknak e célból együtt kell működniük, és információt kell cserélniük.

(41) Ezen irányelv hatékony és következetes alkalmazása érdekében a Bizottságot fel kell hatalmazni arra, hogy az EUMSZ 290. cikkének megfelelően jogi aktusokat fogadjon el abból a célból, hogy az alapvető szolgáltatások jegyzékének összeállításával kiegészítse ezen irányelvet. Az említett jegyzéket az illetékes hatóságoknak a tagállami kockázatértékelések elvégzése és a kritikus szervezetek ezen irányelv szerinti azonosítása céljából kell használniuk. Ezen irányelv minimumharmonizációs megközelítésének fényében az említett jegyzék nem kimerítő jellegű, és a tagállamok nemzeti szinten további alapvető szolgáltatásokkal egészíthetik ki azt annak érdekében, hogy figyelembe lehessen venni az alapvető szolgáltatások nyújtása terén fennálló nemzeti sajátosságokat. Különösen fontos, hogy a Bizottság az előkészítő munkája során megfelelő konzultációkat folytasson, többek között szakértői szinten is, és hogy e konzultációkra a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban ([25]) megállapított elvekkel összhangban kerüljön sor. Így különösen a felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlament és a Tanács a tagállamok szakértőivel egyidejűleg kap kézhez minden dokumentumot, és szakértőik rendszeresen részt vehetnek a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein.

(42) Ezen irányelv végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek ([26]) megfelelően kell gyakorolni.

(43) Mivel ezen irányelv céljait, nevezetesen annak biztosítását, hogy az alapvetően fontos társadalmi funkciók vagy gazdasági tevékenységek fenntartásához nélkülözhetetlen szolgáltatásokat a belső piacon akadálytalan módon nyújtsák, és az ilyen szolgáltatásokat nyújtó kritikus szervezetek rezilienciájának fokozását a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban az intézkedés hatása miatt e célok jobban megvalósíthatók, az Unió intézkedéseket hozhat a szubszidiaritásnak az Európai Unióról szóló szerződés 5. cikkében foglalt elvével összhangban. Az arányosságnak az 5. cikkben foglalt elvével összhangban ez az irányelv nem lépi túl az e célok eléréséhez szükséges mértéket.

(44) Az európai adatvédelmi biztossal az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([27]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos 2021. augusztus 11-én véleményt nyilvánított.

(45) A 2008/114/EK irányelvet ezért hatályon kívül kell helyezni,

([25]) HL L 123., 2016.5.12., 1. o.

([26]) Az Európai Parlament és a Tanács 182/2011/EU rendelete (2011. február 16.) a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról (HL L 55., 2011.2.28., 13. o.).

([27]) 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.).

ELFOGADTA EZT AZ IRÁNYELVET:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy és hatály

(1) Ez az irányelv:

a) kötelezettségeket – különösen a kritikus szervezetek azonosítására és a kritikus szervezetek részére a rájuk rótt kötelezettségek teljesítéséhez nyújtott támogatásra vonatkozó kötelezettségeket – állapít meg a tagállamok számára, hogy hozzanak konkrét intézkedéseket, amelyek célja biztosítani, hogy az EUMSZ 114. cikkének hatálya alá tartozó alapvetően fontos társadalmi funkciók vagy gazdasági tevékenységek fenntartásához nélkülözhetetlen szolgáltatások nyújtására akadálytalan módon kerüljön sor a belső piacon;

b) kötelezettségeket állapít meg a kritikus szervezetek számára, amelyek célja rezilienciájuk és az a) pontban említett szolgáltatások belső piacon történő nyújtására való képességük fokozása;

c) szabályokat állapít meg a következőkre vonatkozóan:

i. a kritikus szervezetek felügyelete;

ii. jogérvényesítés;

iii. a különös európai jelentőségű kritikus szervezetek azonosítása, valamint tanácsadó missziók azon intézkedések értékelésére, amelyeket az ilyen szervezetek a III. fejezet szerinti kötelezettségeik teljesítése érdekében vezettek be;

d) közös eljárásokat határoz meg az ezen irányelv alkalmazásával kapcsolatos együttműködésre és jelentéstételre vonatkozóan;

e) intézkedéseket állapít meg a kritikus szervezetek magas szintű rezilienciájának elérése céljából az alapvető szolgáltatások Unión belüli nyújtásának biztosítása és a belső piac működésének javítása érdekében.

(2) Ezen irányelv 8. cikkének sérelme nélkül, ezen irányelv nem alkalmazandó az (EU) 2022/2555 irányelv hatálya alá tartozó kérdésekre. A kritikus szervezetek fizikai biztonsága és kiberbiztonsága közötti kapcsolat fényében a tagállamok biztosítják, hogy ezen irányelv és az (EU) 2022/2555 irányelv végrehajtására koordinált módon kerüljön sor.

(3) Amennyiben ágazatspecifikus uniós jogi aktusok rendelkezései előírják a kritikus szervezetek számára, hogy hozzanak intézkedéseket rezilienciájuk fokozása érdekében, és amennyiben a tagállamok az említett követelményeket az ezen irányelvben megállapított kötelezettségekkel legalább egyenértékűnek ismerik el, ezen irányelv releváns rendelkezései – többek között a VI. fejezetben megállapított, a felügyeletre és a jogérvényesítésre vonatkozó rendelkezések – nem alkalmazandók.

(4) Az EUMSZ 346. cikkének sérelme nélkül, az uniós vagy a nemzeti szabályok – így például az üzleti titoktartásra vonatkozó szabályok – értelmében bizalmasnak minősülő információkat csak abban az esetben kell megosztani a Bizottsággal és más érintett hatóságokkal ezen irányelvnek megfelelően, ha az említett információmegosztás ezen irányelv alkalmazásához szükséges. A megosztott információknak az említett megosztás célja szempontjából releváns és arányos mértékre kell korlátozódnia. Az információmegosztás során meg kell őrizni az említett információk bizalmas jellegét, valamint a kritikus szervezetek biztonsági és kereskedelmi érdekeit, tiszteletben tartva ugyanakkor a tagállamok biztonságát.

(5) Ez az irányelv nem érinti a tagállamoknak a nemzetbiztonság és védelem megőrzésére irányuló felelősségét, valamint az egyéb alapvető állami funkciók védelmére vonatkozó hatáskörüket, beleértve az állam területi integritásának biztosítását és a közrend fenntartását.

(6) Ez az irányelv nem alkalmazandó azon közigazgatási szervezetekre, amelyek a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés területén végzik tevékenységüket, beleértve a bűncselekményekre irányuló nyomozást, felderítést és vádeljárás lefolytatását is.

(7) A tagállamok dönthetnek úgy, hogy a 11. cikkben, valamint a III., IV. és VI. fejezetben foglalt rendelkezések részben vagy egészben nem alkalmazandók olyan konkrét kritikus szervezetekre, amelyek a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés területén folytatnak tevékenységeket, beleértve a bűncselekményekre irányuló nyomozást, felderítést és vádeljárás lefolytatását is, vagy amelyek kizárólag az e cikk (6) bekezdésében említett közigazgatási szervezeteknek nyújtanak szolgáltatásokat.

(8) Az ezen irányelvben megállapított kötelezettségek nem járhatnak olyan információk biztosításával, amelyek nyilvánosságra hozatala ellentétes volna a tagállamok nemzetbiztonságának, közbiztonságának vagy védelmének alapvető érdekeivel.

(9) Ezen irányelv nem érinti a személyes adatok védelmére vonatkozó uniós jogot, különösen az (EU) 2016/679 európai parlamenti és tanácsi rendeletet ([28]) és a 2002/58/EK európai parlamenti és tanácsi irányelvet ([29]).

2. cikk

Fogalommeghatározások

Ezen irányelv alkalmazásában:

1. „kritikus szervezet”: olyan köz- vagy magánjogi szervezet, amelyet valamely tagállam a 6. cikknek megfelelően a mellékletben foglalt táblázat harmadik oszlopában meghatározott kategóriák egyikébe tartozóként azonosított;

2. „reziliencia”: valamely kritikus szervezet azon képessége, hogy megelőzzön egy eseményt, azzal szemben védekezzen, arra reagáljon, annak ellenálljon, azt enyhítse, tompítsa, ahhoz alkalmazkodjon, és abból helyreálljon;

3. „esemény”: olyan esemény, amely alkalmas arra, hogy jelentős zavart okozzon, vagy amely zavart okoz valamely alapvető szolgáltatás nyújtásában, beleértve, amikor érinti a jogállamiság védelmét biztosító nemzeti rendszereket;

4. „kritikus infrastruktúra”: olyan eszköz, létesítmény, berendezés, hálózat vagy rendszer, vagy valamely eszköz, létesítmény, berendezés, hálózat vagy rendszer része, amely szükséges az alapvető szolgáltatás nyújtásához;

5. „alapvető szolgáltatás”: az alapvetően fontos társadalmi funkciók, a gazdasági tevékenységek, a népegészségügy és a biztonság vagy a környezet fenntartásához elengedhetetlen szolgáltatás;

6. „kockázat”: valamely esemény által okozott potenciális veszteség vagy zavar, és azt az ilyen veszteség vagy zavar nagyságrendjének és az esemény bekövetkezési valószínűségének kombinációjaként kell kifejezni;

7. „kockázatértékelés ”: átfogó eljárás, amely valamely kockázat jellegének és mértékének meghatározására irányul, olyan potenciális releváns fenyegetések, sebezhetőségek és veszélyek azonosításával és elemzésével, amelyek eseményt idézhetnek elő, valamint az alapvető szolgáltatás nyújtása tekintetében felmerülő, az említett esemény által okozott potenciális veszteség vagy zavar értékelésével;

8. „szabvány”: az 1025/2012/EU európai parlamenti és tanácsi rendelet ([30]) 2. cikkének 1. pontjában meghatározott szabvány;

([28]) 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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

([29]) Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) (HL L 201., 2002.7.31., 37. o.).

([30]) Az Európai Parlament és a Tanács 1025/2012/EU rendelete (2012. október 25.) az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről (HL L 316., 2012.11.14., 12. o.).

9. „műszaki előírás”: az 1025/2012/EU rendelet 2. cikkének 4. pontjában meghatározott műszaki előírás;

10. „közigazgatási szervezet”: olyan szervezet, amelyet az adott tagállam a nemzeti joggal összhangban ilyenként ismer el, nem beleértve a bíróságokat, a parlamenteket vagy a központi bankokat, és amely megfelel a következő kritériumoknak:

    a) az általános érdekű szükségletek kielégítése céljából jött létre, és nincs ipari vagy kereskedelmi jellege;

    b) jogi személyiséggel rendelkezik, vagy törvény alapján jogosult egy másik, jogi személyiséggel rendelkező szervezet nevében eljárni;

    c) legnagyobb részben az állami hatóságok vagy egyéb, központi szintű közjogi szervek finanszírozzák, irányítása az említett hatóságok, illetve szervek felügyelete alatt áll, vagy van olyan igazgatási, irányító vagy felügyeleti testülete, amely tagjainak több mint felét az állami hatóságok vagy egyéb, központi szintű közjogi szervek nevezi ki;

    d) hatáskörrel rendelkezik arra, hogy természetes vagy jogi személyekhez a személyek, az áruk, a szolgáltatások vagy a tőke határokon átnyúló mozgásával kapcsolatos jogaikat érintő közigazgatási vagy szabályozási határozatokat intézzen.

