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 intézményeinak 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