



EURÓPAI
BIZOTTSÁG

Brüsszel, 2020.12.16.
COM(2020) 823 final

2020/0359 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE

**az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről,
valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről**

(EGT-vonatkozású szöveg)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

INDOKOLÁS

1. A JAVASLAT HÁTTERE

• A javaslat indokai és céljai

Ez a javaslat egy olyan intézkedéscsomag része, amely tovább javítja az állami és magánszervezetek, az illetékes hatóságok és az Unió egészének rezilienciáját és eseményelhárítási képességeit a kiberbiztonság és a kritikus infrastruktúrák védelme terén. Összhangban áll a Bizottság azon prioritásaival, amelyek célja egyfelől Európának a digitális kor kihívásaira való felkészítése, másfelől a jövő kihívásaira felkészült, az emberek javát szolgáló gazdaság kiépítése. A kiberbiztonság kiemelt fontosságú a Bizottság Covid19-válságra adott válaszában. A csomag új kiberbiztonsági stratégiát tartalmaz, amelynek célja az Unió stratégiai autonómiájának megerősítése a reziliencia és a kollektív válasz javítása, valamint a nyitott és globális internet kiépítése érdekében. Végül a csomag tartalmazza az alapvető szolgáltatásokat nyújtó kritikus szereplők rezilienciájáról szóló irányelvre irányuló javaslatot, amelynek célja az említett szolgáltatókkal szembeni fizikai fenyegetések mérséklése.

Ez a javaslat a hálózati és információs rendszerek biztonságáról szóló (EU) 2016/1148 irányelvre (a kiberbiztonsági irányelv) épít és azt hatályon kívül helyezi, valamint a kiberbiztonságra vonatkozó első uniós szintű jogszabályként jogi intézkedéseket tartalmaz az Unión belüli kiberbiztonság általános szintjének emelésére. A kiberbiztonsági irányelv (1) hozzájárult a kiberbiztonsági képességek nemzeti szintű javításához azáltal, hogy előírta a tagállamoknak, hogy fogadjanak el nemzeti kiberbiztonsági stratégiákat és jelöljenek ki kiberbiztonsági hatóságokat; (2) a tagállamok között fokozta az uniós szintű együttműködést a stratégiai és operatív információk cseréjét megkönnyítő különféle fórumok létrehozásával; valamint (3) javította az állami és magánszervezetek kiberrezilienciáját hét meghatározott ágazatban (energia, közlekedés, banki tevékenység, pénzügyi piaci infrastruktúra, egészségügy, ivóvízellátás és -elosztás, valamint digitális infrastruktúrák) és három digitális szolgáltatásban (online piacterek, online keresőmotorok és felhőszolgáltatások) azáltal, hogy előírja a tagállamoknak, hogy biztosítsák az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók részéről a kiberbiztonsági követelmények bevezetését és az események jelentését.

A javaslat korszerűsíti a meglévő jogi keretet, figyelembe véve a belső piac elmúlt években megnövekedett digitalizálódását és a kiberbiztonsági fenyegetettség alakulását. Mindkét fejlemény tovább erősödött a Covid19-válság kezdete óta. A javaslat számos olyan hiányossággal is foglalkozik, amely akadályozta a kiberbiztonsági irányelv teljes potenciáljának kiaknázását.

Figyelemre méltó eredményei ellenére a kiberbiztonsági irányelv – amely a kiberbiztonság intézményi és szabályozási megközelítésével kapcsolatban számos tagállamban megnyitotta az utat a gondolkodásmód jelentős megváltozása előtt – korlátait is bebizonyította. A társadalom digitális átalakulása (amelyet felgyorsított a Covid19-válság) kibővítette a fenyegetettségek körét, és új kihívásokat hoz, amelyek a helyzethez igazodó és innovatív válaszokat igényelnek. A kibertámadások száma továbbra is növekszik, egyre kifinomultabb támadások érkeznek a legkülönbözőbb, EU-n belüli és azon kívüli forrásokból.

A kiberbiztonsági irányelv működésének a hatásvizsgálat céljából végzett értékelése a következő problémákat azonosította: (1) az Unióban működő vállalkozások alacsony szintű kiberrezilienciája; (2) a tagállamok és az ágazatok rezilienciájának következetlenségei; valamint (3) a közös helyzetismeret alacsony szintje és a közös válsághárítás hiánya. Például egy tagállam bizonyos nagyobb kórházai nem tartoznak a kiberbiztonsági irányelv

hatálya alá, és ezért nem kötelesek végrehajtani az abból eredő biztonsági intézkedéseket, míg egy másik tagállamban az ország szinte minden egyes egészségügyi szolgáltatójára kiterjednek a hálózati és információs rendszerek biztonsági követelményei.

A javaslat a célravezető és hatásos szabályozás (REFIT) programon belüli kezdeményezésként az illetékes hatóságok szabályozási terheinek, valamint az állami és magánszervezetek megfelelési költségeinek csökkentését célozza. Legfőképpen ezt úgy éri el, hogy megszünteti az illetékes hatóságok azon kötelezettségét, hogy azonosítsák az alapvető szolgáltatásokat nyújtó szereplőket, valamint emeli a biztonsági és jelentéstételi követelmények harmonizációjának szintjét, hogy megkönnyítse a határokon átnyúló szolgáltatásokat nyújtó szervezetek szabályozási megfelelését. Ugyanakkor az illetékes hatóságok számos új feladatot is kapnak, ideértve az olyan ágazatokban működő szervezetek felügyeletét, amelyek eddig nem tartoznak a kiberbiztonsági irányelv hatálya alá.

• **Összhang a szabályozási terület jelenlegi rendelkezéseivel**

Ez a javaslat azon meglévő jogi eszközök és küszöbön álló uniós szintű kezdeményezések tágabb körének része, amelyek célja az állami és magánszervezetek fenyegetésekkel szembeni rezilienciájának növelése.

A kiberbiztonság területén ezek különösen az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló (EU) 2018/1972 irányelv (amelynek kiberbiztonsággal kapcsolatos rendelkezéseit jelen javaslat rendelkezései váltják fel), valamint a pénzügyi ágazat digitális működési rezilienciájáról szóló rendeletre irányuló javaslat (COM(2020) 595 final), amely a jelenlegi javaslat hatálybalépését követően *lex specialis*-nak fog minősülni.

A fizikai biztonság területén a javaslat kiegészíti a kritikus jelentőségű szervezetek rezilienciájáról szóló irányelvre irányuló javaslatot, amely felülvizsgálja az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint a védelmük javításának szükségességének értékeléséről szóló 2008/114/EK irányelvet (az európai kritikus infrastruktúrákról szóló irányelv), amely uniós folyamatot hoz létre az európai kritikus infrastruktúrák azonosítására és kijelölésére, valamint megközelítést határoz meg azok védelmének javítására. 2020 júliusában a Bizottság elfogadta a biztonsági unióra vonatkozó uniós stratégiát¹, amely elismerte a fizikai és digitális infrastruktúrák közötti növekvő összekapcsolódást és kölcsönös függőséget. Hangsúlyozta, hogy koherensebb és következetesebb megközelítésre van szükség az európai kritikus infrastruktúrákról szóló irányelv és a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 irányelv között.

A javaslat ezért szorosan illeszkedik a kritikus szervezetek rezilienciájáról szóló irányelvre irányuló javaslathoz, amelynek célja a kritikus szervezetek fizikai fenyegetésekkel szembeni rezilienciájának javítása nagy számú ágazatban. A javaslat célja annak biztosítása, hogy az illetékes hatóságok mindkét jogi aktus alapján egymást kiegészítő intézkedéseket hozzanak és szükség szerint információt cseréljenek a kiberrezilienciáról és nem számítógépes jellegű rezilienciáról, valamint hogy a jelen javaslat szerint „alapvetőnek” tekintett ágazatok különösen kritikus szereplőire is általánosabb rezilienciafokozó kötelezettségeket írjanak elő, hangsúlyozva a nem számítógépes kockázatokat.

¹ COM(2020) 605 final.

- **Összhang az Unió egyéb szakpolitikáival**

Az „Európa digitális jövőjének megteremtése” című közleményben foglaltaknak megfelelően² Európa számára kulcsfontosságú, hogy kiaknázza a digitális kor minden előnyét, és megerősítse ipari és innovációs kapacitását – biztonságos és etikus határokon belül. Az európai adatstratégia négy oszlopot – az adatvédelmet, az alapvető jogokat, a biztonságot és a kiberbiztonságot – határoz meg, amelyek alapvető előfeltételei egy adatok felhasználásával felhatalmazott társadalomnak.

Az Európai Parlament 2019. március 12-i állásfoglalásában felhívja „[...] a Bizottságot, hogy mérje fel az irányelv hatálya más, ágazatspecifikus jogszabály hatálya alá nem tartozó kritikus ágazatokra és szolgáltatásokra való további kiterjesztésének szükségességét;”.³ A Tanács 2020. június 9-i következtetéseiben üdvözli „[...] a Bizottság arra irányuló terveit, hogy a tagállami – többek között nemzetbiztonsági – hatáskörök sérelme nélkül következetes szabályokat dolgozzon ki a piaci szereplőkre vonatkozóan, valamint előmozdítsa a veszélyekkel, illetve a biztonsági eseményekkel kapcsolatos biztonságos, megbízható és megfelelő információmegosztást – többek között a hálózati és információs rendszerek biztonságáról szóló irányelv (a kiberbiztonsági irányelv) felülvizsgálata révén –, valamint hogy feltérképezze a kibernetizáció további erősítésének lehetőségeit és a kibertámadások, különösen az alapvető gazdasági és társadalmi tevékenységeket érintő támadások esetén alkalmazható hatékonyabb válaszingedményeket”.⁴ Ezenkívül a javasolt jogi aktus nem érinti az Európai Unió működéséről szóló szerződésben (EUMSZ) megállapított versenyszabályok alkalmazását.

Tekintettel arra, hogy a kiberbiztonsági fenyegetések jelentős része az EU-n kívülről származik, a nemzetközi együttműködéshez koherens megközelítésre van szükség. Ez az irányelv egy referenciamodell, amelyet elő kell mozdítani az EU harmadik országokkal folytatott együttműködésében, különösen a külső technikai segítségnyújtás során.

2. JOGALAP, SZUBSZIDIARITÁS ÉS ARÁNYOSSÁG

- **Jogalap**

A kiberbiztonsági irányelv jogalapja az Európai Unió működéséről szóló szerződés 114. cikke, amelynek célja a belső piac létrehozása és működése a nemzeti szabályok közelítésére irányuló intézkedések fokozásával. Amint azt az Európai Unió Bírósága a C-58/08. sz., Vodafone és társai ügyben hozott ítéletében megállapította, az EUMSZ 114. cikkének igénybevétele akkor indokolt, ha vannak nemzeti szabályok közötti olyan eltérések, amelyek közvetlen hatással vannak a belső piac működésére. Ugyanígy a Bíróság úgy ítélte meg, hogy amennyiben az EUMSZ 114. cikkén alapuló jogi aktus már megszüntette a kereskedelem minden akadályát az általa harmonizált területen, az uniós jogalkotótól nem tagadható meg annak lehetősége, hogy az aktust a körülmények változásaihoz vagy az ismeretek fejlődéséhez igazítsa, tekintettel a Szerződés által elismert általános érdekek védelmének feladatára. Végül a Bíróság úgy ítélte meg, hogy az EUMSZ 114. cikkének hatálya alá tartozó közelítéssel kapcsolatos intézkedések célja – a harmonizálandó kérdés általános kontextusától és sajátos körülményeitől függően – mérlegelési mozgástér biztosítása, a kívánt eredmény elérése szempontjából legmegfelelőbb közelítési módszert illetően. A javasolt jogi aktus eltávolítaná

² COM(2020) 67 final.