3. cikk

Minimumharmonizáció

Ezen irányelv nem zárja ki, hogy a tagállamok a kritikus szervezetek magasabb szintű rezilienciájának elérése érdekében nemzeti jogi rendelkezéseket fogadjanak el vagy tartsanak fenn, feltéve hogy az ilyen rendelkezések összhangban vannak a tagállamoknak az uniós jogban megállapított kötelezettségeivel.

II. FEJEZET

A KRITIKUS SZERVEZETEK REZILIENCIÁJÁRA VONATKOZÓ NEMZETI KERETEK

4. cikk

A kritikus szervezetek rezilienciájára vonatkozó stratégia

(1) Az érintett érdekelt felek számára – a gyakorlatban lehetséges mértékben – nyitott konzultációt követően minden tagállam 2026. január 17-ig stratégiát fogad el a kritikus szervezetek rezilienciájának fokozására (a továbbiakban: a stratégia). A stratégia a meglévő releváns nemzeti és ágazati stratégiákra, tervekre vagy hasonló dokumentumokra építve meghatározza a stratégiai célokat és szakpolitikai intézkedéseket, a kritikus szervezetek részéről a magas szintű reziliencia elérése és fenntartása céljából, és lefedve legalább a mellékletben meghatározott ágazatokat.

(2) Minden egyes stratégiának legalább a következő elemeket kell tartalmaznia:

a) a kritikus szervezetek általános reziliencájának fokozására vonatkozó stratégiai célkitűzések és prioritások, figyelembe véve a határokon átnyúló és ágazatközi függőségeket és kölcsönös függőségeket;

b) a stratégiai célkitűzések és prioritások elérését szolgáló irányítási keretrendszer, ideértve a különböző hatóságok, a kritikus szervezetek és a stratégia végrehajtásában részt vevő egyéb felek szerepkörének és felelősségének a leírását is;

c) a kritikus szervezetek általános rezilienciájának fokozásához szükséges intézkedések leírása, beleértve az 5. cikkben említett kockázatértékelés leírását is;

d) a kritikus szervezetek azonosítására szolgáló eljárás leírása;

e) a kritikus szervezetek e fejezettel összhangban történő támogatását célzó eljárás leírása, beleértve az egyrészről a közszektor, és másrészről a magánszektor, valamint a közjogi és magánjogi szervezetek közötti együttműködés erősítését célzó intézkedéseket;

f) a stratégia végrehajtásában részt vevő főbb hatóságok és a kritikus szervezetektől eltérő érintett érdekelt felek jegyzéke;

g) az ezen irányelv szerinti illetékes hatóságok (a továbbiakban: illetékes hatóságok) és az (EU) 2022/2555 irányelv szerinti illetékes hatóságok közötti koordinációt szolgáló szakpolitikai keret a kiberbiztonsági kockázatokra, a kiberfenyegetésekre és kiberjellegű eseményekre, valamint a nem kiberjellegű kockázatokra, fenyegetésekre és eseményekre vonatkozó információmegosztás és a felügyeleti feladatok ellátása céljából;

h) a már bevezetett olyan intézkedések leírása, amelyek célja elősegíteni az ezen irányelv III. fejezete szerinti kötelezettségeknek a 2003/361/EK bizottsági ajánlás ([31]) mellékletének értelmében vett, a szóban forgó tagállam által kritikus szervezetként azonosított kis- és középvállalkozások általi végrehajtását.

A releváns érdekelt felek számára – a gyakorlatban lehetséges mértékig – nyitott konzultációt követően a tagállamok legalább négyévente aktualizálják stratégiájukat.

(3) A tagállamok továbbítják a Bizottságnak a stratégiájukat és annak jelentősen aktualizált változatait az elfogadásukat követő három hónapon belül.

5. cikk

A tagállamok általi kockázatértékelés

(1) A Bizottság felhatalmazást kap arra, hogy a 23. cikknek megfelelően 2023. november 17-ig felhatalmazáson alapuló jogi aktust fogadjon el annak érdekében, hogy kiegészítse ezt az irányelvet a mellékletben meghatározott ágazatokban és alágazatokban nyújtott alapvető szolgáltatások nem kimerítő jegyzékének megállapítása révén. Az illetékes hatóságok 2026. január 17-ig, és azt követően szükség esetén, de legalább négyévente felhasználják az alapvető szolgáltatások említett jegyzékét kockázatértékelés elvégzése céljából (a továbbiakban: tagállami kockázatértékelés). Az illetékes hatóságok a tagállami kockázatértékelést felhasználják abból a célból, hogy a 6. cikkel összhangban azonosítsák a kritikus szervezeteket, és segítséget nyújtsanak az említett kritikus szervezeteknek a 13. cikk szerinti intézkedések meghozatalához.

A tagállami kockázatértékeléseknek ki kell terjednie a releváns természeti és ember okozta kockázatokra, beleértve a több ágazatot érintő vagy a határokon átnyúló jellegű kockázatokat, a baleseteket, a természeti katasztrófákat, a népegészségügyi szükséghelyzeteket és a hibrid fenyegetéseket vagy egyéb ellenséges fenyegetéseket, ideértve az (EU) 2017/541 európai parlamenti és tanácsi irányelvben ([32]) foglaltak szerinti terrorista bűncselekményeket.

(2) A tagállami kockázatértékelések elvégzése során a tagállamok figyelembe veszik legalább a következőket:

a) az 1313/2013/EU határozat 6. cikkének (1) bekezdése alapján elvégzett általános kockázatértékelés;

b) a releváns ágazatspecifikus uniós jogi aktusok – többek között az (EU) 2017/1938 ([33]) és az (EU) 2019/941 ([34]) európai parlamenti és tanácsi rendelet, valamint a 2007/60/EK ([35]) és a 2012/18/EU ([36]) európai parlamenti és tanácsi irányelv – követelményeinek megfelelően elvégzett egyéb releváns kockázatértékelések;

([31]) A Bizottság 2003/361/EK ajánlása (2003. május 6.) a mikro-, kis- és középvállalkozások fogalmának meghatározásáról (HL L 124., 2003.5.20., 36. o.).

([32]) Az Európai Parlament és a Tanács (EU) 2017/541 irányelve (2017. március 15.) a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról (HL L 88., 2017.3.31., 6. o.).

([33]) Az Európai Parlament és a Tanács (EU) 2017/1938 rendelete (2017. október 25.) a földgázellátás biztonságának megőrzését szolgáló intézkedésekről és a 994/2010/EU rendelet hatályon kívül helyezéséről (HL L 280., 2017.10.28., 1. o.).

([34]) Az Európai Parlament és a Tanács (EU) 2019/941 rendelete (2019. június 5.) a villamosenergia-ágazati kockázatokra való felkészülésről és a 2005/89/EK irányelv hatályon kívül helyezéséről (HL L 158., 2019.6.14., 1. o.).

([35]) Az Európai Parlament és a Tanács 2007/60/EK irányelve (2007. október 23.) az árvízkockázatok értékeléséről és kezeléséről (HL L 288., 2007.11.6., 27. o.).

([36]) Az Európai Parlament és a Tanács 2012/18/EU irányelve (2012. július 4.) a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről, valamint a 96/82/EK tanácsi irányelv módosításáról és későbbi hatályon kívül helyezéséről (HL L 197., 2012.7.24., 1. o.).

c) a mellékletben meghatározott ágazatok egymás közötti függőségének mértékéből eredő releváns kockázatok, ideértve a más tagállamokban és harmadik országokban található szervezetektől való függőségük mértékét is, valamint az egyik ágazatban bekövetkező jelentős zavarok más ágazatokra gyakorolt esetleges hatása, ideértve a polgárokat és a belső piacot érintő jelentős kockázatokat is;

d) a 15. cikknek megfelelően bejelentett eseményekre vonatkozó információk.

Az első albekezdés c) pontjának alkalmazásában a tagállamok adott esetben együttműködnek más tagállamok illetékes hatóságaival és harmadik országok illetékes hatóságaival.

(3) A tagállamok a 6. cikkel összhangban általuk azonosított kritikus szervezetek rendelkezésére bocsátják a tagállami kockázatértékelés releváns elemeit, adott esetben az egyedüli nemzeti kapcsolattartó pontjukon keresztül. A tagállamok biztosítják, hogy a kritikus szervezeteknek nyújtott információk segítsenek nekik a 12. cikk szerinti kockázatértékelésük elvégzésében, valamint a rezilienciájukat biztosító intézkedéseknek a 13. cikk szerinti meghozatalában.

(4) A tagállami kockázatértékelés elvégzésétől számított három hónapon belül, a tagállam a mellékletben meghatározott ágazatonkénti és alágazatonkénti bontásban a Bizottság rendelkezésére bocsátja az említett tagállami kockázatértékelést követően azonosított kockázati típusokra és az említett tagállami kockázatértékelés eredményeire vonatkozó releváns információkat.

(5) A Bizottság – a tagállamokkal együttműködve – önkéntes közös jelentéstételi mintadokumentumot dolgoz ki a (4) bekezdésnek való megfelelés céljából.

6. cikk

A kritikus szervezetek azonosítása

(1) Minden egyes tagállam 2026. július 17-ig a mellékletben meghatározott ágazatok és alágazatok tekintetében azonosítja a kritikus szervezeteket.

(2) Amikor egy tagállam az (1) bekezdés értelmében kritikus szervezeteket azonosít, figyelembe veszi a tagállami kockázatértékelésének eredményeit és a stratégiáját, továbbá alkalmazza a következő kritériumok mindegyikét:

a) a szervezet egy vagy több alapvető szolgáltatást nyújt;

b) az említett tagállam területén működik a szervezet, és ott található a kritikus infrastruktúrája; és

c) egy esemény a 7. cikk (1) bekezdésével összhangban meghatározottak szerint jelentős zavart keltő hatásokkal járna egy vagy több alapvető szolgáltatásnak a szervezet által történő biztosítására nézve, vagy egyéb olyan alapvető szolgáltatások biztosítására nézve a mellékletben meghatározott ágazatokban, amelyek az említett egy vagy több alapvető szolgáltatástól függenek.

(3) Minden tagállam összeállítja a (2) bekezdés alapján azonosított kritikus szervezetek jegyzékét, és biztosítja, hogy az említett kritikus szervezeteket az azonosításukat követő egy hónapon belül értesítsék a kritikus szervezetként való azonosításukról. A tagállamok tájékoztatják az említett kritikus szervezeteket a III. és a IV. fejezet szerinti kötelezettségeikről és azon időpontról, amelytől kezdve az említett kötelezettségek – a 8. cikk sérelme nélkül – alkalmazandók rájuk. Amennyiben a nemzeti intézkedések másként nem rendelkeznek, a tagállamok tájékoztatják a mellékletben foglalt táblázat 3., 4. és 8. pontjában meghatározott ágazatokban működő kritikus szervezeteket arról, hogy nincsenek a III. és a IV. fejezet szerinti kötelezettségeik.

Az érintett kritikus szervezetek tekintetében a III. fejezet az e bekezdés első albekezdésében említett értesítés időpontjától számított 10 hónap elteltével alkalmazandó.

(4) A tagállamok biztosítják, hogy az ezen irányelv szerinti illetékes hatóságaik az azonosítást követő egy hónapon belül értesítsék az (EU) 2022/2555 irányelv szerinti illetékes hatóságokat azon kritikus szervezetek identitásáról, amelyeket e cikk alapján azonosítottak. Az említett értesítésben adott esetben pontosítani kell, hogy az érintett kritikus szervezetek az ezen irányelv mellékletében foglalt táblázat 3., 4. és 8. pontjában meghatározott ágazatokban működő szervezetek, és nincsenek az ezen irányelv III. és IV. fejezete szerinti kötelezettségeik.

(5) A tagállamok szükség esetén, de legalább négyévente felülvizsgálják, és adott esetben aktualizálják a (3) bekezdésben említett azonosított kritikus szervezetek jegyzékét. Amennyiben az említett aktualizálások további kritikus szervezetek azonosításához vezetnek, a (3) és a (4) bekezdést kell alkalmazni az említett további kritikus szervezetekre. Ezen túlmenően a tagállamok biztosítják, hogy azon szervezeteket, amelyeket egy ilyen aktualizálást követően már nem azonosítanak kritikus szervezetként, kellő időben értesítsék erről a tényről, továbbá arról a tényről, hogy az említett értesítés kézhezvételének napjától már nem vonatkoznak rájuk a III. fejezet szerinti kötelezettségek.

(6) A Bizottság – a tagállamokkal együttműködve – ajánlásokat és nem kötelező erejű iránymutatásokat dolgoz ki, hogy támogatást nyújtson a tagállamoknak a kritikus szervezetek azonosításához.

7. cikk

Jelentős zavart keltő hatás

(1) A 6. cikk (2) bekezdésének c) pontjában említett zavart keltő hatások jelentőségének meghatározásakor a tagállamok a következő kritériumokat veszik figyelembe:

a) az érintett szervezet által nyújtott alapvető szolgáltatásra támaszkodó felhasználók száma;

b) a mellékletben meghatározott egyéb ágazatok és alágazatok függésének mértéke a szóban forgó alapvető szolgáltatástól;

c) azon hatás, amelyet az események – mértéküket és időtartamukat tekintve – gyakorolhatnak a gazdasági és társadalmi tevékenységekre, a környezetre, a közvédelemre és -biztonságra, vagy a lakosság egészségére;

d) a szervezet piaci részesedése az érintett alapvető szolgáltatás vagy alapvető szolgáltatások piacán;

e) azon földrajzi terület, amelyet egy esemény érinthet, ideértve a határokon átnyúló hatásokat is, figyelembe véve bizonyos típusú, olyan földrajzi területeknek az elszigeteltség mértékével összefüggő sebezhetőségét, mint például a szigeti régiók, a távoli régiók és a hegyvidéki területek;

f) a szervezet jelentősége az alapvető szolgáltatás elégséges szintjének fenntartásában, figyelembe véve az adott alapvető szolgáltatás nyújtásához rendelkezésre álló egyéb lehetőségeket is.

(2) Minden egyes tagállam – a kritikus szervezetek 6. cikk (1) bekezdés szerinti azonosítását követően – indokolatlan késedelem nélkül benyújtja a Bizottságnak a következő információkat:

a) az említett tagállamban nyújtott alapvető szolgáltatások jegyzéke, amennyiben van bármely további alapvető szolgáltatás az 5. cikk (1) bekezdésében említett alapvető szolgáltatások jegyzékéhez képest;

b) a mellékletben meghatározott egyes ágazatok és alágazatok, valamint az egyes alapvető szolgáltatások tekintetében azonosított kritikus szervezetek száma;

c) az (1) bekezdésben foglalt egy vagy több kritérium meghatározásához alkalmazott küszöbértékek.

Az első albekezdés c) pontjában említett küszöbértékeket önmagukban vagy aggregált formában lehet közölni.

A tagállamok ezt követően szükség esetén, de legalább négyévente nyújtják be az első albekezdésben említett információkat.

(3) A Bizottság – a 19.cikkben említett, a kritikus szervezetek rezilienciájával foglalkozó csoporttal folytatott konzultációt követően – az e cikk (2) bekezdésében említett információk figyelembevételével nem kötelező erejű iránymutatásokat fogad el az e cikk (1) bekezdésben említett kritériumok alkalmazásának elősegítése érdekében.

8. cikk

Kritikus szervezetek a banki szolgáltatások, a pénzügyi piaci infrastruktúra és a digitális infrastruktúra ágazatában

A tagállamok biztosítják, hogy a 11. cikk, valamint a III., a IV. és a VI. fejezet ne legyen alkalmazandó olyan kritikus szervezetekre, amelyeket a mellékletben foglalt táblázat 3., 4. és 8. pontjában meghatározott ágazatokban azonosítottak. A tagállamok az említett kritikus szervezetek magasabb szintű rezilienciájának elérése érdekében nemzeti jogi rendelkezéseket fogadhatnak el vagy tarthatnak fenn, feltéve, hogy az említett rendelkezések összhangban vannak az alkalmazandó uniós joggal.

9. cikk

Illetékes hatóságok és egyedüli kapcsolattartó pont

(1) Minden egyes tagállam kijelöl vagy létrehoz egy vagy több, az ezen irányelvben meghatározott szabályok helyes nemzeti szintű alkalmazásáért és szükség esetén érvényesítéséért felelős nemzeti illetékes hatóságot.

Az ezen irányelv mellékletében foglalt táblázat 3. és 4. pontjában meghatározott ágazatokban működő kritikus szervezetek tekintetében az illetékes hatóságoknak főszabályként meg kell egyezniük az (EU) 2022/2554 rendelet 46. cikkében említett illetékes hatóságokkal. Az ezen irányelv mellékletében foglalt táblázat 8. pontjában meghatározott ágazatban működő kritikus szervezetek tekintetében az illetékes hatóságoknak főszabályként meg kell egyezniük az (EU) 2022/2555 irányelv szerinti illetékes hatóságokkal. A tagállamok az ezen irányelv mellékletében foglalt táblázat 3., 4. és 8. pontjában meghatározott ágazatok tekintetében kijelölhetnek egy különböző illetékes hatóságot a meglévő nemzeti keretekkel összhangban.

Amennyiben a tagállamok egynél több hatóságot jelölnek ki vagy hoznak létre, egyértelműen meghatározzák minden egyes érintett hatóság feladatait, és biztosítják, hogy azok hatékonyan együttműködjenek az ezen irányelv szerinti feladataik teljesítése érdekében, többek között a (2) bekezdésben említett egyedüli kapcsolattartó pont kijelölése és tevékenységei tekintetében.

(2) Minden egyes tagállam kijelöl vagy létrehoz egy egyedüli kapcsolattartó pontot, hogy összekötő funkciót lásson el a többi tagállam egyedüli kapcsolattartó pontjaival és a 19. cikkben említett, a kritikus szervezetek rezilienciájával foglalkozó csoporttal való, határokon átnyúló együttműködés biztosítása céljából. A tagállam az egyedüli kapcsolattartó pontját adott esetben egy illetékes hatóságon belül jelöli ki. A tagállam adott esetben úgy rendelkezhet, hogy egyedüli kapcsolattartó pontja összekötő funkciót is ellát a Bizottság felé, és együttműködést biztosít harmadik országokkal.

(3) Az egyedüli kapcsolattartó pont 2028. július 17-ig, és azt követően kétévente összefoglaló jelentést nyújt be a Bizottságnak és a 19. cikkben említett, a kritikus szervezetek rezilienciájával foglalkozó csoportnak az általuk kapott értesítésekről, beleértve az értesítések számát, a bejelentett események jellegét és a 15. cikk (3) bekezdésével összhangban hozott intézkedéseket.

A Bizottság – a kritikus szervezetek rezilienciájával foglalkozó csoporttal együttműködve – közös jelentéstételi mintadokumentumot dolgoz ki. Az illetékes hatóságok önkéntes alapon használhatják a közös jelentéstételi mintadokumentumot az első albekezdésben említett összefoglaló jelentések benyújtása céljából.

(4) Minden egyes tagállam biztosítja, hogy illetékes hatósága és az egyedüli kapcsolattartó pont rendelkezzen hatáskörrel, valamint a megfelelő pénzügyi, emberi és technikai erőforrásokkal a rá bízott feladatok hatékony és eredményes módon történő ellátásához.

(5) Minden egyes tagállam biztosítja, hogy illetékes hatósága – adott esetben – az uniós és a nemzeti jogszabályokkal összhangban egyeztessen és működjön együtt más releváns nemzeti hatóságokkal, ideértve a polgári védelemért, a bűnüldözésért és a személyes adatok védelméért felelős hatóságokat, továbbá a kritikus szervezetekkel és a releváns érdekelt felekkel is.

(6) Minden egyes tagállam biztosítja, hogy az ezen irányelv szerinti illetékes hatósága együttműködjön és információt cseréljen az (EU) 2022/2555 irányelv szerinti illetékes hatóságokkal a kritikus szervezeteket érintő kiberbiztonsági kockázatokról, kiberfenyegetésekről és kiberjellegű eseményekről, valamint nem kiberjellegű kockázatokról, fenyegetésekről és eseményekről, beleértve az illetékes hatósága és az (EU) 2022/2555 irányelv szerinti illetékes hatóságok által hozott releváns intézkedések tekintetében.

(7) Az illetékes hatóság és az egyedüli kapcsolattartó pont kijelölését vagy létrehozását követő három hónapon belül minden egyes tagállam értesíti a Bizottságot azok identitásáról, valamint az ezen irányelv szerinti feladataikról és hatáskörükről, elérhetőségeikről és ezek bármely későbbi változásairól. A tagállamok tájékoztatják a Bizottságot, amennyiben úgy döntenek, hogy az (1) bekezdés második albekezdésében említett illetékes hatóságtól eltérő hatóság kijelöléséről határoznak a mellékletben foglalt táblázat 3., 4. és 8. pontjában meghatározott szektorokban működő kritikus szervezetek tekintetében illetékes hatóságként. Minden egyes tagállam közzéteszi, hogy mely illetékes hatóságot és egyedüli kapcsolattartó pontot jelölte ki.

(8) A Bizottság nyilvánosságra hozza az egyedüli kapcsolattartó pontok jegyzékét.

10. cikk

A kritikus szervezetek tagállamok általi támogatása

(1) A tagállamok támogatják a kritikus szervezeteket rezilienciájuk fokozásában. E támogatás részét képezheti iránymutatások és módszerek kidolgozása, a reziliencia tesztelésére szolgáló gyakorlatok szervezésének támogatása, valamint a kritikus szervezetek személyzete számára tanácsadás és képzés biztosítása. A tagállamok – az állami támogatásokra vonatkozóan alkalmazandó szabályok sérelme nélkül – pénzügyi forrásokat biztosíthatnak a kritikus szervezetek számára, amennyiben ez szükséges és közérdekű célokból indokolt.

(2) Minden egyes tagállam biztosítja, hogy az illetékes hatósága működjön együtt, valamint cseréljen információkat és bevált gyakorlatokat a mellékletben meghatározott ágazatok kritikus szervezeteivel.