³ https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_HU.html

⁴ <https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/hu/pdf>

az akadályokat és javítaná a belső piac létrehozását és működését az alapvető és fontos szervezetek számára azáltal, hogy egyértelmű, általánosan alkalmazandó szabályok meghatározása a kiberbiztonsági irányelv alkalmazási körére, a kiberbiztonsági kockázatkezelés és az események bejelentése területén alkalmazandó szabályok harmonizálása. Az ezen a területen jelenleg meglévő egyenlőtlenségek mind jogszabályi, mind felügyeleti szinten, illetőleg nemzeti és uniós szinten akadályokat képeznek a belső piac előtt, mivel a határokon átnyúló tevékenységet folytató szervezetek eltérő és esetlegesen átfedő szabályozási követelményekkel és/vagy azok alkalmazásával szembesülnek, a letelepedési és szolgáltatásnyújtási szabadságuk gyakorlása kárára. Az eltérő szabályok negatív hatással vannak a belső piaci verseny feltételeire is, ha különböző tagállamokban működő, azonos típusú szervezetekről van szó.

- **Szubszidiaritás (nem kizárólagos hatáskör esetén)**

A kiberreziliencia nem lehet tényleges az Unió egészében, ha azt nemzeti vagy regionális adatsílokon keresztül eltérő módon közelítik meg. A kiberbiztonsági irányelv részben orvosolta ezt a hiányosságot azzal, hogy nemzeti és uniós szinten meghatározta a hálózati és információs rendszerek biztonsági kereteit. Átültetése és végrehajtása azonban rávilágított bizonyos rendelkezések vagy megközelítések eredendő hiányosságaira és korlátaira, például az irányelv hatályának homályos körülhatárolására, amely jelentős különbségekhez vezetett tagállami szinten a tényleges uniós beavatkozás mértéke és mélysége között. Ezenkívül a Covid19-válság óta az európai gazdaság minden eddigénél jobban függ a hálózati és információs rendszerektől, és az ágazatok és a szolgáltatások egyre inkább összekapcsolódnak. A kiberbiztonsági irányelv jelenlegi intézkedésein túlmutató uniós beavatkozást elsősorban a következők indokolják: i. a kiberbiztonsággal kapcsolatos fenyegetések és kihívások fokozódó mértékben határokon átnyúlóbb jellege; ii. az uniós fellépés lehetőségei a hatékony és összehangolt nemzeti politikák javítása és megkönnyítése végett; és iii. összehangolt és együttműködő politikai fellépések szerepe az adatvédelemben és a magánélet hatékony védelmében.

- **Arányosság**

Az ezen irányelvben javasolt szabályok nem lépik túl a konkrét célok kielégítő eléréséhez szükséges mértéket. A biztonsági intézkedések és a jelentéstételi kötelezettségek tervezett összehangolása és korszerűsítése a tagállamok és a vállalkozások jelenlegi keret javítására vonatkozó kéréseihez kapcsolódik.

A javaslat figyelembe veszi a tagállamokban már létező gyakorlatokat. Az említett korszerűsített és összehangolt követelmények révén elért magasabb szintű védelem arányos az egyre nagyobb kockázatokkal, beleértve a határokon átnyúló elemet mutató kockázatokat is; ezek észszerűek, és általában megfelelnek az érintett szervezetek szolgáltatásaik folyamatosságának és minőségének biztosításához fűződő érdekeinek. A tagállamok közötti módszeres együttműködés biztosításának költségei alacsonyak lennének a kiberbiztonsági események által okozott gazdasági és társadalmi veszteségekhez és károkhoz képest. Ezenkívül az érdekelt felekkel folytatott konzultációk a kiberbiztonsági irányelv felülvizsgálata kapcsán – beleértve a nyílt nyilvános konzultációk és célzott felmérések eredményeit – a kiberbiztonsági irányelv fent említett irányú felülvizsgálatának támogatottságát jelzik.

- **A jogi aktus típusának megválasztása**

A javaslat tovább egyszerűsíti a vállalkozásokra rótt kötelezettségeket, és biztosítja azok magasabb szintű harmonizációját. Ugyanakkor a javaslat célja a tagállamok számára a nemzeti sajátosságok figyelembevételéhez szükséges rugalmasság biztosítása (például a jogi aktus által meghatározott alapforgatókönyvön túli további alapvető vagy fontos szervezetek azonosításának lehetősége). A jövőbeni jogi eszköznek ezért irányelvnek kell lennie, mivel ez a jogi eszköz lehetővé teszi a célzottabb harmonizációt, valamint az illetékes hatóságok számára bizonyos fokú rugalmasságot.

3. AZ UTÓLAGOS ÉRTÉKELÉSEK, AZ ÉRDEKELT FELEKKEL FOLYTATOTT KONZULTÁCIÓK ÉS A HATÁSVIZSGÁLATOK EREDMÉNYEI

- **A jelenleg hatályban lévő jogszabályok utólagos értékelése/célravezetőségi vizsgálata**

A Bizottság elvégezte a kiberbiztonsági irányelv működésének értékelését.⁵ Elemezte relevanciáját, uniós hozzáadott értékét, koherenciáját, eredményességét és hatékonyságát. Az elemzés fő megállapításai a következők:

- a kiberbiztonsági irányelv hatálya az érintett ágazatok tekintetében túl korlátozott, elsősorban a következők miatt: i. az utóbbi években megnövekedett digitalizálás és magasabb szintű összekapcsoltság; ii. a kiberbiztonsági irányelv már nem tükrözi a gazdaság és a társadalom egésze számára kulcsfontosságú szolgáltatásokat nyújtó összes digitalizált ágazatot.
- A kiberbiztonsági irányelv nem elég egyértelmű az alapvető szolgáltatásokat nyújtó szereplők körét illetően, és rendelkezései nem nyújtanak kellő egyértelműséget a digitális szolgáltatók feletti nemzeti hatáskörrel kapcsolatban. Ez olyan helyzethez vezetett, amelyben bizonyos típusú szervezeteket nem azonosítottak minden tagállamban, ezért nem kötelesek biztonsági intézkedéseket bevezetni és az eseményeket jelenteni.
- A kiberbiztonsági irányelv tág mérlegelési mozgásteret engedett a tagállamoknak az alapvető szolgáltatásokat nyújtó szereplőkre vonatkozó biztonsági és eseményjelentési követelmények megállapításakor. Az értékelés azt mutatja, hogy egyes esetekben a tagállamok ezeket a követelményeket jelentősen eltérő módon hajtották végre, további terheket róva a több tagállamban működő vállalatokra.
- A kiberbiztonsági irányelv felügyeleti és végrehajtási rendszere hatástalan. Például: a tagállamok erősen vonakodnak szankciók alkalmazásától azon szervezetek esetében, amelyek nem vezetnek be biztonsági követelményeket vagy nem jelentik az eseményeket. Ennek negatív következményei lehetnek az egyes szervezetek kiberrezilienciájára.
- A tagállamok által feladataik ellátására elkülönített pénzügyi és emberi erőforrások (például az alapvető szolgáltatások üzemeltetőinek azonosítása vagy felügyelete), és következésképpen a kiberbiztonsági kockázatok kezelésének különböző érettségi szintjei nagyon eltérőek. Ez tovább súlyosbítja a kiberreziliencia terén a tagállamok között fennálló különbségeket.

⁵ [A hatásvizsgálat 5. melléklete].

- A tagállamok nem osztják meg rendszeresen az információkat egymással, ennek negatív következményei vannak, különösen a kiberbiztonsági intézkedések hatékonyságára és az uniós szintű közös helyzetismeret szintjére nézve. Ez vonatkozik a magánvállalkozások közötti információmegosztásra, valamint az uniós szintű együttműködési struktúrák és a magánvállalkozások közötti együttműködésre is.

- **Az érdekelt felekkel folytatott konzultációk**

A Bizottság az érdekelt felek széles körével konzultált. A tagállamokat és az érdekelt feleket felkérték, hogy vegyenek részt a nyílt nyilvános konzultációban, valamint a Wavestone, a CEPS és az ICF – amelyeket a Bizottság a kiberbiztonsági irányelv felülvizsgálatát támogató tanulmány elkészítésével megbízott – által szervezett felméréseken és műhelytalálkozókon. A konzultációban részt vett érintettek között voltak illetékes hatóságok, kiberbiztonsággal foglalkozó uniós szervek, alapvető szolgáltatásokat nyújtó szereplők, digitális szolgáltatók, a jelenlegi kiberbiztonsági irányelv hatályán kívül eső szolgáltatásokat nyújtó szervezetek, szakmai szövetségek és fogyasztói szervezetek, valamint állampolgárok.

Ezenkívül a Bizottság állandó kapcsolatban állt a kiberbiztonsági irányelv végrehajtásáért felelős illetékes hatóságokkal. Az együttműködési csoport intenzíven foglalkozott a különböző horizontális és ágazati megvalósítási szempontokkal. Végül a hálózati és információs rendszerek biztonságáról szóló irányelv 2019-es és 2020-as országlátogatásai során a Bizottság 154 állami és magánvállalkozást, valamint 117 illetékes hatóságot hallgatott meg.

- **Szakértői vélemények beszerzése és felhasználása**

A Bizottság a Wavestone, a CEPS és az ICF konzorciumával szerződött a Bizottság kiberbiztonsági irányelv felülvizsgálatában való támogatására.⁶ A vállalkozó nem csak célzott felmérések és műhelytalálkozók útján kereste meg a kiberbiztonsági irányelv közvetlen érintettjeit, hanem a kiberbiztonsági terület számos szakértőjével is konzultált, például kiberbiztonsági kutatókkal és kiberbiztonsági iparági szakemberekkel.

- **Hatásvizsgálat**

Ezt a javaslatot hatásvizsgálat kíséri⁷, amelyet 2020. október 23-án nyújtottak be a Szabályozási Ellenőrzési Testülethez (RSB), és az RSB észrevételeivel 2020. november 20-án pozitív véleményt kapott. Az RSB bizonyos területeken javításokat javasolt a következők érdekében: (1) a javaslat jobban tükrözze a nemzetközi tovaggyűrés szerepét a problémaelemzésben; (2) jobban fejtsse ki, mi lesz a kezdeményezés sikere; (3) indokolja részletesebben a szakpolitikai alternatívák listáját; (4) dolgozza ki részletesebben a javasolt intézkedések költségeit. A hatásvizsgálatot e pontok, valamint az RSB részletesebb észrevételeinek figyelembevétele érdekében kiigazították. A vizsgálat most részletesebb magyarázatokat tartalmaz a nemzetközi tovaggyűrés kiberbiztonság területén betöltött szerepéről, világosabb áttekintést nyújt a siker mérésének módjáról, részletesebb magyarázatot ad az ezekben az alternatívákban figyelembe vett különböző szakpolitikai

⁶ Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) [Tanulmány a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 irányelv (a kiberbiztonsági irányelv) felülvizsgálatának támogatására] – 2020-665. Wavestone, CEPS és ICF.