(3) A tagállamok – az uniós és a nemzeti jogszabályokkal, különösen a minősített és az érzékeny adatokra vonatkozó szabályokkal, a versenyszabályokkal, valamint a személyes adatok védelmére vonatkozó szabályokkal összhangban – elősegítik a kritikus szervezetek közötti önkéntes információmegosztást az ezen irányelv hatálya alá tartozó kérdésekkel kapcsolatban.

11. cikk

Tagállamok közötti együttműködés

(1) Adott esetben a tagállamok konzultálnak egymással a kritikus szervezetekkel kapcsolatban ezen irányelv következetes módon történő alkalmazásának biztosítása céljából. Az ilyen konzultációkra különösen azon kritikus szervezetekkel kapcsolatban kerül sor,

a) amelyek olyan kritikus infrastruktúrát vesznek igénybe, amely két vagy több tagállam között fizikailag össze van kötve;

b) amelyek olyan vállalati struktúrák részét képezik, amelyek más tagállamokban lévő kritikus szervezetekkel összeköttetésben vagy kapcsolatban állnak;

c) amelyeket kritikus szervezetként azonosítottak egy tagállamban, és alapvető szolgáltatásokat nyújtanak más tagállamoknak vagy tagállamokban.

(2) Az (1) bekezdésben említett konzultációk célja a kritikus szervezetek rezilienciájának fokozása és – amennyiben lehetséges – a rájuk nehezedő adminisztratív terhek csökkentése.

III. FEJEZET

A KRITIKUS SZERVEZETEK REZILIENCIÁJA

12. cikk

A kritikus szervezetek általi kockázatértékelés

(1) A 6. cikk (3) bekezdése második albekezdésében meghatározott határidőtől eltérve, a tagállamok biztosítják, hogy a kritikus szervezetek – a 6. cikk (3) bekezdésében említett értesítés kézhezvételétől számított kilenc hónapon belül, és azt követően szükség esetén, de legalább négyévente – a tagállami kockázatértékelések és más releváns információforrások alapján kockázatértékelést végezzenek valamennyi olyan releváns kockázat értékelése érdekében, amely zavart okozhat az alapvető szolgáltatásaik nyújtásában (a továbbiakban: kritikus szervezet általi kockázatértékelés).

(2) A kritikus szervezet általi kockázatértékeléseknek ki kell terjedniük valamennyi olyan releváns természeti és ember okozta kockázatokra, amelyek eseményhez vezethetnek, beleértve a több ágazatot érintő vagy a határokon átnyúló jellegű kockázatokat, baleseteket, természeti katasztrófákat, népegészségügyi szükséghelyzeteket és hibrid fenyegetéseket, valamint egyéb ellenséges fenyegetéseket, köztük az (EU) 2017/541 irányelvben foglaltak szerinti terrorista bűncselekményeket. A kritikus szervezet általi kockázatértékelésben figyelembe kell venni, hogy a mellékletben meghatározott más ágazatok milyen mértékben függenek a kritikus szervezet által nyújtott alapvető szolgáltatástól, és hogy az említett kritikus szervezet milyen mértékben függ az ilyen más ágazatokban működő más szervezetek által nyújtott alapvető szolgáltatásoktól.

Amennyiben egy kritikus szervezet – a saját kritikus szervezet általi kockázatértékelése számára releváns egyéb jogi aktusokban megállapított kötelezettségek alapján – egyéb kockázatértékeléseket végzett, vagy dokumentumokat készített, az említett értékeléseket és dokumentumokat felhasználhatja az e cikkben meghatározott követelményeknek való megfeleléshez. Az illetékes hatóság – felügyeleti funkcióinak gyakorlása során – kijelentheti, hogy egy kritikus szervezet által végzett olyan kockázatértékelés, amely kitér az e bekezdés első albekezdésében említett kockázatokra és függőségi mértékre, részben vagy egészben megfelel az e cikk szerinti kötelezettségeknek.

13. cikk

A kritikus szervezetek reziliencia-intézkedései

(1) A tagállamok biztosítják, hogy a kritikus szervezetek – a tagállami kockázatértékelésről a tagállamok által szolgáltatott releváns információk és a kritikus szervezet általi kockázatértékelés eredményei alapján – megfelelő és arányos technikai, biztonsági és szervezeti intézkedéseket hozzanak rezilienciájuk biztosítása érdekében, beleértve a következőkhöz szükséges intézkedéseket:

a) az események bekövetkezésének megelőzése, kellő figyelemmel a katasztrófakockázatok csökkentését és az éghajlatváltozáshoz való alkalmazkodást célzó intézkedésekre;

b) a helyiségeik és területeik, valamint kritikus infrastruktúrájuk megfelelő fizikai védelmének biztosítása, kellő figyelemmel például a következőkre: kerítések, akadályok, periméterfigyelő eszközök és rutinok, érzékelő berendezések és belépési ellenőrzések;

c) az események következményeire való reagálás, az azoknak való ellenállás és azok enyhítése, kellő figyelemmel a kockázat- és válságkezelési eljárások és protokollok, valamint riasztási rutinok végrehajtására;

d) az eseményekből történő helyreállás, kellő figyelemmel az üzletmenet-folytonossági intézkedésekre és az alternatív ellátási láncok azonosítására az alapvető szolgáltatás nyújtásának újraindítása érdekében;

e) hatékony munkavállalói biztonságirányítás garantálása, kellő figyelemmel olyan intézkedésekre, mint a kritikus funkciókat ellátó személyzet kategóriáinak meghatározása, a helyiségekhez és területekhez, kritikus infrastruktúrához és az érzékeny információkhoz való hozzáférési jogok megállapítása, a 14. cikkel összhangban háttérellenőrzésekre vonatkozó eljárások kialakítása és azon személyek kategóriáinak megjelölése, akik kötelesek magukat ilyen háttérellenőrzéseknek alávetni, továbbá megfelelő képzési követelmények és képesítések megállapítása;

f) az érintett személyzet figyelmének felhívása az a)–e) pontban említett intézkedésekre, kellő figyelemmel a képzésekre, tájékoztató anyagokra és gyakorlatokra.

Az első albekezdés e) pontjának alkalmazásában a tagállamok biztosítják, hogy a kritikus funkciókat ellátó személyzet kategóriáinak meghatározásakor a kritikus szervezetek figyelembe vegyék a külső szolgáltatók személyzetét.

(2) A tagállamok biztosítják, hogy a kritikus szervezetek az (1) bekezdés alapján megtett intézkedéseket leíró reziliencia-tervvel vagy azzal egyenértékű dokumentummal vagy dokumentumokkal rendelkezzenek, és alkalmazzák azt vagy azokat. Amennyiben a kritikus szervezetek az (1) bekezdésben említett intézkedések szempontjából releváns egyéb jogi aktusokban megállapított kötelezettségek alapján készítettek dokumentumokat vagy hoztak intézkedéseket, az említett dokumentumokat és intézkedéseket felhasználhatják az e cikkben meghatározott követelményeknek való megfeleléshez. Az illetékes hatóság – felügyeleti funkcióinak gyakorlása során – kijelentheti, hogy egy kritikus szervezet által hozott olyan meglévő reziliencia-fokozási intézkedések, amelyek megfelelő és arányos módon kitérnek az (1) bekezdésben említett technikai, biztonsági és szervezeti intézkedésekre, részben vagy egészben megfelel az e cikk szerinti kötelezettségeknek.

(3) A tagállamok biztosítják, hogy minden egyes kritikus szervezet kijelöljön egy összekötő tisztviselőt vagy egy ezzel egyenértékű személyt kapcsolattartó pontként az illetékes hatóságok felé.

(4) A kritikus szervezetet azonosító tagállam kérésére és az érintett kritikus szervezet egyetértésével a Bizottság – a 18. cikk (6), (8) és (9) bekezdésében meghatározott szabályoknak megfelelően – tanácsadó missziókat szervez, hogy tanáccsal lássa el az érintett kritikus szervezetet a III. fejezet szerinti kötelezettségeinek teljesítéséhez. A tanácsadó misszió a megállapításairól köteles jelentést tenni a Bizottságnak, az adott tagállamnak és az érintett kritikus szervezetnek.

(5) A Bizottság – a 19. cikkben említett, a kritikus szervezetek rezilienciájával foglalkozó csoporttal folytatott konzultációt követően – nem kötelező erejű iránymutatásokat fogad el az e cikk (1) bekezdése alapján hozható technikai, biztonsági és szervezeti intézkedések további pontosítása érdekében.

(6) A Bizottság végrehajtási jogi aktusokat fogad el az e cikk (1) bekezdésében említett intézkedések alkalmazására vonatkozó, szükséges technikai és módszertani előírások meghatározása érdekében. Ezeket a végrehajtási jogi aktusokat a 24. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

14. cikk

Háttérellenőrzések

(1) A tagállamok pontosan meghatározzák azon feltételeket, amelyek mellett egy kritikus szervezet számára megengedett, hogy – kellően indokolt esetekben és a tagállami kockázatértékelés figyelembevételével – kérelmet nyújtson be azon személyek háttérellenőrzésére vonatkozóan,

a) akik érzékeny szerepet töltenek be a kritikus szervezetben vagy a számára, különösen a kritikus szervezet rezilienciájával kapcsolatban;

b) akik engedéllyel rendelkeznek arra, hogy – közvetlenül vagy távolról – hozzáférjenek a kritikus szervezet helyiségeihez és területeihez, illetve információs vagy kontrollrendszereihez, többek között a kritikus szervezet biztonságával összefüggésben;

c) akiknek a felvételét mérlegelik olyan álláshelyekre, amelyekre az a) vagy b) pontban meghatározott kritériumok vonatkoznak.

(2) Az e cikk (1) bekezdésében említett kérelmeket észszerű időn belül értékelni kell, és azokat a nemzeti joggal és eljárásokkal, valamint a releváns és alkalmazandó uniós joggal, többek között az (EU) 2016/679 rendelettel és az (EU) 2016/680 európai parlamenti és tanácsi irányelvvel ([37]) összhangban kell feldolgozni. A háttérellenőrzéseknek arányosnak kell lenniük, és szigorúan a szükséges mértékre kell korlátozódniuk. Azokat kizárólag az érintett kritikus szervezetet érintő potenciális biztonsági kockázat értékelése céljából kell elvégezni.

(3) Az (1) bekezdésben említett háttérellenőrzésnek ki kell terjednie legalább a következőkre:

a) a háttérellenőrzésnek alávetett személy személyazonosságának megerősítése;

b) az említett személy bűnügyi nyilvántartásban fellelhető adatainak ellenőrzése olyan bűncselekmények vonatkozásában, amelyek egy konkrét álláshely szempontjából relevánsak volnának.

A háttérellenőrzések végzésekor a tagállamok a 2009/315/IB kerethatározatban és – adott esetben és amennyiben alkalmazandó – az (EU) 2019/816 rendeletben meghatározott eljárásoknak megfelelően az Európai Bűnügyi Nyilvántartási Információs Rendszert veszik igénybe abból a célból, hogy más tagállamok által fenntartott bűnügyi nyilvántartásokból szerezzenek be információkat. A 2009/315/IB kerethatározat 3. cikkének (1) bekezdésében és az (EU) 2019/816 rendelet 3. cikkének 5. pontjában említett központi hatóságok a megkeresésnek a 2009/315/IB kerethatározat 8. cikkének (1) bekezdésével összhangban történő kézhezvételétől számított 10 munkanapon belül válaszolnak az ilyen információkérésekre.

([37]) Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről. (HL L 119., 2016.5.4., 89. o.).

15. cikk

Az eseményekre vonatkozó értesítés

(1) A tagállamok biztosítják, hogy a kritikus szervezetek indokolatlan késedelem nélkül értesítsék az illetékes hatóságokat azon eseményekről, amelyek jelentős zavart okoznak vagy okozhatnak az alapvető szolgáltatások nyújtásában. A tagállamok biztosítják – kivéve, ha ezt operatív okokból nem tudják megtenni –, hogy a kritikus szervezet 24 órán belül benyújtsa a kezdeti értesítést azt követően, hogy tudomást szerzett valamely eseményről, majd ezt legfeljebb egy hónappal később adott esetben részletes jelentésnek kell követnie. A zavar jelentőségének meghatározása érdekében különösen a következő paramétereket kell figyelembe venni:

a) a zavar által érintett felhasználók száma és aránya;

b) a zavar időtartama;

c) a zavar által érintett földrajzi terület, figyelembe véve azt is, hogy földrajzilag elszigetelt területről van-e szó.

Amennyiben valamely esemény hat vagy több tagállamban jelentős hatást gyakorol vagy gyakorolhat az alapvető szolgáltatások nyújtásának folytonosságára, a zavar által érintett tagállamok illetékes hatóságainak értesíteniük kell a Bizottságot az említett eseményről.

(2) Az (1) bekezdés első albekezdésében említett értesítéseknek tartalmazniuk kell minden olyan rendelkezésre álló információt, amely szükséges ahhoz, hogy az illetékes hatóság megérthesse az esemény jellegét, okát és lehetséges következményeit, beleértve minden olyan rendelkezésre álló információt, amely az esemény esetleges határokon átnyúló hatásainak meghatározásához szükséges. Az ilyen értesítések nem róhatnak többletfelelősséget a kritikus szervezetekre.

(3) A kritikus szervezet által az (1) bekezdésben említett értesítésben nyújtott információk alapján a releváns illetékes hatóság az egyedüli kapcsolattartó ponton keresztül tájékoztatja a többi érintett tagállam egyedüli kapcsolattartó pontját, amennyiben az jelentős hatást gyakorol vagy gyakorolhat a kritikus szervezetekre és az alapvető szolgáltatások egy vagy több más tagállam számára vagy tagállamban való nyújtásának folytonosságára.

Az első albekezdés alapján információkat küldő és fogadó egyedüli kapcsolattartó pontok – az uniós vagy a nemzeti joggal összhangban – olyan módon kezelik az említett információkat, amely tiszteletben tartja azok bizalmas jellegét, valamint védi az érintett kritikus szervezet biztonsági és kereskedelmi érdekeit.

(4) Az (1) bekezdésben említett értesítést követően az érintett illetékes hatóság a lehető leghamarabb biztosítja az érintett kritikus szervezet számára a releváns utánkövetési információkat, ideértve az olyan információkat, amelyek támogathatják az említett kritikus szervezetnek a szóban forgó eseményre való hatékony reagálását. A tagállamok tájékoztatják a nyilvánosságot, amennyiben úgy ítélik meg, hogy ez a közérdeket szolgálná.

16. cikk

Szabványok

Ezen irányelv konvergens végrehajtásának előmozdítása érdekében a tagállamok – amennyiben az hasznos, és anélkül, hogy előírnák vagy előnyben részesítenék egy konkrét technológia-típus alkalmazását – ösztönzik a kritikus szervezetekre alkalmazandó biztonsági és reziliencia-intézkedések szempontjából releváns, európai és nemzetközi szabványok és műszaki előírások alkalmazását.

IV. FEJEZET

KÜLÖNÖS EURÓPAI JELENTŐSÉGŰ KRITIKUS SZERVEZETEK

17. cikk

A különös európai jelentőségű kritikus szervezetek azonosítása

(1) Egy szervezet különös európai jelentőségű kritikus szervezetnek minősül, amennyiben:

a) a 6. cikk (1) bekezdése értelmében kritikus szervezetként azonosították;

b) hat vagy több tagállamban vagy tagállam számára azonos vagy hasonló alapvető szolgáltatásokat nyújt;

c) e cikk (3) bekezdésének értelmében értesítették.

(2) A tagállamok biztosítják, hogy a 6. cikk (3) bekezdésében említett értesítést követően a kritikus szervezet tájékoztassa az illetékes hatóságát, amennyiben hat vagy több tagállam számára vagy tagállamban nyújt alapvető szolgáltatásokat. Ilyen esetben a tagállamok biztosítják, hogy a kritikus szervezet tájékoztassa az illetékes hatóságát azon alapvető szolgáltatásokról, amelyeket az említett tagállamok számára vagy tagállamokban nyújt, valamint azon tagállamokról, amelyek számára vagy amelyekben nyújt ilyen alapvető szolgáltatásokat. A tagállamok indokolatlan késedelem nélkül értesítik a Bizottságot az ilyen kritikus szervezetek identitásáról és azon információkról, amelyeket e bekezdés alapján nyújtanak.

A Bizottság konzultál azon tagállam illetékes hatóságával, amely az első albekezdésben említettek szerint azonosított egy kritikus szervezetet, a többi érintett tagállam illetékes hatóságával és a szóban forgó kritikus szervezettel. Az említett konzultációk során minden egyes tagállam tájékoztatja a Bizottságot, amennyiben úgy ítéli meg, hogy a kritikus szervezet által az említett tagállam számára nyújtott szolgáltatások alapvető szolgáltatások.

(3) Amennyiben a Bizottság az e cikk (2) bekezdésében említett konzultációk alapján megállapítja, hogy az érintett kritikus szervezet hat vagy több tagállam számára vagy tagállamban nyújt alapvető szolgáltatásokat, a Bizottság értesíti a kritikus szervezetet annak illetékes hatóságán keresztül, hogy különös európai jelentőségű kritikus szervezetnek minősül, továbbá tájékoztatja az említett kritikus szervezetet az e fejezet szerinti kötelezettségeiről és arról az időpontról, amelytől kezdve az említett kötelezettségek alkalmazandók rá. Mihelyt a Bizottság tájékoztatja az illetékes hatóságot azon döntéséről, hogy egy kritikus szervezetet különös európai jelentőségű kritikus szervezetnek minősít, az illetékes hatóság indokolatlan késedelem nélkül továbbítja az említett értesítést az említett kritikus szervezetnek.

(4) E fejezetet az érintett különös európai jelentőségű kritikus szervezetre az e cikk (3) bekezdésében említett értesítés kézhezvételének napjától kell alkalmazni.

18. cikk

Tanácsadó missziók

(1) Azon tagállam kérésére, amely a 6. cikk (1) bekezdése alapján kritikus szervezetként azonosított egy különös európai jelentőségű kritikus szervezetet, a Bizottság tanácsadó missziót szervez az említett kritikus szervezet által a III. fejezet szerinti kötelezettségeinek teljesítése érdekében bevezetett intézkedések értékelése céljából.

(2) A Bizottság – saját kezdeményezésére vagy egy vagy több olyan tagállam kérésére, amely számára vagy amelyben az alapvető szolgáltatást nyújtják, és feltéve, hogy az a tagállam, amely a 6. cikk (1) bekezdése alapján kritikus szervezetként azonosított egy különös európai jelentőségű kritikus szervezetet, ezzel egyetért – az e cikk (1) bekezdésében említettek szerinti tanácsadó missziót szervez.

(3) A Bizottság vagy egy vagy több olyan tagállam indokolt kérésére, amely számára vagy amelyben az alapvető szolgáltatást nyújtják, azon tagállam, amely a 6. cikk (1) bekezdése alapján kritikus szervezetként azonosított egy különös európai jelentőségű kritikus szervezetet, a Bizottság rendelkezésére bocsátja a következőket:

a) a kritikus szervezet általi kockázatértékelés releváns részei;

b) a 13. cikknek megfelelően hozott releváns intézkedések listája;

c) azon felügyeleti vagy jogérvényesítési intézkedések – ideértve a megfelelési értékeléseket vagy kibocsátott határozatokat is –, amelyeket az említett kritikus szervezet tekintetében annak illetékes hatósága a 21. és a 22. cikk értelmében végrehajtott.

(4) A tanácsadó misszió a tanácsadó misszió lezárásától számított három hónapon belül beszámol a megállapításairól a Bizottságnak, azon tagállamnak, amely a 6. cikk (1) bekezdése alapján kritikus szervezetként azonosított egy különös európai jelentőségű kritikus szervezetet, azon tagállamoknak, amelyek számára vagy amelyekben az alapvető szolgáltatást nyújtják, és az érintett kritikus szervezetnek.

Azon tagállamok, amelyek számára vagy amelyekben az alapvető szolgáltatást nyújtják, elemzik az első albekezdésben említett jelentést, és szükség esetén tanácsot adnak a Bizottságnak arra vonatkozóan, hogy az érintett különös európai jelentőségű kritikus szervezet teljesíti-e a III. fejezet szerinti kötelezettségeit, és adott esetben azon intézkedésekre vonatkozóan, amelyeket az említett kritikus szervezet rezilienciájának javítása érdekében lehetne hozni.

A Bizottság az e bekezdés második albekezdésében említett tanács alapján közli a véleményét azon tagállammal, amely a 6. cikk (1) bekezdése alapján kritikus szervezetként azonosított egy különös európai jelentőségű kritikus szervezetet, azon tagállamokkal, amelyek számára vagy amelyekben az alapvető szolgáltatást nyújtják, valamint az említett kritikus szervezettel arra vonatkozóan, hogy az említett kritikus szervezet teljesíti-e a III. fejezet szerinti kötelezettségeit, és adott esetben azon intézkedésekre vonatkozóan, amelyeket az említett kritikus szervezet rezilienciájának javítása érdekében lehetne hozni.

A tagállam, amely a 6. cikk (1) bekezdése alapján kritikus szervezetként azonosított egy különös európai jelentőségű kritikus szervezetet, biztosítja, hogy az illetékes hatósága és az érintett kritikus szervezet figyelembe vegye az e bekezdés harmadik albekezdésében említett véleményt, és tájékoztatást ad a Bizottságnak és azon tagállamoknak, amelyek számára vagy amelyekben az alapvető szolgáltatást nyújtják, az említett vélemény alapján általa hozott intézkedésekről.

(5) Minden egyes tanácsadó missziónak a következő személyekből kell állnia: azon tagállam szakértői, amelyben a különös európai jelentőségű kritikus szervezet található, azon tagállamok szakértői, amelyek számára vagy amelyekben az alapvető szolgáltatást nyújtják, valamint a Bizottság képviselői. Az említett tagállamok jelölteket javasolhatnak a tanácsadó misszióban való részvételre. A Bizottság – az azon tagállammal folytatott konzultációt követően, amely a 6. cikk (1) bekezdése alapján kritikus szervezetként azonosított egy különös európai jelentőségű kritikus szervezetet – kiválasztja és kinevezi az egyes tanácsadó missziók tagjait a szakmai alkalmasságuknak megfelelően, és amennyiben lehetséges, biztosítva valamennyi említett tagállam földrajzi szempontból kiegyensúlyozott képviseletét. Bármely szükséges esetben a tanácsadó misszió tagjainak érvényes és megfelelő biztonsági tanúsítvánnyal kell rendelkezniük. A tanácsadó missziókban való részvétellel kapcsolatos költségeket a Bizottság viseli.