⁷ [A végleges dokumentumra és az összefoglaló lapra mutató linkek beillesztendők.]

alternatívák és cselekvések felépítéséről és logikájáról, a kiberbiztonsági irányelv ágazati hatálya kapcsán elemzett szempontokról részletesebb magyarázatot nyújt és a költségeket tovább pontosítja.

A Bizottság számos szakpolitikai alternatívát mérlegelt a kiberreziliencia és az események elhárítása területén a jogszabályi keret javítására:

- „Intézkedés mellőzése”: a kiberbiztonsági irányelv változatlan marad, és a nem jogalkotási jellegű intézkedéseken kívül a kiberbiztonsági irányelv értékelésével azonosított problémák kezelésére más intézkedés nem kerül elfogadásra.
- 1. szakpolitikai alternatíva: Jogalkotási szinten nem történne változás. Ehelyett a Bizottság ajánlásokat és iránymutatásokat adna ki (például az alapvető szolgáltatásokat nyújtó szereplők azonosítására, a biztonsági követelményekre, az események bejelentési eljárásaira és a felügyeletre vonatkozóan), konzultálva az együttműködési csoporttal, az EU Kiberbiztonsági Ügynökségével (ENISA), és adott esetben a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) hálózata.
- 2. szakpolitikai alternatíva: Ez a lehetőség a kiberbiztonsági irányelv célzott módosításával jár, beleértve a hatály kiterjesztését és számos más azt célzó módosítást, hogy az azonosított problémákra garantáltan szülessenek bizonyos azonnali megoldások, nagyobb egyértelműség és további harmonizáció valósuljon meg (például az azonosítási küszöbök harmonizálását célzó rendelkezések). A módosított kiberbiztonsági irányelv azonban fenntartaná a fő építőelemeket, a megközelítést és célokat.
- 3. szakpolitikai alternatíva: Ez a forgatókönyv a kiberbiztonsági irányelv rendszerszintű és strukturális változásait vonja maga után (egy új irányelv révén), alapvetőbb szemléletváltást irányozva elő az Unió egész területén a gazdaságok szélesebb körének lefedése felé, ugyanakkor nagyobb és kulcsfontosságú szereplőket megcélzó, koncentráltabb felügyelet mellett. Ez egyszerűsítene a vállalkozásokra rótt kötelezettségeket, és biztosítaná azok magasabb szintű harmonizációját, hatékonyabb környezetet teremtené az operatív szempontok számára, valamint egyértelmű alapot teremtené a különböző érdekelték nagyobb megosztott felelősségéhez és elszámoltathatóságához a kiberbiztonsági intézkedésekkel kapcsolatban.

A hatásvizsgálat arra a következtetésre jut, hogy az előnyben részesített alternatíva a 3. lehetőség (azaz a kiberbiztonsági irányelv keretének rendszerszintű és strukturális változásai). A hatékonyság szempontjából az előnyben részesített alternatíva egyértelműen meghatározná a kiberbiztonsági irányelv alkalmazási körét, kiterjesztve azt az uniós gazdaságok és társadalmak reprezentatívabb hányadára, és a követelményeket egyszerűsítene, a felügyelet és a végrehajtás egyértelműbb keretei mellett, amelynek célja a megfelelés szintjének növelése. Olyan intézkedéseket is magában foglal, amelyek célja a szakpolitika-kialakítás tagállami szintű megközelítéseinek fejlesztése és paradigmájának megváltoztatása, a szállítói kapcsolatok kockázatkezelése új keretrendszerének népszerűsítése és a biztonsági részek összehangolt közzététele. Ugyanakkor az előnyben részesített szakpolitikai alternatíva egyértelmű alapot teremt a megosztott felelősség és elszámoltathatóság számára, és olyan mechanizmusokat irányoz elő, amelyek célja a tagállamok, a hatóságok és az ipar közötti bizalom fokozása, az információmegosztás ösztönzése és az operatívabb megközelítés – például a kölcsönös segítségnyújtás, valamint a szakértői értékelési mechanizmusok – biztosítása. Ez az alternatíva az Unió válságkezelési keretrendszerét is létrehozná, amely a nemrégiben elindított uniós operatív hálózatra épülne, és biztosítaná az ENISA jelenlegi

megbízásán belüli nagyobb részvételét az Unió kiberbiztonsági helyzetének pontos áttekintésében.

A hatékonyság szempontjából, bár az előnyben részesített alternatíva további megfelelési és végrehajtási költségeket jelentene a vállalkozások és a tagállamok számára, hatékony kompromisszumokat és szinergiákat is eredményezne, az elemzett szakpolitikai alternatívák közül adja a lehető legjobb esélyt az egész Unióban a kulcsfontosságú szervezetek fokozott és következetes kiberrezilienciájának biztosítására, ami végül költségmegtakarítást eredményezne a vállalkozások és a társadalom számára egyaránt. Ez a szakpolitikai alternatíva bizonyos további adminisztratív terheket és megfelelési költségeket jelentene a tagállami hatóságok számára. Összességében azonban közép- és hosszú távon jelentős előnyökkel járna a tagállamok közötti fokozott együttműködés révén, többek között operatív szinten is, valamint ösztönözné a kölcsönös segítségnyújtást, a szakértői értékelési mechanizmusokat, valamint a kulcsfontosságú szervezetek jobb áttekintését és a velük való együttműködést, a kiberbiztonsági képességeket általánosan növelve nemzeti és regionális szinten. Az előnyben részesített szakpolitikai alternatíva nagyban biztosítaná a koherenciát más jogszabályokkal, kezdeményezésekkel vagy szakpolitikai intézkedésekkel is, beleértve az ágazatspecifikus *lex specialis* jellegűeket is.

A kiberbiztonsági készség tagállami szintű, jelenleg is fennálló elégtelenségének kezelése hatékonyságnövelést és a kiberbiztonsági eseményekből eredő többletköltségek csökkenését eredményezheti.

- Az alapvető és fontos szervezetek esetében a kiberbiztonsági felkészültség szintjének növelése enyhítheti a zavarok – ideértve az ipari kémkedést is – miatti esetleges bevételkiesést, és csökkentheti az eseti fenyegetések mérséklésének jelentős költségeit. Az említett nyereség valószínűleg meghaladja a szükséges beruházási költségeket. A belső piac szétagoltságának csökkentése szintén javítaná a szereplők közötti egyenlő versenyfeltételeket.
- A tagállamok számára ez tovább csökkentheti az ad hoc fenyegetések mérséklésével járó növekvő költségvetési kiadások és a kiberbiztonsági eseményekhez kapcsolódó vészhelyzetek esetén felmerülő további költségek kockázatát.
- A polgárok számára a kiberbiztonsági események kezelése várhatóan csökkenti a gazdasági zavarok miatti jövedelemkiesést.

A kiberbiztonság megnövekedett szintje a tagállamokban, valamint a vállalatok és hatóságok azon képessége, hogy gyorsan reagáljanak egy eseményre és mérsékeljék annak hatásait, nagy valószínűséggel a polgárok digitális gazdaságba vetett általános bizalmának növekedését eredményezi, amelynek pozitív hatása lehet a növekedésre és a beruházásokra.

A kiberbiztonság általános szintjének növelése valószínűleg megnövekedett általános biztonsághoz és a társadalom számára kritikus alapvető szolgáltatások zavartalan, folyamatos működéséhez is elvezet. A kezdeményezés hozzájárulhat más társadalmi hatásokhoz is, például a számítógépes bűnözés és a terrorizmus csökkenéséhez, valamint az erősebb polgári védelemhez. A kibernetikai felkészültség növelése a vállalkozások és más szervezetek számára megelőzheti a kibertámadásokból eredő esetleges pénzügyi veszteségeket, így kiiktatva a munkavállalók elbocsátásának szükségességét.

A kiberbiztonság általános szintjének növelése a környezeti kockázatok/károk megelőzését is eredményezheti egy alapvető szolgáltatás elleni támadás esetén. Ez különösen érvényes lehet az energia, a vízellátás és az elosztás, illetve a közlekedési ágazatok területén. A kiberbiztonsági képességek megerősítésével a kezdeményezés a környezetvédelmi

szempontból is fenntarthatóbb, legújabb generációs IKT-infrastruktúrák és -szolgáltatások fokozottabb kihasználásához vezethet, a nem hatékony és kevésbé biztonságos örökségi infrastruktúrák cseréje mellett. Ez várhatóan hozzájárul a költséges kiberbiztonsági események számának csökkenéséhez, felszabadítva fenntartható beruházásokhoz elérhető forrásokat.

- **Célravezető szabályozás és egyszerűsítés**

A javaslat a mikro- és kisvállalkozások kiberbiztonsági irányelv hatálya alóli általános kizárását írja elő és egy könnyebb *utólagos* felügyeleti rendszert alkalmaz a felülvizsgált hatály alá újonnan bekerülő szervezetek nagy részére (az úgynevezett fontos szervezetekre). Ezen intézkedések célja a vállalatokra és a közigazgatásra nehezedő terhek legkisebbre csökkentése és kiegyensúlyozása. Ezenkívül a javaslat felváltja az alapvető szolgáltatásokat nyújtó szereplők összetett azonosítási rendszerét egy általánosan alkalmazandó kötelezettséggel, és magasabb szintű harmonizációt vezet be a biztonsági és jelentési kötelezettségek terén, ami csökkentené a megfelelés terheit, különösen a határokon átnyúló szolgáltatásokat nyújtó szervezetek számára.

A javaslat minimalizálja a kkv-k megfelelési költségeit, mivel a szervezeteknek csak azokat az intézkedéseket kell megtenniük, amelyek szükségesek a hálózati és információs rendszerek jelen lévő kockázatnak megfelelő biztonsági szintjének biztosításához.

- **Alapjogok**

Az EU elkötelezett az alapvető jogok magas szintű védelmének biztosítása mellett. A szervezetek közötti minden önkéntes információmegosztási konstrukció – amelyet ez az irányelv támogat, megbízható környezetben működne, teljes mértékben tiszteletben tartva az uniós adatvédelmi szabályokat, nevezetesen az (EU) 2016/679 európai parlamenti és tanácsi rendeletet⁸.

4. KÖLTSÉGVETÉSI VONZATOK

Lásd a pénzügyi adatlapot

5. EGYÉB ELEMEK

- **Végrehajtási tervek, valamint a nyomon követés, az értékelés és a jelentéstétel szabályai**

A javaslat tartalmaz egy általános tervet a konkrét célkitűzésekre gyakorolt hatás nyomon követésére és értékelésére, amely előírja a Bizottság számára, hogy a hatálybalépést követően legalább [54 hónappal] végezzen felülvizsgálatot, és tegyen jelentést az Európai Parlamentnek és a Tanácsnak a fő megállapításairól.