A Bizottság szervezi meg minden egyes tanácsadó misszió programját, a szóban fogó tanácsadó misszió tagjaival konzultálva, és azon tagállam egyetértésével, amely a 6. cikk (1) bekezdése alapján kritikus szervezetként azonosított egy különös európai jelentőségű kritikus szervezetet.

(6) A Bizottság végrehajtási jogi aktust fogad el, amelyben meghatározza a következőkre vonatkozó eljárási szabályokat: a tanácsadó missziók szervezésére irányuló kérések, az ilyen kérések kezelése, a tanácsadó missziók lebonyolítása és jelentései, valamint a Bizottság e cikk (4) bekezdésének harmadik albekezdésében említett véleményére és a meghozott intézkedésekre vonatkozó kommunikáció kezelése, kellő figyelemmel az érintett információk bizalmas és üzleti szempontból érzékeny jellegére. Az említett végrehajtási jogi aktust a 24. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(7) A tagállamok biztosítják, hogy a különös európai jelentőségű kritikus szervezetek hozzáférést biztosítsanak a tanácsadó missziók számára az alapvető szolgáltatásaik nyújtásával kapcsolatos olyan információkhoz, rendszerekhez és létesítményekhez, amelyek az érintett tanácsadó misszió lebonyolításához szükségesek.

(8) A tanácsadó missziókat azon tagállam alkalmazandó nemzeti jogával összhangban kell lebonyolítani, amelyben azokra sor kerül, tiszteletben tartva az említett tagállamnak a nemzetbiztonságért és a biztonsági érdekeinek védelméért való felelősségét.

(9) Tanácsadó missziók szervezésekor a Bizottság figyelembe veszi a Bizottság által az érintett kritikus szervezet tekintetében a 725/2004/EK és a 300/2008/EK rendelet alapján végzett ellenőrzésekről szóló jelentéseket, valamint a Bizottság által a 2005/65/EK irányelv alapján végzett nyomon követésről szóló jelentéseket.

(10) A Bizottság minden olyan esetben tájékoztatja a 19. cikkben említett, a kritikus szervezetek rezilienciájával foglalkozó csoportot, amikor tanácsadó misszió szervezésére kerül sor. Azon tagállam, amelyben a tanácsadó misszióra sor került, és a Bizottság – a kölcsönös tanulás előmozdítása céljából – tájékoztatja a kritikus szervezetek rezilienciájával foglalkozó csoportot is a tanácsadó misszió főbb megállapításairól és a levont tanulságokról.

V. FEJEZET

EGYÜTTMŰKÖDÉS ÉS JELENTÉSTÉTEL

19. cikk

A kritikus szervezetek rezilienciájával foglalkozó csoport

(1) Létrejön a kritikus szervezetek rezilienciájával foglalkozó csoport. A kritikus szervezetek rezilienciájával foglalkozó csoportnak támogatnia kell a Bizottságot, és elő kell segítenie a tagállamok közötti együttműködést és az információcserét az ezen irányelvvel kapcsolatos kérdésekben.

(2) A kritikus szervezetek rezilienciájával foglalkozó csoport a tagállamok és a Bizottság képviselőiből áll, akik adott esetben biztonsági tanúsítvánnyal rendelkeznek. Amennyiben a feladatai ellátása szempontjából releváns, a kritikus szervezetek rezilienciájával foglalkozó csoport felkérhet releváns érdekelt feleket, hogy vegyenek részt a munkájában. Az Európai Parlament kérésére a Bizottság szakértőket hívhat meg az Európai Parlamentből, hogy vegyenek részt a kritikus szervezetek rezilienciájával foglalkozó csoport ülésein.

A kritikus szervezetek rezilienciájával foglalkozó csoport elnöki tisztségét a Bizottság képviselője tölti be.

(3) A kritikus szervezetek rezilienciájával foglalkozó csoport a következő feladatokat látja el:

a) a Bizottság támogatása abban, hogy segítse a tagállamokat azon képességük megerősítésében, hogy ezen irányelvvel összhangban hozzájáruljanak a kritikus szervezetek rezilienciájának biztosításához;

b) a stratégiák elemzése a legjobb gyakorlatok azonosítása érdekében a stratégiák tekintetében;

c) a legjobb gyakorlatok megosztásának elősegítése a kritikus szervezeteknek a tagállamok által a 6. cikk (1) bekezdése alapján elvégzett azonosítása tekintetében, többek között a határokon átnyúló és a több ágazatot érintő függőségekkel kapcsolatban, valamint a kockázatokra és eseményekre vonatkozóan;

d) adott esetben hozzájárulás – az ezen irányelvvel kapcsolatos kérdéseket illetően – az uniós szintű rezilienciára vonatkozó dokumentumokhoz;

e) hozzájárulás a 7. cikk (3) bekezdésében és a 13. cikk (5) bekezdésében említett iránymutatások, valamint – kérésre – az ezen irányelv alapján elfogadott bármely felhatalmazáson alapuló vagy végrehajtási jogi aktus elkészítéséhez;

f) a 9. cikk (3) bekezdésében említett összefoglaló jelentések elemzése a 15. cikk (3) bekezdésének megfelelően hozott intézkedésekkel kapcsolatos legjobb gyakorlatok megosztásának előmozdítása céljából;

g) az eseményekre vonatkozó, a 15. cikkben említett értesítéssel kapcsolatos legjobb gyakorlatok cseréje;

h) a tanácsadó missziók összefoglaló jelentéseinek és a levont tanulságoknak a megvitatása a 18. cikk (10) bekezdésének megfelelően;

i) a kritikus szervezetek ezen irányelv szerinti rezilienciájával kapcsolatos innovációra, kutatásra és fejlesztésre vonatkozó információk és legjobb gyakorlatok cseréje;

j) adott esetben a kritikus szervezetek rezilienciájával kapcsolatos kérdésekről az érintett uniós intézményekkel, szervekkel, hivatalokkal és ügynökségekkel folytatott információcsere.

(4) A kritikus szervezetek rezilienciájával foglalkozó csoport 2025. január 17-ig, és azt követően kétévente munkaprogramot állít össze a célkitűzései és feladatai végrehajtása érdekében végzendő tevékenységek tekintetében. Az említett munkaprogramnak összhangban kell lennie ezen irányelv követelményeivel és célkitűzéseivel.

(5) A kritikus szervezetek rezilienciájával foglalkozó csoport rendszeresen és minden esetben évente legalább egy alkalommal összeül az (EU) 2022/2555 irányelv alapján létrehozott együttműködési csoporttal az együttműködés és az információcsere ösztönzése és elősegítése érdekében.

(6) A Bizottság – az 1. cikk (4) bekezdését tiszteletben tartva – végrehajtási jogi aktusokat fogadhat el a kritikus szervezetek rezilienciájával foglalkozó csoport működéséhez szükséges eljárásrend megállapítása céljából. Ezeket a végrehajtási jogi aktusokat a 24. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(7) A Bizottság – 2027. január 17-ig, azt követően szükség esetén, de legalább négyévente – a kritikus szervezetek rezilienciájával foglalkozó csoport számára összefoglaló jelentést biztosít a tagállamok által a 4. cikk (3) bekezdése és az 5. cikk (4) bekezdése alapján szolgáltatott információkról.

20. cikk

A Bizottság által az illetékes hatóságoknak és a kritikus szervezeteknek nyújtott támogatás

(1) A Bizottság adott esetben támogatja a tagállamokat és a kritikus szervezeteket az ezen irányelv szerinti kötelezettségeik teljesítésében. A Bizottság uniós szintű áttekintést készít az alapvető szolgáltatások nyújtásával kapcsolatos, határokon átnyúló és több ágazatot érintő kockázatokról, tanácsadó missziókat szervez a 13. cikk (4) bekezdésében és a 18. cikkben említettek szerint, valamint az Unió egész területén elősegíti a tagállamok és a szakértők közötti információcserét.

(2) A Bizottság kiegészíti a tagállamok 10. cikkben említett tevékenységeit azáltal, hogy legjobb gyakorlatokat, iránymutatásokat és módszertanokat, valamint határokon átnyúló képzési tevékenységeket és a kritikus szervezetek rezilienciájának tesztelését szolgáló gyakorlatokat dolgoz ki.

(3) A Bizottság tájékoztatja a tagállamokat azon uniós szintű pénzügyi forrásokról, amelyek a kritikus szervezetek rezilienciájának fokozása érdekében a tagállamok rendelkezésére állnak.

VI. FEJEZET

FELÜGYELET ÉS JOGÉRVÉNYESÍTÉS

21. cikk

Felügyelet és jogérvényesítés

(1) Annak értékelése érdekében, hogy a tagállamok által a 6. cikk alapján kritikus szervezetként azonosított szervezetek megfelelnek-e az ezen irányelvben megállapított kötelezettségeknek, a tagállamok biztosítják, hogy az illetékes hatóságok rendelkezzenek a következőkhöz szükséges hatáskörrel és eszközökkel:

a) helyszíni ellenőrzéseket végezni a kritikus infrastruktúránál és a kritikus szervezet által alapvető szolgáltatásai nyújtásához használt telephelyeken, valamint külső ellenőrzéseket végezni a kritikus szervezetek által a13. cikknek megfelelően hozott intézkedések tekintetében;

b) a kritikus szervezetek tekintetében ellenőrzéseket végezni vagy elrendelni.

(2) A tagállamok biztosítják, hogy az illetékes hatóságok rendelkezzenek az ahhoz szükséges hatáskörrel és eszközökkel, hogy – amennyiben az ezen irányelv szerinti feladataik ellátásához szükséges – előírják, hogy az (EU) 2022/2555 irányelv szerinti szervezetek, amelyeket a tagállamok ezen irányelv alapján kritikus szervezetként azonosítottak, az említett hatóságok által meghatározott észszerű határidőn belül biztosítsák a következőket:

a) az annak értékeléséhez szükséges információk, hogy az említett szervezetek által a rezilienciájuk biztosítása érdekében hozott intézkedések megfelelnek-e a 13. cikkben meghatározott követelményeknek;

b) az említett intézkedések tényleges végrehajtására vonatkozó bizonyítékok, beleértve az adott szervezet által kiválasztott független és képesített ellenőr által a szervezet költségén végzett ellenőrzés eredményeit is.

Az illetékes hatóságoknak az említett tájékoztatási kötelezettség előírásakor fel kell tüntetniük az előírás célját, és meg kell határozniuk a kért információkat.

(3) A 22. cikknek megfelelő szankciókiszabás lehetőségének sérelme nélkül, az illetékes hatóságok az e cikk (1) bekezdésében említett felügyeleti intézkedéseket vagy az információk e cikk (2) bekezdésében említett értékelését követően elrendelhetik, hogy az érintett kritikus szervezetek az említett hatóságok által meghatározott észszerű határidőn belül tegyék meg a szükséges és arányos intézkedéseket az ezen irányelvet érintő, feltárt jogsértések orvoslására, és tájékoztassák az említett hatóságokat a meghozott intézkedésekről. Az említett elrendelő határozatokban különösen a jogsértés súlyosságát kell figyelembe venni.