A felülvizsgálatot a Bizottság minőségi jogalkotásra vonatkozó iránymutatásainak megfelelően kell lefolytatni.

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.).

- **A javaslat egyes rendelkezéseinek részletes magyarázata**

A javaslat több fő szakpolitikai terület köré épül, amelyek összefüggenek egymással, és azt a célt szolgálja, hogy növelje az Unióban a kiberbiztonság szintjét.

Tárgy és hatály (1. cikk és 2. cikk)

Az irányelv különösen: a) előír kötelezettségeket a tagállamok számára a nemzeti kiberbiztonsági stratégia elfogadására, az illetékes nemzeti hatóságok, az egyedüli kapcsolattartó pontok és a CSIRT-ek kijelölésére vonatkozóan; b) előírja, hogy a tagállamoknak kiberbiztonsági kockázatkezelési és jelentéstételi kötelezettségeket kell megállapítaniuk az I. mellékletben említett alapvető szervezetek és a II. mellékletben említett fontos szervezetek számára; c) előírja, hogy a tagállamok határozzanak meg kiberbiztonsági információk megosztására vonatkozó kötelezettségeket.

Az irányelv az I. mellékletben felsorolt ágazatokban (energia; szállítás; banki szolgáltatások; pénzügyi piaci infrastruktúrák; egészségügy, ivóvíz; szennyvíz; digitális infrastruktúra; közigazgatás és úrkutatás) működő egyes alapvető állami és magánszervezetekre, valamint a II. mellékletben felsorolt ágazatokban (postai és futárszolgálatok; hulladékgazdálkodás; vegyi anyagok gyártása, előállítása és forgalmazása; élelmiszer-előállítás, -feldolgozás és -forgalmazás; gyártás és digitális szolgáltatók) ágazatokban tevékenykedő, egyes fontos állami és magánszervezetekre vonatkozik. A 2003. május 6-i 2003/361/EK bizottsági ajánlás értelmében vett mikro- és kisvállalkozások nem tartoznak az irányelv hatálya alá, kivéve az elektronikus hírközlő hálózatok vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatások szolgáltatóit, a megbízható szolgáltatókat, a legfelső szintű doménnev-nyilvántartókat és közhiteles nyilvántartását vezetőket, valamint bizonyos egyéb szervezeteket, például egy tagállamban a szolgáltatás egyedüli szolgáltatóját.

Nemzeti kiberbiztonsági keretek (5–11. cikk)

A tagállamoknak nemzeti kiberbiztonsági stratégiát kell elfogadniuk, amely meghatározza a stratégiai célokat, valamint a megfelelő politikai és szabályozási intézkedéseket a magas szintű kiberbiztonság elérése és fenntartása céljából.

Az irányelv keretet hoz létre a biztonsági rések összehangolt közzétételére is, és előírja a tagállamoknak, hogy jelöljenek ki CSIRT-eket megbízható közvetítőként történő eljárásra, és az adatszolgáltató szervezetek és az IKT-termékek és IKT-szolgáltatások gyártói vagy szolgáltatói közötti interakció megkönnyítésére. Az ENISA-nak ki kell fejlesztenie és fenn kell tartania egy európai biztonságírás-nyilvántartást a felfedezett biztonsági rések vonatkozásában.

A tagállamok kötelesek létrehozni a nemzeti kiberbiztonsági válságkezelési kereteket, többek között a nagyszabású kiberbiztonsági események és válságok kezeléséért felelős nemzeti illetékes hatóságok kijelölésével.

A tagállamoknak egy vagy több nemzeti kiberbiztonsági hatóságot is ki kell jelölniük az ezen irányelv szerinti felügyeleti feladatok ellátására, valamint egy nemzeti kiberbiztonsági kapcsolattartó pontot (SPOC), amely kapcsolattartó funkciót lát el a tagállami hatóságok határokon átnyúló együttműködésének biztosítása érdekében. A tagállamoknak ki kell jelölniük CSIRT-eket is.

Együttműködés (12–16. cikk)

Az irányelv létrehoz egy együttműködési csoportot a stratégiai együttműködés és a tagállamok közötti információmegosztás támogatása és megkönnyítése, valamint a bizalom erősítése érdekében. Ezenkívül létrehoz egy CSIRT-hálózatot, hogy hozzájáruljon a tagállamok közötti bizalom kialakulásához, és elősegítse a gyors és hatékony operatív együttműködést.

Létrehozza az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (EU-CyCLONe), hogy támogassa a nagyszabású kiberbiztonsági események és válságok összehangolt kezelését, és biztosítsa a tagállamok és az uniós intézmények közötti rendszeres információmegosztást.

Az ENISA-nak a Bizottsággal együttműködve két évente jelentést kell kiadnia az Unió kiberbiztonsági helyzetéről.

A Bizottságnak létre kell hoznia egy szakértői értékelési rendszert, amely lehetővé teszi a kiberbiztonsági szakpolitikák tagállami eredményességének rendszeres szakértői értékelését.

Kiberbiztonsági kockázatkezelési és jelentéstételi kötelezettségek (17–23. cikk)

Az irányelv előírja a tagállamoknak, hogy rendelkezzenek arról, hogy a hatálya alá tartozó valamennyi szervezet vezető testületei hagyják jóvá az érintett szervezetek által hozott kiberbiztonsági kockázatkezelési intézkedéseket, és kövessék a kiberbiztonsággal kapcsolatos speciális képzést.

A tagállamoknak biztosítaniuk kell, hogy az irányelv hatálya alá tartozó szervezetek megfelelő és arányos technikai és szervezési intézkedéseket hozzanak a hálózati és információs rendszerek biztonsága által keltett kiberbiztonsági kockázatok kezelésére. Arról is gondoskodniuk kell, hogy a szervezetek értesítsék az illetékes nemzeti hatóságokat vagy a CSIRT-eket minden olyan kiberbiztonsági eseményről, amely jelentős hatással van az általuk nyújtott szolgáltatás biztosítására.

A legfelső szintű doménnév-nyilvántartók és a legfelső szintű domén (TLD) vonatkozásában doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek pontos és teljes doménnév-nyilvántartási adatokat gyűjtenek és vezetnek. Ezenkívül az említett szervezeteknek hatékony hozzáférést kell biztosítaniuk a doménnyilvántartás adataihoz a jogosult hozzáférés-igénylők számára.

Joghatóság és nyilvántartásba vétel (24. és 25. cikk)

Alapvető fontosságú, hogy az alapvető és fontos szervezetek annak a tagállamnak a joghatósága alá tartozónak minősüljenek, ahol szolgáltatásaikat nyújtják. Bizonyos típusú szervezetek (DNS-szolgáltatók, legfelső szintű doménnév-nyilvántartók, felhőszolgáltatók, adatközpont-szolgáltatók és tartalomszolgáltató hálózati szolgáltatók, valamint bizonyos digitális szolgáltatók) azonban annak a tagállamnak a joghatósága alá tartoznak, amelyben üzleti tevékenység fő helye az Unióban van. Ennek célja annak biztosítása, hogy az említett szervezetek ne szembesüljenek eltérő jogszabályi követelményekkel, mivel különösen nagy mértékben nyújtanak határokon átnyúlóan szolgáltatásokat. Az ENISA-nak kell létrehoznia és vezetnie az utóbbi típusú szervezetek nyilvántartását.

Információmegosztás (26. és 27. cikk)

A tagállamok olyan szabályokat határoznak meg, amelyek lehetővé teszik a szervezetek számára, hogy az EUMSZ 101. cikkével összhangban konkrét kiberbiztonsági információmegosztási megállapodások keretében vegyenek részt a kiberbiztonsággal kapcsolatos információk megosztásában. Ezenkívül a tagállamok lehetővé teszik az ezen irányelv hatályán kívül eső szervezetek számára, hogy önkéntes alapon jelentést tegyenek jelentős eseményekről, kiberfenyegetésekről vagy majdnem bekövetkezett (near miss) eseményekről.

Felügyelet és végrehajtás (28–34. cikk)

Az illetékes hatóságok kötelesek felügyelni az irányelv hatálya alá tartozó szervezeteket, különös tekintettel annak biztosítására, hogy megfeleljenek a biztonsági és eseménybejelentési követelményeknek. Megkülönbözteti az alapvető szervezetekre vonatkozó előzetes felügyeleti rendszert és a fontos szervezetekre vonatkozó utólagos felügyeleti rendszert, amely utóbbi azt igényli az illetékes hatóságoktól, hogy tegyenek lépéseket, ha bizonyítékokat vagy jelzést kapnak arról, hogy egy fontos szervezet nem felel meg a biztonsági és eseménybejelentési követelményeknek.

Az irányelv azt is előírja a tagállamoknak, hogy adminisztratív bírságokat szabjanak ki az alapvető és fontos szervezetek számára, és meghatározza a bírságok maximális értékét.

A tagállamoknak szükség szerint együtt kell működniük és segíteniük kell egymást, ha a szervezetek több tagállamban nyújtanak szolgáltatást, vagy ha a szervezet üzleti tevékenységének fő helye vagy képviselője egy adott tagállamban található, de hálózata és információs rendszerei egy vagy több más tagállamban találhatók.

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE

**az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről,
valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről**

(EGT-vonatkozású szöveg)

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,
tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 114. cikkére,
tekintettel az Európai Bizottság javaslatára,
a jogalkotási aktus tervezetének a nemzeti parlamenteknek való megküldését követően,
tekintettel az Európai Gazdasági és Szociális Bizottság véleményére⁹,
tekintettel a Régiók Bizottságának véleményére¹⁰,
rendes jogalkotási eljárás keretében,
mivel:

- (1) Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve¹¹ célja a kiberbiztonsági képességek egész Unióban történő kiépítése, a kulcsfontosságú ágazatokban az alapvető szolgáltatások nyújtására használt hálózati és információs rendszerek fenyegetéseinek enyhítése és az említett szolgáltatások folyamatosságának biztosítása a kiberbiztonsági események során, hozzájárulva ezzel az Unió gazdaságának és társadalmának hatékony működéséhez.
- (2) Az (EU) 2016/1148 irányelv hatálybalépése óta jelentős előrelépés történt az Unió kiberrezilienciájának növelése terén. Az irányelv felülvizsgálata megmutatta, hogy katalizátorként szolgált az uniós kiberbiztonság intézményi és szabályozási megközelítésében, utat nyitva a gondolkodásmód jelentős változásának. Ez az irányelv a nemzeti kiberbiztonsági stratégiák meghatározásával, a nemzeti képességek kialakításával és az egyes tagállamok által azonosított alapvető infrastruktúrákra és szereplőkre vonatkozó szabályozási intézkedések végrehajtásával biztosította a nemzeti keretek kiteljesedését. Az együttműködési csoport¹², valamint a nemzeti számítógép-biztonsági eseményekre reagáló csoportok hálózata („CSIRT-hálózat”)¹³ létrehozásával hozzájárult az uniós szintű együttműködéshez is. Ezen eredmények ellenére az (EU) 2016/1148 irányelv felülvizsgálata olyan hiányosságokat

⁹ HL C [...], [...], [...] o.

¹⁰ HL C [...], [...], [...] o.

¹¹ 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 194/1., 2016.7.19., 1. o.).

¹² Az (EU) 2016/1148 irányelv 11. cikke.

¹³ Az (EU) 2016/1148 irányelv 12. cikke.

tárt fel, amelyek megakadályozzák, hogy eredményesen kezelje az aktuális és 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 kiberbiztonsági fenyegetettség bővüléséhez vezetett, új kihívások támasztásával, amelyek minden tagállamban kiigazított, összehangolt és innovatív reagálást igényelnek. A kiberbiztonsági események száma, nagysága, kifinomultsága, gyakorisága és hatása növekszik, és komoly veszélyt jelentenek a hálózati és információs rendszerek működésére. Ennek következtében a kiberbiztonsági események akadályozhatják a belső piaci gazdasági tevékenységek folytatását, pénzügyi veszteségeket okozhatnak, alááshatják a felhasználók bizalmát, és jelentős károkat okozhatnak az Unió gazdaságában és a társadalmában. A kiberbiztonsági felkészültség és hatásosság ezért minden eddiginél elengedhetlenebb a belső piac megfelelő működéséhez.
- (4) Az 1148/2016/EU irányelv jogalapja az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikke volt, amelynek célja a belső piac létrehozása és működése a nemzeti szabályok közelítésére irányuló intézkedések fokozásával. A szolgáltatásokat nyújtó vagy gazdaságilag releváns tevékenységeket végző szervezetekre előírt kiberbiztonsági követelmények jelentősen eltérnek a tagállamokban a követelmények típusa, részletessége szintje és a felügyelet módja tekintetében. Ezek az eltérések többletköltségekkel járnak és nehézségeket okoznak a határokon átnyúló viszonylatban árukat vagy szolgáltatásokat kínáló vállalkozások számára. Az egyik tagállam által előírt, a másik tagállam által előírtaktól eltérő vagy akár azoknak ellentmondó követelmények jelentősen befolyásolhatják ezeket a határokon átnyúló tevékenységeket. Ezenkívül egy tagállamban a kiberbiztonsági előírások nem optimális kialakításának vagy végrehajtásának lehetősége valószínűleg visszahat más tagállamok kiberbiztonsági szintjére, különös tekintettel az intenzív, határokon átnyúló információmegosztásra. Az (EU) 2016/1148 irányelv felülvizsgálata jelentős eltéréseket mutatott a tagállamok általi végrehajtás terén, ideértve a hatállyal kapcsolatban is, amelynek lehatárolása nagyrészt a tagállamok mérlegelési jogkörében maradt. Az (EU) 2016/1148 irányelv szintén nagyon tág mérlegelési mozgásteret biztosított a tagállamoknak az abban meghatározott biztonsági és eseményjelentési kötelezettségek végrehajtása tekintetében. Ezeket a kötelezettségeket tehát nemzeti szinten jelentősen eltérő módon hajtották végre. Hasonló eltérések mutatkoztak a végrehajtásban az irányelv felügyeletre és végrehajtásra vonatkozó rendelkezéseivel kapcsolatban.
- (5) Mindezek az eltérések a belső piac széttöredezettségével járnak, és káros hatással lehetnek annak működésére, különösen az eltérő előírások alkalmazása miatt a határokon átnyúló szolgáltatások nyújtására és a kiberreziliencia szintjére. 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 szankciók biztosításával, amelyek kulcsfontosságúak e kötelezettségek tényleges érvényesítéséhez. Ezért az (EU) 2016/1148 irányelvet hatályon kívül kell helyezni, és azt ez az irányelv váltja fel.
- (6) Ez az irányelv nem érinti a tagállamok azon képességét, hogy meghozzák alapvető biztonsági érdekeik védelme, a közrend és a közbiztonság védelme, valamint a

bűncselekmények kivizsgálásának, felderítésének és üldözésének lehetővé tétele érdekében a szükséges intézkedéseket, az uniós joggal összhangban. Az EUMSZ 346. cikkének megfelelően egyetlen tagállam sem köteles olyan információkat szolgáltatni, amelyek nyilvánosságra hozatala ellentétes lenne alapvető közbiztonsági érdekeivel. Ebben az összefüggésben jelentőséggel bírnak a minősített információk védelmére vonatkozó nemzeti és uniós szabályok, a titoktartási megállapodások és az informális titoktartási megállapodások, például a jelzőlámpás protokoll (TLP)¹⁴.

- (7) Az (EU) 2016/1148 irányelv hatályon kívül helyezésével az ágazati alkalmazási kört ki kell terjeszteni a gazdaság nagyobb részére, a (4)–(6) preambulumbekzdésben foglalt megfontolásokra figyelemmel. Az (EU) 2016/1148 irányelv hatálya alá tartozó ágazatokat ezért ki kell terjeszteni, hogy átfogóan lefedjék azokat az ágazatokat és szolgáltatásokat, amelyek létfontosságúak a belső piacon kulcsfontosságú társadalmi és gazdasági tevékenységek szempontjából. A szabályoknak nem szabad különbözniük aszerint, hogy a szervezetek alapvető szolgáltatásokat nyújtó szereplők vagy digitális szolgáltatók. E megkülönböztetés elavultsága bebizonyosodott, mivel nem tükrözi az ágazatok vagy szolgáltatások tényleges jelentőségét a belső piaci társadalmi és gazdasági tevékenységek szempontjából.
- (8) Az (EU) 2016/1148 irányelvvel összhangban a tagállamok voltak felelősek annak megállapításáért, hogy mely szervezetek felelnek meg az alapvető szolgáltatásokat nyújtó szereplők minősítés kritériumainak („azonosítási folyamat”). A tagállamok között e tekintetben mutatkozó nagy eltérések kiküszöbölése, valamint az összes érintett szervezet vonatkozásában a kockázatkezelési követelmények és a jelentéstételi kötelezettségek tekintetében a jogbiztonság biztosítása érdekében egy olyan egységes kritériumot kell megállapítani, amely meghatározza az ezen irányelv alkalmazásának hatálya alá tartozó szervezeteket. Ennek a kritériumnak tartalmaznia kell a méretkorlát szabály alkalmazását, amelynek során – a 2003/361/EK bizottsági ajánlás¹⁵ meghatározása szerinti – minden olyan közép- és nagyvállalkozás, amely az ezen irányelv hatálya alá tartozó ágazatokban működik vagy az irányelv hatálya alá tartozó típusú szolgáltatásokat nyújt, az irányelv hatálya alá tartoznak. A tagállamoktól nem követelhető meg azon szervezetek listájának létrehozása, amelyek megfelelnek ennek az általánosan alkalmazható, mérethez kapcsolódó kritériumnak.
- (9) Azonban az irányelvnek hatálya alá kell tartozniuk azoknak a kis- vagy mikrovállalkozásoknak is, amelyek megfelelnek azt jelző bizonyos feltételeknek, hogy kulcsfontosságú szerepet töltenek be a tagállamok gazdasága vagy társadalma, illetve bizonyos ágazatok vagy szolgáltatástípusok szempontjából. A tagállamoknak kell felelniük az említett szervezetek listájának elkészítéséért, és azt be kell nyújtaniuk a Bizottsághoz.
- (10) A Bizottság az együttműködési csoporttal együttműködve iránymutatásokat adhat ki a mikro- és kisvállalkozásokra alkalmazandó kritériumok végrehajtásáról.
- (11) Az ezen irányelv hatálya alá tartozó szervezeteket – attól függően, hogy mely ágazatban működnek vagy milyen típusú szolgáltatást nyújtanak – kettő, a nélkülözhetetlen és a fontos kategóriába kell sorolni. A besorolás során figyelembe

¹⁴ A jelzőlámpás protokoll (TLP) arra szolgál, hogy az információkat megosztó személyek tájékoztassák közönségüket az információk további terjesztésének korlátairól. Használják szinte az összes CSIRT-közösségben és néhány információelemző és -megosztó központban (ISAC).

¹⁵ A Bizottság 2003/361/EK ajánlása (2003. május 6.) a mikro-, kis- és középvállalkozások meghatározásáról (HL L 124., 2003.5.20., 36. o.).

kell venni az ágazat vagy a szolgáltatás típusának kritikusságát, valamint az egyéb ágazatok vagy szolgáltatástípusok függőségének szintjét. Mind az alapvető, mind a fontos szervezetekre ugyanazokat a kockázatkezelési követelményeket és jelentési kötelezettségeket kell alkalmazni. A szervezetek e két kategóriája között a felügyeleti és büntetési rendszer tekintetében különbséget kell tenni, hogy biztosítani lehessen az egyensúlyt a követelmények és kötelezettségek, valamint a megfelelés felügyeletéből adódó adminisztratív terhek között.

- (12) Az ágazatspecifikus jogszabályok és eszközök hozzájárulhatnak a magas szintű kiberbiztonság biztosításához, miközben teljes mértékben figyelembe veszik ezen ágazatok sajátosságait és összetettségét. Amennyiben egy ágazatspecifikus uniós jogi aktus előírja az alapvető vagy fontos szervezetek számára, hogy fogadjanak el kiberbiztonsági kockázatkezelési intézkedéseket, vagy jelentsék az eseményeket vagy a jelentős kiberfenyegetéseket, amelyek legalább egyenértékűek az ebben az irányelvben megállapított kötelezettségekkel, akkor ezeket az ágazatspecifikus rendelkezéseket kell alkalmazni, ideértve a felügyeletet és végrehajtást is. A Bizottság iránymutatásokat adhat ki a *lex specialis* végrehajtásával kapcsolatban. Ez az irányelv nem zárja ki a kiberbiztonsági kockázatkezelési intézkedésekkel és az események bejelentésével foglalkozó további ágazatspecifikus uniós jogi aktusok elfogadását. Ez az irányelv nem érinti a Bizottságra számos ágazatban – ideértve a közlekedést és az energiaágazatot is – átruházott, meglévő végrehajtási hatásköröket.
- (13) Az XXXX/XXXX európai parlamenti és tanácsi rendelet¹⁶ ezen irányelv vonatkozásában ágazatspecifikus uniós jogi aktusnak kell tekinteni a pénzügyi ágazat szervezetei tekintetében. Az ezen irányelv alapján létrehozott rendelkezések helyett az XXXX/XXXX rendelet információs és kommunikációs technológiai (IKT) kockázatkezelési intézkedésekre, az IKT-vel kapcsolatos események kezelésére és különösen az események jelentésére, valamint a digitális működési reziliencia tesztekre, az információmegosztási megállapodásokra és a harmadik féllel kapcsolatos IKT-kockázatokra vonatkozó rendelkezéseit kell alkalmazni. A tagállamok ezért nem alkalmazhatják ezen irányelv kiberbiztonsági kockázatkezelési és jelentési kötelezettségekre, információmegosztásra, felügyeletre és végrehajtásra vonatkozó rendelkezéseit a XXXX/XXXX rendelet hatálya alá tartozó pénzügyi szervezetekre. Ugyanakkor fontos, hogy ezen irányelv alapján fennmaradjon a szoros kapcsolat és információmegosztás a pénzügyi ágazattal. Ennek érdekében a XXXX/XXXX rendelet értelmében valamennyi pénzügyi felügyelet, a pénzügyi ágazat európai felügyeleti hatóságai és az illetékes nemzeti hatóságok a XXXX/XXXX rendelet szerint részt vehetnek stratégiai politikai megbeszéléseken és az együttműködési csoport technikai munkájában, valamint információt cserélhetnek és együttműködhetnek az ezen irányelv alapján kijelölt egyedüli kapcsolattartó ponttal és a nemzeti CSIRT-ekkel. A XXXX/XXXX rendelet szerint illetékes hatóságoknak továbbítaniuk kell az IKT-vel kapcsolatos jelentős események részleteit az ezen irányelv alapján kijelölt egyedüli kapcsolattartó pontra is. Ezenkívül a tagállamoknak továbbra is be kell vonniuk a pénzügyi ágazatot kiberbiztonsági stratégiájukba, és a nemzeti CSIRT-ek tevékenységei kiterjedhetnek a pénzügyi ágazatra.
- (14) A kiberbiztonság és a szervezetek fizikai biztonsága közötti összefüggésekre tekintettel koherens megközelítést kell biztosítani az (EU) XXX/XXX európai parlamenti és tanácsi irányelv¹⁷ és ezen irányelv között. Ennek elérése érdekében a

¹⁶ [illessze be a teljes címet és a HL-kiadvány hivatkozását, amikor ismertté válik].