(4) A tagállamok biztosítják, hogy az (1), a (2) és a (3) bekezdésben meghatározott hatásköröket csak megfelelő biztosítékok mellett lehessen gyakorolni. Az említett biztosítékoknak garantálniuk kell különösen, hogy e hatáskörök gyakorlására objektív, átlátható és arányos módon kerüljön sor, valamint hogy az érintett kritikus szervezetek jogai és jogos érdekei – így például a kereskedelmi és üzleti titkok védelme – megfelelő védelemben részesüljenek, ideértve a meghallgatáshoz való jogot, a védelemhez való jogot és a független bíróság előtti hatékony jogorvoslathoz való jogot is.

(5) A tagállamok biztosítják, hogy amikor egy ezen irányelv szerinti illetékes hatóság e cikk alapján értékeli valamely kritikus szervezet megfelelőségét, az említett illetékes hatóság tájékoztassa az érintett tagállamoknak az (EU) 2022/2555 irányelv szerinti illetékes hatóságait. E célból a tagállamok biztosítják, hogy az ezen irányelv szerinti illetékes hatóságok felkérhessék az (EU) 2022/2555 irányelv szerinti illetékes hatóságokat arra, hogy gyakorolják felügyeleti és jogérvényesítési hatáskörüket egy, az említett irányelv szerinti olyan szervezet tekintetében, amelyet ezen irányelv alapján kritikus szervezetként azonosítottak. E célból a tagállamok biztosítják, hogy az ezen irányelv szerinti illetékes hatóságok együttműködjenek és információt cseréljenek az (EU) 2022/2555 irányelv szerinti illetékes hatóságokkal.

22. cikk

Szankciók

A tagállamok megállapítják az ezen irányelv alapján elfogadott nemzeti rendelkezések megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és meghoznak minden szükséges intézkedést ezek végrehajtására. Az előírt szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük. A tagállamok e szabályokról és intézkedésekről 2024. október 17-ig tájékoztatják a Bizottságot, és haladéktalanul tájékoztatják a Bizottságot az e szabályokat és intézkedéseket érintő minden későbbi módosításról.

VII. FEJEZET

FELHATALMAZÁSON ALAPULÓ JOGI AKTUSOK ÉS VÉGREHAJTÁSI JOGI AKTUSOK

23. cikk

A felhatalmazás gyakorlása

(1) A felhatalmazáson alapuló jogi aktusok elfogadására vonatkozóan a Bizottság részére adott felhatalmazás feltételeit ez a cikk határozza meg.

(2) A Bizottságnak az 5. cikk (1) bekezdésében említett, felhatalmazáson alapuló jogi aktus elfogadására vonatkozó felhatalmazása ötéves időtartamra szól 2023. január 16-tól kezdődő hatállyal.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja az 5. cikk (1) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon, vagy a benne megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

(4) A felhatalmazáson alapuló jogi aktus elfogadása előtt a Bizottság a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban megállapított elvekkel összhangban konzultál az egyes tagállamok által kijelölt szakértőkkel.

(5) A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul és egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.

(6) Az 5. cikk (1) bekezdése értelmében elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha az Európai Parlamentnek és a Tanácsnak a jogi aktusról való értesítését követő két hónapon belül sem az Európai Parlament, sem a Tanács nem emelt ellene kifogást, illetve ha az említett időtartam lejártát megelőzően mind az Európai Parlament, mind a Tanács arról tájékoztatta a Bizottságot, hogy nem fog kifogást emelni. Az Európai Parlament vagy a Tanács kezdeményezésére ez az időtartam két hónappal meghosszabbodik.

24. cikk

A bizottsági eljárás

(1) A Bizottságot egy bizottság segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottságnak minősül.

(2) Az e bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 5. cikkét kell alkalmazni.

VIII. FEJEZET

ZÁRÓ RENDELKEZÉSEK

25. cikk

Jelentéstétel és felülvizsgálat

A Bizottság 2027. július 17-ig jelentést nyújt be az Európai Parlamentnek és a Tanácsnak, amelyben értékeli, hogy az egyes tagállamok milyen mértékben tették meg az irányelvnek való megfeleléshez szükséges intézkedéseket.

A Bizottság rendszeres időközönként felülvizsgálja ezen irányelv működését, és jelentést tesz arról az Európai Parlamentnek és a Tanácsnak. Az említett jelentésben értékelni kell különösen az irányelv hozzáadott értékét, hatását a kritikus szervezetek rezilienciájának biztosítása szempontjából, és azt, hogy szükséges-e módosítani ezen irányelv mellékletét. A Bizottság az első ilyen jelentést 2029. június 17-ig nyújtja be. Az e cikk szerinti jelentéstétel céljából a Bizottság figyelembe veszi a kritikus szervezetek rezilienciájával foglalkozó csoport releváns dokumentumait.

26. cikk

Átültetés

(1) A tagállamok legkésőbb 2024. október 17-ig elfogadják és kihirdetik azokat a rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek megfeleljenek. Erről haladéktalanul tájékoztatják a Bizottságot.

A tagállamok ezeket a rendelkezéseket 2024. október 18-tól alkalmazzák.

(2) Amikor a tagállamok elfogadják az (1) bekezdésben említett rendelkezéseket, azokban hivatkozni kell erre az irányelvre, vagy azokhoz hivatalos kihirdetésük alkalmával ilyen hivatkozást kell fűzni. A hivatkozás módját a tagállamok határozzák meg.

27. cikk

A 2008/114/EK irányelv hatályon kívül helyezése

A 2008/114/EK irányelv 2024. október 18-ával hatályát veszti.

A hatályon kívül helyezett irányelvre való hivatkozásokat erre az irányelvre való hivatkozásnak kell tekinteni.

28. cikk

Hatálybalépés

Ez az irányelv az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

29. cikk

Címzettek

Ennek az irányelvnek a tagállamok a címzettjei.

Kelt Strasbourgban, 2022. december 14-én.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*
R. METSOLA	M. BEK

MELLÉKLET

ÁGAZATOK, ALÁGAZATOK ÉS A SZERVEZETEK KATEGÓRIÁI

Ágazatok	Alágazatok	Szervezetek kategóriái
1. Energia	a) Villamos energia	– Az (EU) 2019/944 európai parlamenti és tanácsi irányelv ([1]) 2. cikkének 57. pontjában meghatározott villamosenergia-ipari vállalkozások, amelyek az említett irányelv 2. cikkének 12. pontjában meghatározott „ellátás” funkciót látják el
		– Az (EU) 2019/944 irányelv 2. cikkének 29. pontjában meghatározott elosztórendszer-üzemeltetők
		– Az (EU) 2019/944 irányelv 2. cikkének 35. pontjában meghatározott átvitelirendszer-üzemeltetők
		– Az (EU) 2019/944 irányelv 2. cikkének 38. pontjában meghatározott termelők
		– Az (EU) 2019/943 európai parlamenti és tanácsi rendelet ([2]) 2. cikkének 8. pontjában meghatározott kijelölt villamosenergiapiac-üzemeltetők
		– Az (EU) 2019/944 irányelv 2. cikkének 18., 20. és 59. pontjában meghatározott aggregálási, keresletoldali válasz- vagy energiatárolási szolgáltatásokat nyújtó, az (EU) 2019/943 rendelet 2. cikkének 25. pontjában meghatározott piaci szereplők
	b) Távfűtés vagy távhűtés	– Az (EU) 2018/2001 európai parlamenti és tanácsi irányelv ([3]) 2. cikkének 19. pontjában meghatározott távfűtés vagy távhűtés üzemeltetői
	c) Kőolaj	– Kőolajvezetékek üzemeltetői
		– Kőolajtermelő, -finomító és -feldolgozó létesítmények, -tárolás és -szállítás üzemeltetői
		– A 2009/119/EK tanácsi irányelv ([4]) 2. cikkének f) pontjában meghatározott központi készletezőszervek

Ágazatok	Alágazatok	Szervezetek kategóriái
	d) Földgáz	– A 2009/73/EK európai parlamenti és tanácsi irányelv ([5]) 2. cikkének 8. pontjában meghatározott ellátó vállalkozások
		– A 2009/73/EK irányelv 2. cikkének 6. pontjában meghatározott elosztórendszer-üzemeltetők
		– A 2009/73/EK irányelv 2. cikkének 4. pontjában meghatározott szállításirendszer-üzemeltetők
		– A 2009/73/EK irányelv 2. cikkének 10. pontjában meghatározott tárolásirendszer-üzemeltetők
		– A 2009/73/EK irányelv 2. cikkének 12. pontjában meghatározott LNG-létesítmény-rendszerüzemeltetők
		– A 2009/73/EK irányelv 2. cikkének 1. pontjában meghatározott földgázipari vállalkozások
		– Földgázfinomító és -feldolgozó létesítmények üzemeltetői
	e) Hidrogén	– A hidrogéntermelés, -tárolás és -szállítás üzemeltetői
2. Közlekedés	a) Légi	– A 300/2008/EK rendelet 3. cikkének 4. pontjában meghatározott, kereskedelmi célra igénybe vett légi fuvarozók
		– A 2009/12/EK európai parlamenti és tanácsi irányelv ([6]) 2. cikkének 2. pontjában meghatározott repülőtér-irányító szervezetek, az említett irányelv 2. cikkének 1. pontjában meghatározott repülőterek, a törzshálózathoz tartozó, az 1315/2013/EU európai parlamenti és tanácsi rendelet ([7]) II. mellékletének 2. szakaszában felsorolt törzshálózati repülőtereket is beleértve, valamint a repülőtereken található kapcsolódó létesítményeket üzemeltető szervezetek
		– Az 549/2004/EK európai parlamenti és tanácsi rendelet ([8]) 2. cikkének 1. pontjában meghatározott légiforgalmi irányító (ATC) szolgálatot ellátó forgalomirányítási üzemeltetők

Ágazatok	Alágazatok	Szervezetek kategóriái
	b) Vasúti	– A 2012/34/EU európai parlamenti és tanácsi irányelv ([9]) 3. cikkének 2. pontjában meghatározott pályahálózat-működtetők
		– A 2012/34/EU irányelv 3. cikkének 1. pontjában meghatározott vállalkozó vasúti társaságok és az említett irányelv 3. cikkének 12. pontjában meghatározott, a kiszolgáló létesítmények üzemeltetői
	c) Vízi	– A tengeri szállítás vonatkozásában a 2004/725/EK rendelet I. mellékletében meghatározott belvízi, tengeri és part menti személy- és teherszállító vállalkozások, az említett vállalkozások által üzemeltetett egyes hajók kivételével
		– A 2005/65/EK irányelv 3. cikkének 1. pontjában meghatározott kikötőket irányító szervek, a 725/2004/EK rendelet 2. cikkének 11. pontjában meghatározott kikötőlétesítményeket is beleértve, valamint a kikötőkben található létesítményeket és berendezéseket üzemeltető szervek
		– A 2002/59/EK európai parlamenti és tanácsi irányelv ([10]) 3. cikkének o) pontjában meghatározott hajóforgalmi szolgálatok üzemeltetői
	d) Közúti	– Az (EU) 2015/962 felhatalmazáson alapuló bizottsági rendelet ([11]) 2. cikkének 12. pontjában meghatározott, a forgalomirányításért felelős közúti hatóságok, azon közigazgatási szervek kivételével, amelyek általános tevékenységének nem alapvető része a forgalomszervezés vagy az intelligens közlekedési rendszerek üzemeltetése
		– A 2010/40/EU európai parlamenti és tanácsi irányelv ([12]) 4. cikkének 1. pontjában meghatározott intelligens közlekedési rendszerek üzemeltetői
	e) Tömegközlekedés	– Az 1370/2007/EK európai parlamenti és tanácsi rendelet ([13]) 2. cikkének d) pontjában meghatározott közszolgáltatók
3. Banki szolgáltatások		– Az 575/2013/EU rendelet 4. cikkének 1. pontjában meghatározott hitelintézetek
4. Pénzügyi piaci infrastruktúra		– A 2014/65/EU irányelv 4. cikkének 24. pontjában meghatározott kereskedési helyszínek üzemeltetői
		– A 648/2012/EU rendelet 2. cikkének 1. pontjában meghatározott központi szerződő felek