¹⁷ [illessze be a teljes címet és a HL-kiadvány hivatkozását, amikor ismertté válik].

tagállamoknak biztosítaniuk kell, hogy az (EU) XXX/XXX irányelv alapján a kritikus jelentőségű szervezeteket és azokkal egyenértékű szervezeteket ezen irányelv alapján alapvető szervezeteknek tekintsék. A tagállamoknak arról is gondoskodniuk kell, hogy kiberbiztonsági stratégiáik biztosítsanak egy politikai keretet az ezen irányelv és az (EU) XXX/XXX irányelv szerinti illetékes hatóság közötti fokozott koordinációra az eseményekkel és a kiberfenyegetésekkel kapcsolatos információk megosztása és felügyeleti feladatok összefüggésében. A két irányelv szerinti hatóságoknak együtt kell működniük és információt kell cserélniük, különös tekintettel a kritikus szervezetek azonosítására, a kiberfenyegetésekre, a kiberbiztonsági kockázatokra, a kritikus szervezeteket érintő eseményekre, valamint a kritikus szervezetek által végrehajtott kiberbiztonsági intézkedésekre. Az (EU) XXX/XXX irányelv szerinti illetékes hatóságok kérésére az ezen irányelv alapján illetékes hatóságok számára lehetővé kell tenni, hogy felügyeleti és végrehajtási hatáskörüket gyakorolhassák a kritikusnak minősített alapvető szervezeteknél. E célból a két hatóságnak együtt kell működnie és információt kell cserélnie.

- (15) 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 ezt az irányelvet a DNS-feloldási lánc mentén minden DNS-szolgáltatóra alkalmazni kell, ideértve a gyökérnévhez tartozó szerverek üzemeltetőit, a legfelső szintű domén (TLD) névszervereket, a doménnevek hiteles névszervereit és a rekurzív felbontókat.
- (16) A felhőszolgáltatásoknak ki kell terjedniük azokra a szolgáltatásokra, amelyek igény szerinti és széles távoli hozzáférést tesznek lehetővé a megosztható és elosztott számítástechnikai erőforrások méretezhető és rugalmas készletéhez. E 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 telepítési modelljeinek ki kell terjedniük a magán-, a közösségi, a nyilvános és a hibrid felhőre. A fent említett 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 önkiszolgáló 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, munkaállomásokat) használatát elősegítő mechanizmusok révén érik el azokat. 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 számítási 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 számítási 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 számítási erőforrások leírására szolgál, amelyek olyan különböző hálózatba

kötött számítógépeken vagy eszközökön találhatók, amelyek üzenetközvetítéssel kommunikálnak és koordinálják magukat.

- (17) Tekintettel az innovatív technológiák és az új üzleti modellek megjelenésére, várhatóan új felhőalapú számítástechnika telepítési és szolgáltatási modellek jelennek meg a piacon, a változó 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”).
- (18) 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 biztonságára fennálló összes kockázat kezelése érdekében ennek az irányelvnek 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 informatika és hálózati berendezések központosított elhelyezésére, összekapcsolására és működtetésére szolgálnak, a villamosenergia-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.
- (19) A 97/67/EK európai parlamenti és tanácsi irányelv értelmében¹⁸ vett postai szolgáltatóknak, valamint az expressz és futárszállítási szolgáltatóknak ezen irányelv hatálya alá kell tartozniuk, ha a postai kézbesítési lánc legalább egyik lépését biztosítják, különös tekintettel az elszámolásra, a válogatásra vagy a terjesztésre, ideértve az átvételi szolgáltatásokat is. Azoknak a szállítási szolgáltatásoknak, amelyeket nem e lépések egyikével kapcsolatban végeznek, a postai szolgáltatások körén kívül kell esniük.
- (20) 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 az energia-, a közlekedési, a digitális infrastruktúra, az ivóvíz- és szennyvíz-, az egészségügyi ágazatban, a közigazgatás bizonyos vonatkozásaiban, valamint az űrágazatban, amennyiben bizonyos szolgáltatások nyújtása olyan földi infrastruktúráktól függ, amelyek tulajdonosai, kezelői és üzemeltetői tagállamok vagy magánszemélyek, tehát nem tartoznak ide az Unió vagy űrprogramja részeként annak megbízottja tulajdonában lévő, általa kezelt vagy üzemeltetett infrastruktúrák. Ezek az egymásrautaltságok azt jelentik, hogy bármilyen zavar – 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 megmutatta az egyre inkább egymásra utalt társadalmaink sérülékenységet az alacsony valószínűségű kockázatokkal szemben.

¹⁸

Az Európai Parlament és a Tanács 97/67/EK irányelve (1997. december 15.) a közösségi postai szolgáltatások belső piacának fejlesztésére és a szolgáltatás minőségének javítására vonatkozó közös szabályokról (HL L 15., 1998.1.21., 14. o.).

- (21) Figyelemmel a nemzeti irányítási struktúrák közötti különbségekre, és a már meglévő ágazati megállapodások vagy az uniós felügyeleti és szabályozó testületek védelme érdekében a tagállamok több olyan nemzeti illetékes hatóságot jelölhetnek ki, amelyek a hálózat és az ezen irányelv szerinti alapvető és fontos szervezetek információs rendszerei biztonságával kapcsolatos feladatok ellátásáért felelnek. A tagállamok ezt a szerepkört egy meglévő hatóságra bízhatják.
- (22) A határokon átnyúló együttműködés és a hatóságok közötti kommunikáció megkönnyítése és ezen irányelv hatékony végrehajtásának lehetővé tétele érdekében minden tagállamnak ki kell jelölnie egy nemzeti kapcsolattartó pontot, amely felelős a hálózati és információs rendszerek biztonságával kapcsolatos kérdések koordinálásáért és a határokon átnyúló együttműködésért uniós szinten.
- (23) Az illetékes hatóságoknak vagy a CSIRT-eknek ténylegesen és hatékonyan meg kell kapniuk a szervezetektől az eseményekre vonatkozó bejelentéseket. Az egyedüli kapcsolattartó pontokat azzal kell megbízni, hogy továbbítsák az eseményekre vonatkozó bejelentéseket a többi érintett tagállam egyedüli kapcsolattartó pontjának. A tagállamok hatóságainak szintjén, annak biztosítása érdekében, hogy minden tagállamban egyetlen egyedüli kapcsolattartó pont legyen, az illetékes hatóságoktól az XXXX/XXXX rendelet alapján a pénzügyi ágazatbeli szervezetekkel kapcsolatos eseményekkel kapcsolatos releváns információkat az egyedüli kapcsolattartó pontnak kell megküldeni, amely adott esetben azokat ezen irányelv alapján az illetékes nemzeti illetékes hatóságoknak vagy a CSIRT-eknek továbbíthatja.
- (24) A tagállamoknak mind technikai, mind szervezeti képességek tekintetében megfelelő felszereléssel kell rendelkezniük a hálózati és információs rendszerekkel kapcsolatos események és kockázatok megelőzésére, felderítésére, azok kezelésére és mérséklésére. A tagállamoknak ezért biztosítaniuk kell, hogy jól működő CSIRT-ekkel, más néven számítógépes vészhelyzeteket elhárító csoportokkal (CERT-ek) rendelkezzenek, amelyek megfelelnek az alapvető követelményeknek annak érdekében, hogy garantálják az események és kockázatok kezelésének hatékony és kompatibilis képességeit, valamint hogy uniós szinten biztosítsák a hatékony együttműködést. Figyelemmel a szervezetek és a CSIRT-ek közötti bizalmi kapcsolat fokozására, azokban az esetekben, amikor a CSIRT az illetékes hatóság része, a tagállamoknak fontolóra kell venniük a CSIRT-ek által biztosított operatív feladatok funkcionális elkülönítését, különösen az információmegosztással és a szervezetek és az illetékes hatóságok felügyeleti tevékenységei támogatásával kapcsolatban.
- (25) A személyes adatok tekintetében a CSIRT-ek az (EU) 2016/679 európai parlamenti és tanácsi rendelettel¹⁹ összhangban a személyes adatok tekintetében ezen irányelv alapján valamely szervezet nevében és kérésére a szolgáltatások nyújtásához használt hálózati és információs rendszereket proaktív átvizsgálhatják. A tagállamoknak arra kell törekedniük, hogy valamennyi ágazati CSIRT számára egyenlő szintű technikai képességeket biztosítsanak. A tagállamok kérhetik az Európai Unió Kiberbiztonsági Ügynökségének (ENISA) segítségét a nemzeti CSIRT-ek fejlesztéséhez.

¹⁹ 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.).