Ágazatok	Alágazatok	Szervezetek kategóriái
5. Egészségügy		– A 2011/24/EU európai parlamenti és tanácsi irányelv ([14]) 3. cikkének g) pontjában meghatározott egészségügyi szolgáltatók
		– Az (EU) 2022/2371 európai parlamenti és tanácsi rendelet ([15]) 15. cikkében meghatározott uniós referencialaboratóriumok
		– A 2001/83/EK európai parlamenti és tanácsi irányelv ([16]) 1. cikkének 2. pontjában meghatározott, gyógyszerek kutatásával és fejlesztésével foglalkozó szervezetek
		– A NACE Rev. 2. C nemzetgazdasági ágának 21. ágazatában említett gyógyszeripari alaptermékeket és gyógyszerkészítményeket gyártó szervezetek
		– Az (EU) 2022/123 európai parlamenti és tanácsi rendelet ([17]) 22. cikke értelmében népegészségügyi szükséghelyzet idején kritikus fontosságúnak ítélt orvostechnikai eszközöket („a népegészségügyi szükséghelyzet kritikus fontosságú eszközeinek jegyzéke") előállító szervezetek
		– A 2001/83/EK irányelv 79. cikkében említett nagykereskedelmi forgalmazási engedélyek birtokában lévő szervezetek
6. Ivóvíz		– Az (EU) 2020/2184 európai parlamenti és tanácsi irányelv ([18]) 2. cikke 1. pontjának a) alpontjában meghatározott, emberi fogyasztásra szánt víz szállítói és forgalmazói, azon forgalmazókat kivéve, amelyek számára az emberi fogyasztásra szánt víz forgalmazása a más áruk és javak forgalmazásából álló általános tevékenységüknek nem alapvető része
7. Szennyvíz		– A 91/271/EGK tanácsi irányelv ([19]) 2. cikkének 1., 2. és 3. pontjában meghatározott települési szennyvíz, háztartási szennyvíz és ipari szennyvíz összegyűjtését, ártalmatlanítását vagy kezelését végző vállalkozások, azon vállalkozásokat kivéve, amelyek általános tevékenységének nem alapvető része a települési szennyvíz, háztartási szennyvíz és ipari szennyvíz összegyűjtése, ártalmatlanítása és kezelése

Ágazatok	Alágazatok	Szervezetek kategóriái
8. Digitális infrastruktúra		– Az (EU) 2022/2555 irányelv 6. cikkének 18. pontjában meghatározott internetkapcsolódási pontok szolgáltatói
		– Az (EU) 2022/2555 irányelv 6. cikkének 20. pontjában meghatározott DNS-szolgáltatók, a gyökérnév szerverek üzemeltetőinek kivételével
		– Az (EU) 2022/2555 irányelv 6. cikkének 21. pontjában meghatározott legfelső szintű doménnév-nyilvántartók
		– Az (EU) 2022/2555 irányelv 6. cikkének 30. pontjában meghatározott felhőszolgáltatások szolgáltatói
		– Az (EU) 2022/2555 irányelv 6. cikkének 31. pontjában meghatározott adatközpont-szolgáltatás nyújtói
		– Az (EU) 2022/2555 irányelv 6. cikkének 32. pontjában meghatározott tartalomszolgáltató hálózatok szolgáltatói
		– A 910/2014/EU európai parlamenti és tanácsi rendelet ([20]) 3. cikkének 19. pontjában meghatározott bizalmi szolgáltatók
		– Az (EU) 2018/1972 európai parlamenti és tanácsi irányelv ([21]) 2. cikkének 8. pontjában meghatározott nyilvános elektronikus hírközlő hálózatok üzemeltetői
		– Az (EU) 2018/1972 irányelv 2. cikkének 4. pontjában meghatározott elektronikus hírközlési szolgáltatások nyújtói, amennyiben szolgáltatásaik nyilvánosan elérhetőek
9. Közigazgatás		– A központi kormányzat közigazgatási szervezetei, a tagállamok által a nemzeti joggal összhangban meghatározottak szerint
10. Világűr		– A tagállamok vagy magánfelek tulajdonában, kezelésében és üzemeltetésében lévő azon földi infrastruktúra üzemeltetői, amelyek támogatják az űralapú szolgáltatások nyújtását, kivéve az (EU) 2018/1972 irányelv 2. cikkének 8. pontjában meghatározott nyilvános elektronikus hírközlő hálózatok üzemeltetőit

Ágazatok	Alágazatok	Szervezetek kategóriái
11. Élelmiszer-előállítás, -feldolgozás és -forgalmazás		– A 178/2002/EK európai parlamenti és tanácsi rendelet ([22]) 3. cikkének 2. pontjában meghatározott élelmiszer-vállalkozások, amelyek kizárólag logisztikával és nagykereskedelmi forgalmazással, valamint nagyléptékű ipari termeléssel és feldolgozással foglalkoznak

([1]) Az Európai Parlament és a Tanács (EU) 2019/944 irányelve (2019. június 5.) a villamos energia belső piacára vonatkozó közös szabályokról és a 2012/27/EU irányelv módosításáról (HL L 158., 2019.6.14., 125. o.).

([2]) Az Európai Parlament és a Tanács (EU) 2019/943 rendelete (2019. június 5.) a villamos energia belső piacáról (HL L 158., 2019.6.14., 54. o.).

([3]) Az Európai Parlament és a Tanács (EU) 2018/2001 irányelve (2018. december 11.) a megújuló energiaforrásokból előállított energia használatának előmozdításáról (HL L 328., 2018.12.21., 82. o.).

([4]) A Tanács 2009/119/EK irányelve (2009. szeptember 14.) a tagállamok minimális kőolaj- és/vagy kőolajtermék-készletezési kötelezettségéről (HL L 265., 2009.10.9., 9. o.).

([5]) Az Európai Parlament és a Tanács 2009/73/EK irányelve (2009. július 13.) a földgáz belső piacára vonatkozó közös szabályokról és a 2003/55/EK irányelv hatályon kívül helyezéséről (HL L 211., 2009.8.14., 94. o.).

([6]) Az Európai Parlament és a Tanács 2009/12/EK irányelve (2009. március 11.) a repülőtéri díjakról (HL L 70., 2009.3.14., 11. o.).

([7]) Az Európai Parlament és a Tanács 1315/2013/EU rendelete (2013. december 11.) a transzeurópai közlekedési hálózat fejlesztésére vonatkozó uniós iránymutatásokról és a 661/2010/EU határozat hatályon kívül helyezéséről (HL L 348., 2013.12.20., 1. o.).

([8]) Az Európai Parlament és a Tanács 549/2004/EK rendelete (2004. március 10.) az egységes európai égbolt létrehozására vonatkozó keret megállapításáról (keretrendelet) (HL L 96., 2004.3.31., 1. o.).

([9]) Az Európai Parlament és a Tanács 2012/34/EU irányelve (2012. november 21.) az egységes európai vasúti térség létrehozásáról (HL L 343., 2012.12.14., 32. o.).

([10]) Az Európai Parlament és a Tanács 2002/59/EK irányelve (2002. június 27.) a közösségi hajóforgalomra vonatkozó megfigyelő és információs rendszer létrehozásáról és a 93/75/EGK irányelv hatályon kívül helyezéséről (HL L 208., 2002.8.5., 10. o.).

([11]) A Bizottság (EU) 2015/962 felhatalmazáson alapuló rendelete (2014. december 18.) a 2010/40/EU európai parlamenti és tanácsi irányelvnek az EU egészére kiterjedő valós idejű forgalmi információs szolgáltatások nyújtása tekintetében történő kiegészítéséről (HL L 157., 2015.6.23., 21. o.).

([12]) Az Európai Parlament és a Tanács 2010/40/EU irányelve (2010. július 7.) az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről (HL L 207., 2010.8.6., 1. o.).

([13]) Az Európai Parlament és a Tanács 1370/2007/EK rendelete (2007. október 23.) a vasúti és közúti személyszállítási közszolgáltatásról, valamint az 1191/69/EGK és az 1107/70/EGK tanácsi rendelet hatályon kívül helyezéséről (HL L 315., 2007.12.3., 1. o.).

([14]) Az Európai Parlament és a Tanács 2011/24/EU irányelve (2011. március 9.) a határon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről (HL L 88., 2011.4.4., 45. o.).

([15]) Az Európai Parlament és a Tanács (EU) 2022/2371 rendelete (2022. november 23.) a határokon át terjedő súlyos egészségügyi veszélyekről és az 1082/2013/EU határozat hatályon kívül helyezéséről (HL L 314., 2022.12.6., 26. o.).

([16]) Az Európai Parlament és a Tanács 2001/83/EK irányelve (2001. november 6.) az emberi felhasználásra szánt gyógyszerek közösségi kódexéről (HL L 311., 2001.11.28., 67. o.).

([17]) Az Európai Parlament és a Tanács (EU) 2022/123 rendelete (2022. január 25.) az Európai Gyógyszerügynökség által a gyógyszerek és orvostechnikai eszközök tekintetében a válsághelyzetekre való felkészültség és a válságkezelés terén betöltött szerep megerősítéséről (HL L 20., 2022.1.31., 1. o.).

([18]) Az Európai Parlament és a Tanács (EU) 2020/2184 irányelve (2020. december 16.) az emberi fogyasztásra szánt víz minőségéről (HL L 435., 2020.12.23., 1. o.).

([19]) A Tanács 91/271/EGK irányelve (1991. május 21.) a települési szennyvíz kezeléséről (HL L 135., 1991.5.30., 40. o.).

([20]) Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (HL L 257., 2014.8.28., 73. o.).

([21]) Az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról (HL L 321., 2018.12.17., 36. o.).

([22]) Az Európai Parlament és a Tanács 178/2002/EK rendelete (2002. január 28.) az élelmiszerjog általános elveiről és követelményeiről, az Európai Élelmiszerbiztonsági Hatóság létrehozásáról és az élelmiszerbiztonságra vonatkozó eljárások megállapításáról (HL L 31., 2002.2.1., 1. o.).

ISSN 1977-0731 (elektronikus kiadás)
ISSN 1725-5090 (nyomtatott kiadás)

Az Európai Unió
Kiadóhivatala
L-2985 Luxembourg
LUXEMBURG

HU