- (26) Tekintettel a kiberbiztonság terén folytatott nemzetközi együttműködés fontosságára, a CSIRT-ek részt vehetnek az ezen irányelv által létrehozott CSIRT-hálózatok mellett nemzetközi együttműködési hálózatokban is.
- (27) A nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló (EU) 2017/1548 bizottsági ajánlás („Útmutató”) mellékletével összhangban²⁰, nagyszabású eseménynek azt az eseményt kell jelentenie, amelynek legalább két tagállamra jelentős hatása van, vagy amelyből származó zavar meghaladja egy tagállam elhárítási képességét. Okuktól és hatásuktól függően a nagyszabású események eszkalálódhatnak, és olyan teljes körű válsággá válhatnak, amely nem teszi lehetővé a belső piac megfelelő működését. Tekintettel az említett események széles skálájára és a legtöbb esetben határokon átnyúló jellegére, a tagállamoknak és az érintett uniós intézményeknek, szervezeteknek és ügynökségeknek technikai, operatív és politikai szinten együtt kell működniük a reagálás Unión belüli megfelelő összehangolása érdekében.
- (28) Mivel a hálózati és információs rendszerek biztonsági réseinek kiaknázása jelentős zavarokat és kárt okozhat, a biztonsági rések gyors azonosítása és elhárítása fontos tényező a kiberbiztonsági kockázat csökkentésében. Az említett rendszereket fejlesztő szervezeteknek ezért megfelelő eljárásokat kell kidolgozniuk a biztonsági rések felfedezéskor történő kezelésére. Mivel a biztonsági réseket gyakran harmadik felek (adatszolgáltatásra kötelezett szervezetek) fedezik fel és jelentik (közlik), az IKT-termékek vagy -szolgáltatások gyártójának vagy szolgáltatójának szintén be kell vezetnie a biztonsági résre vonatkozó információk harmadik felektől történő fogadásához szükséges eljárásokat. Ebben a tekintetben az ISO/IEC 30111 és az ISO/IEC 29417 nemzetközi szabvány útmutatást nyújt a biztonsági rések kezeléséhez, illetve rendre a biztonsági rés nyilvánosságra hozatalához. A biztonsági rés nyilvánosságra hozatalát illetően különösen fontos az adatszolgáltatásra kötelezett szervezetek és az IKT-termékek vagy -szolgáltatók gyártói vagy szolgáltatói közötti koordináció. A biztonsági rés összehangolt nyilvánosságra hozatala strukturált folyamatot határoz meg, amelyen keresztül a szervezetek a biztonsági réseket oly módon jelentik, hogy a szervezet diagnosztizálja és orvosolja a biztonsági rést, mielőtt a biztonsági résre vonatkozó részletes információkat harmadik felekkel vagy a nyilvánossággal közölné. A biztonsági rés összehangolt nyilvánosságra hozatalának magában kell foglalnia az adatszolgáltatásra kötelezett szervezet és a szervezet közötti koordinációt a hiányosságok orvoslásának és közzétételének időzítése tekintetében.
- (29) A tagállamoknak ezért intézkedéseket kell hozniuk a biztonsági rés összehangolt nyilvánosságra hozatalának egy megfelelő nemzeti politika kialakításával történő megkönnyítésére. Ebben a tekintetben a tagállamoknak ki kell jelölniük egy CSIRT-et, amely betölti a „koordinátor” szerepét, és közvetítőként jár el az adatszolgáltatásra kötelezett szervezetek és az IKT-termékek vagy -szolgáltatások gyártói vagy szolgáltatói között, amennyiben ez szükséges. A CSIRT-koordinátor feladatai közé tartozik különösen az érintett szervezetek azonosítása és a velük való kapcsolatfelvétel, az adatszolgáltatásra kötelezett szervezetek támogatása, a nyilvánosságra hozatali ütemtervek letárgyalása és a több szervezetet érintő biztonsági rések kezelése (több felet érintő biztonsági rés közzététele). Ha a biztonsági rések IKT-termékek vagy -szolgáltatók több tagállamban letelepedett több gyártóját vagy

²⁰

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.).

szolgáltatóját érintik, az érintett tagállamok kijelölt CSIRT-jeinek együtt kell működniük a CSIRT-hálózaton belül.

- (30) Az IKT-termékeket és -szolgáltatásokat érintő biztonsági résekkel kapcsolatos helyes és időszerű információkhoz való hozzáférés hozzájárul a jobb kiberbiztonsági kockázatkezeléshez. E tekintetben a biztonsági résekről nyilvánosan elérhető információk forrásai fontos eszköznek minősülnek a szervezetek és azok felhasználói, de az illetékes nemzeti hatóságok és a CSIRT-ek számára is. Emiatt az ENISA-nak biztonságrés-nyilvántartást kell létrehoznia, amelyben az alapvető és fontos szervezetek és beszállítók, valamint az ezen irányelv alkalmazásának hatálya alá nem tartozó szervezetek önkéntes alapon nyilvánosságra hozhatják a biztonsági réseket és megadhatják a biztonsági résre vonatkozó azon információkat, amelyek lehetővé teszi a felhasználók számára a megfelelő mérséklési intézkedések megtételét.
- (31) Noha léteznek hasonló biztonságrés-nyilvántartások vagy adatbázisok, ezeket nem az Unióban letelepedett szervezetek üzemeltetik és tartják fenn. Az ENISA által fenntartott európai biztonságrés-nyilvántartás javulást hoz a biztonsági rések hivatalos nyilvánosságra hozatala előtti közzétételi folyamat átláthatósága tekintetében, valamint rezilienciát a hasonló szolgáltatások nyújtásának megszakadása vagy zavara esetére. A kettős erőfeszítések megelőzése és a lehető legnagyobb mértékű kiegészítő jelleg elérése érdekében az ENISA-nak fel kell tárnia harmadik országok jogrendszerében hasonló nyilvántartásokkal strukturált együttműködési megállapodások megkötésének lehetőségét.
- (32) Az együttműködési csoportnak kétfévente munkaprogramot kell kidolgoznia, amely tartalmazza a csoport céljainak és feladatainak végrehajtása érdekében végrehajtandó intézkedéseket. Az ezen irányelv alapján elfogadott első program időkeretét összhangba kell hozni az utolsó, az (EU) 2016/1148 irányelv alapján elfogadott program időkeretével a csoport munkájában bekövetkező esetleges zavarok elkerülése érdekében.
- (33) 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, amelyeket a meglévő szabályok jobb végrehajtása révén kell megfogalmazni.
- (34) Az együttműködési csoportnak továbbra is rugalmas fórumnak kell maradnia, és reagálnia kell a változó és új politikai prioritásokra és kihívásokra, az erőforrások rendelkezésre állásának figyelembevételével. Rendszeres közös megbeszéléseket kell szerveznie az Unió egész területéről érkező érdekeltekkel, hogy megvitassák a csoport tevékenységeit, és információkat gyűjtsenek a felmerülő szakpolitikai kihívásokról. Az uniós szintű együttműködés fokozása érdekében a csoportnak fontolóra kell vennie a kiberbiztonsági szakpolitikában részt vevő uniós testületek és ügynökségek – például a Kiberbűnözés Elleni Európai Központ (EC3), az Európai Unió Repülésbiztonsági Ügynöksége (EASA) és az Európai Unió Űrprogramja (EUSPA) meghívását a munkájában történő részvétellel.
- (35) Az együttműködés javítása érdekében az illetékes hatóságokat és a CSIRT-eket fel kell hatalmazni arra, hogy más tagállamok tisztviselőinek csereprogramjaiban részt vegyenek. Az illetékes hatóságoknak meg kell hozniuk a szükséges intézkedéseket annak érdekében, hogy más tagállamok tisztviselői tényleges szerepet tölthessenek be a fogadó illetékes hatóság tevékenységeiben.

- (36) Az Uniónak adott esetben nemzetközi megállapodásokat kell kötnie az EUMSZ 218. cikkével összhangban harmadik országokkal vagy nemzetközi szervezetekkel, lehetővé téve és megszervezve részvételüket az együttműködési csoport és a CSIRT-hálózat egyes tevékenységeiben. Az említett megállapodásoknak biztosítaniuk kell az adatok megfelelő védelmét.
- (37) A tagállamoknak hozzá kell járulniuk az (EU) 2017/1584 ajánlásban meghatározott uniós kiberbiztonsági válságelhárítási keret létrehozásához a meglévő együttműködési hálózatokon, nevezetesen az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatán (EU-CyCLONe), a CSIRT-hálózaton és az együttműködési csoporton keresztül. Az EU-CyCLONe-nak és a CSIRT-hálózatoknak az együttműködés módozatait meghatározó eljárási megállapodások alapján kell együttműködniük. Az EU-CyCLONe eljárási szabályzatának részletesen meg kell határoznia a hálózat működésének módját, a teljesség igénye nélkül ideértve a szerepköröket, 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 a politikai szintű integrált válságelhárítási (IPCR) megállapodásokra kell támaszkodniuk. A Bizottságnak erre a célra az ARGUS magas szintű, ágazatok közötti válságkoordinációs folyamatát kell alkalmaznia. Ha a válságnak fontos külső vagy a közös biztonság- és védelempolitika (KBVP) dimenziója van, aktiválni kell az Európai Külügyi Szolgálat (EKSZ) válságelhárítási mechanizmusát (VEM).
- (38) Ezen irányelv alkalmazásában a „kockázat” kifejezésnek a kiberbiztonsági esemény által okozott veszteség vagy zavar lehetőségére kell utalnia, és ezt az említett veszteség vagy zavar nagyságrendje és az említett esemény bekövetkezési valószínűsége kombinációjaként kell kifejezni.
- (39) Ezen irányelv alkalmazásában a „majdnem bekövetkezett (near miss) esemény” kifejezésnek olyan eseményre kell utalnia, amely potenciálisan kárt okozhatott volna, de a teljes bekövetkezését sikeresen megakadályozták.
- (40) A kockázatkezelési intézkedéseknek az események kockázatainak azonosítására, az események megelőzésére, felderítésére és kezelésére, valamint azok hatásainak enyhítésére irányuló intézkedéseket kell tartalmazniuk. A hálózati és információs rendszerek biztonságának magában kell foglalnia a tárolt, továbbított és feldolgozott adatok biztonságát.
- (41) Az alapvető és fontos szervezetekre aránytalan pénzügyi és adminisztratív terhek előírásának elkerülése érdekében a kiberbiztonsági kockázatkezelési követelményeknek arányosnak kell lenniük az érintett hálózat és információs rendszer által jelentett kockázattal, figyelembe véve az említett intézkedések korszerűségét.
- (42) Az alapvető és fontos szervezeteknek biztosítaniuk kell a tevékenységük során használt hálózati és információs rendszerek biztonságát. Ezek elsősorban magánhálózatok és információs rendszerek, amelyeket belső informatikai személyzetük kezel, vagy amelyek biztonságát kiszervezték. Az ezen irányelv szerinti kiberbiztonsági kockázatkezelési és jelentéstételi követelményeket az érintett alapvető és fontos szervezetekre alkalmazni kell, függetlenül attól, hogy hálózatuk és információs rendszereik karbantartását házon belül végzik-e vagy kiszervezik.
- (43) A szervezet ellátási láncából és a beszállítóival való kapcsolatából eredő kiberbiztonsági kockázatok kezelése különösen fontos, tekintettel azokra az esetekre, amikor a szervezetek kibertámadások áldozatává válnak, és amikor a rosszindulatú

szereplők azzal tudják veszélyeztetni a szervezet hálózatának és információs rendszereinek biztonságát, hogy harmadik fél termékeit és szolgáltatásait érintő biztonsági réseket kihasználnak. A szervezeteknek ezért fel kell mérniük és figyelembe kell venniük a termékek általános minőségét és beszállítóik és szolgáltatóik kiberbiztonsági gyakorlatait, beleértve a biztonságos fejlesztési eljárásaikat is.

- (44) A szolgáltatók közül az irányított biztonsági szolgáltatók olyan területeken, mint az események elhárítása, behatolási tesztek, biztonsági auditok és tanácsadás, különösen fontos szerepet töltenek be abban, hogy segítsék a szervezeteket az események felderítésében és azok elhárításában. Azonban maguk az irányított biztonsági szolgáltatók is kibertámadások célpontjai, és az üzemeltetők működésébe való szoros integrációjuk révén különös kiberbiztonsági kockázatot jelentenek. A szervezeteknek ezért fokozott gondossággal kell eljárniuk az irányított biztonsági szolgáltató kiválasztása során.
- (45) A szervezeteknek foglalkozniuk kell azon kiberbiztonsági kockázatokkal is, amelyek egy szélesebb ökoszisztémán belüli más érdekelttel folytatott interakcióikból és kapcsolataikból fakadnak. A szervezeteknek különösen meg kell tenniük a megfelelő intézkedéseket annak biztosítása érdekében, hogy az egyetemekkel és a kutatóintézetekkel folytatott együttműködésük kiberbiztonsági politikájukkal összhangban történjen, és a bevált gyakorlatokat kövessék az információkhoz való általános hozzáférés és terjesztés, valamint különösen a szellemi tulajdon védelme tekintetében. Hasonlóképpen – tekintettel az adatok szervezetek tevékenysége szempontjából fennálló fontosságára és értékére – amennyiben az adatok átalakítására és harmadik felektől származó adatelemzési szolgáltatásokra támaszkodnak, a szervezeteknek meg kell tenniük a megfelelő kiberbiztonsági intézkedéseket.
- (46) Az ellátási lánc kulcsfontosságú kockázatainak további kezelése és az ezen irányelv hatálya alá tartozó ágazatokban működő szervezetek számára az ellátási láncsal és a szállítóval kapcsolatos kiberbiztonsági kockázatok megfelelő kezelésének elősegítése érdekében az érintett nemzeti hatóságokat bevonó együttműködési csoportnak a Bizottsággal és az ENISA-val együttműködve koordinált ágazati ellátásilánc-kockázatértékelést kell végeznie, az 5G hálózatok kiberbiztonságáról szóló (EU) 2019/534 ajánlást követően az 5G hálózatok esetében már megtettek szerint²¹, annak meghatározása céljából, hogy melyek a kritikus IKT-szolgáltatások, -rendszerek vagy -termékek, a releváns fenyegetések és a biztonsági rések.
- (47) Az ellátásilánc-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 biztonságának uniós összehangolt kockázatértékelése során és az együttműködési csoport által elfogadott 5G kiberbiztonsági uniós eszköztárban meghatározottakat is. Az összehangolt 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

²¹ A Bizottság (EU) 2019/534 ajánlása (2019. március 26.) az 5G hálózatok kiberbiztonságáról (HL L 88., 2019.3.29., 42. o.).

termékek elérhetősége; iv. az IKT-szolgáltatások, -rendszerek vagy -termékek teljes ellátási láncának rezilienciája a zavaró eseményekkel szemben és v. a megjelenő IKT-szolgáltatások, -rendszerek vagy -termékek esetében azok jövőbeli jelentősége a szervezetek tevékenysége szempontjából.

- (48) A nyilvános elektronikus hírközlő hálózatok vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatások szolgáltatóira, valamint a hálózati és információs rendszereik biztonságával kapcsolatos megbízható szolgáltatókra előírt jogszabályi kötelezettségek észszerűsítése, valamint annak lehetővé tétele érdekében, hogy ezek a szervezetek és illetékes hatóságai kiaknázhassák az ezen irányelv által létrehozott jogi keret előnyeit (ideértve a kockázatok és események kezeléséért felelős CSIRT kijelölését, az illetékes hatóságok és szervek részvételét az együttműködési csoport és a CSIRT hálózat munkájában), ezeket be kell vonni ezen irányelv hatálya alá. A 910/2014/EU európai parlamenti és tanácsi rendelet²² és az (EU) 2018/1722 európai parlamenti és tanácsi irányelv²³ megfelelő, az említett típusú szervezetekre vonatkozó biztonsági és bejelentési követelmények előírásával kapcsolatos rendelkezéseit ezért hatályon kívül kell helyezni. A jelentési kötelezettségekre vonatkozó szabályok nem érinthetik az (EU) 2016/679 rendeletet és a 2002/58/EK európai parlamenti és tanácsi irányelvet²⁴.
- (49) Adott esetben és a szükségtelen zavarok elkerülése érdekében az (EU) 2018/1722 irányelv 40. cikkének (1) bekezdésében meghatározott biztonsági intézkedésekre vonatkozó szabályok átültetésére elfogadott meglévő nemzeti iránymutatásokat és nemzeti jogszabályokat, illetve az irányelv az esemény jelentőségével kapcsolatos paraméterekre vonatkozó 40. cikkének (2) bekezdését a felügyeletért és a végrehajtásért felelős illetékes hatóságoknak ezen irányelv alkalmazásában továbbra is alkalmazniuk kell.
- (50) A 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. Az említett szolgáltatások nyújtóinak tehát biztosítaniuk kell azt is, 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 szolgáltatások kockázatának mértéke bizonyos szempontból alacsonyabbnak tekinthető, mint a hagyományos elektronikus hírközlési szolgáltatások esetében. Ugyanez vonatkozik azon személyközi hírközlési szolgáltatásokra, amelyek számokat használnak, és amelyek nem gyakorolnak tényleges ellenőrzést a jelátvitel felett.
- (51) A belső piac minden eddiginél jobban támaszkodik az internet működésére. Gyakorlatilag minden lényeges és fontos szervezet szolgáltatásai az interneten keresztül nyújtott szolgáltatásoktól függenek. Az alapvető és fontos szervezetek által nyújtott szolgáltatások zavartalanságának biztosítása érdekében fontos, hogy a

²² 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.).

²³ Az Európai Parlament és a Tanács (EU) 2018/1722 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról (HL L 321., 2018.12.17., 36. o.).

²⁴ 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.).

nyilvános elektronikus hírközlő hálózatok – például az internetes gerinchálózat vagy a tenger alatti hírközlésre szolgáló kábelek – megfelelő kiberbiztonsági intézkedéseket vezessenek be, és jelentsék az ezekkel kapcsolatos eseményeket.

- (52) Adott esetben a szervezeteknek tájékoztatniuk kell a szolgáltatásaikat igénybe vevőket a sajátos és jelentős fenyegetésekről, valamint azokról az intézkedésekről, amelyeket megtehetnek a rájuk nézve ebből eredő kockázat csökkentése érdekében. A szolgáltatás említett igénybe vevői ilyen fenyegetésekről történő tájékoztatásának követelménye nem mentesítheti a szervezeteket azon kötelezettség alól, hogy saját költségeikre megfelelő és azonnali intézkedéseket hozzanak a kiberfenyegetések megelőzésére vagy elhárítására, valamint a szolgáltatás normál biztonsági szintjének helyreállítására. A biztonsági fenyegetésekkel kapcsolatos említett információkat a szolgáltatást igénybe vevőknek ingyenesen kell megkapniuk.
- (53) A nyilvános elektronikus hírközlő hálózatok vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatások szolgáltatóinak különösen tájékoztatniuk kell a szolgáltatást igénybe vevőket a különleges és jelentős kiberfenyegetésekről, valamint azokról az intézkedésekről, amelyeket megtehetnek a kommunikáció biztonságának védelme érdekében, például bizonyos típusú szoftverek vagy titkosítási technológiák használata révén.
- (54) Az elektronikus hírközlő hálózatok és szolgáltatások biztonságának megőrzése érdekében elő kell mozdítani a titkosítást és különösen a végponttól végpontig terjedő titkosítást, amelyet szükség esetén kötelezővé kell tenni az említett szolgáltatások és hálózatok szolgáltatói számára, a 18. cikk alkalmazásában alapértelmezett és beépített, a biztonsággal és a magánélet védelmével kapcsolatos elvekkel összhangban. 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 nyomozását, felderítését és a vádeljárás lefolytatását az uniós joggal összhangban. A végponttól végpontig terjedő titkosított kommunikációban az információkhoz való jogszerű hozzáférés megoldásainak meg kell őrizniük a titkosítás hatékonyságát a magánélet és a kommunikáció biztonságának védelme mellett, miközben ténylegesen el kell hárítaniuk a bűnözést.
- (55) Ez az irányelv kétlépcsős megközelítést állapít meg az események bejelentésével kapcsolatban annak érdekében, hogy megtalálja a megfelelő egyensúlyt egyrészt a gyors bejelentések között, amelyek segítenek enyhíteni az események potenciális terjedését, és lehetővé teszik a szervezetek számára, hogy támogatást kérjenek, másrészt pedig az olyan mélyreható jelentés érdekében, amely értékes tanulságokat von le az egyes eseményekből, és idővel javítja az egyes vállalatok és teljes ágazatok kiberfenyegetésekkel szembeni rezilienciáját. Ha a szervezetek tudomást szereznek egy eseményről, meg kell követelni, hogy 24 órán belül nyújtsanak be első bejelentést, amelyet legkésőbb egy hónappal később zárójelentésnek kell követnie. Az első bejelentésnek csak azokat az információkat kell tartalmaznia, amelyek feltétlenül szükségesek ahhoz, hogy az illetékes hatóságok tudomást szerezzenek az eseményről, és lehetővé tegyék a szervezet számára, hogy szükség esetén segítséget kérjen. Az említett bejelentésnek adott esetben fel kell tüntetnie, hogy az eseményt vélhetően jogellenes vagy rosszindulatú cselekmény okozta-e. A tagállamoknak biztosítaniuk kell, hogy az első bejelentés benyújtásának követelménye ne vonja el az adatszolgáltató szervezet erőforrásait az események kezelésével kapcsolatos tevékenységektől, amelyeket prioritásként kell kezelni. Annak elkerülése érdekében, hogy az események bejelentési kötelezettségei elvonják az erőforrásokat az események

kezelésétől, vagy más módon veszélyeztessék a szervezetek e tekintetben tett erőfeszítéseit, a tagállamoknak azt is elő kell írniuk, hogy kellően indokolt esetekben, az illetékes hatóságokkal vagy a CSIRT-tel egyetértésben az érintett szervezet eltérhet az első bejelentés 24 órás és a zárójelentés egy hónapos határidejétől.

- (56) 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 terheket jelentenek, és bizonytalansághoz vezethetnek az említett bejelentések formátumát és eljárásait illetően is. Erre figyelemmel, valamint a biztonsági események bejelentésének egyszerűsítése céljából a tagállamoknak létre kell hozniuk egy *egyedüli kapcsolattartó pontot* az ezen irányelv, valamint más uniós jogszabályok, például az (EU) 2016/679 rendelet és a 2002/58/EK irányelv által előírt összes bejelentés tekintetében. Az ENISA-nak az együttműködési csoporttal együttműködve közös bejelentési sablonokat kell kidolgoznia olyan iránymutatások révén, amelyek egyszerűsítik és összehangolják az uniós jog által kért jelentéstételi információkat, és csökkentik a vállalatok terheit.
- (57) 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 az EC3 és az ENISA megkönnyítse a koordinációt a különböző tagállamok illetékes hatóságai és bűnüldöző hatóságai között.
- (58) Az események következtében sok esetben személyes adatok kerülnek veszélybe. Ebben az összefüggésben az illetékes hatóságoknak a 2002/58/EK irányelv szerint együtt kell működniük és információt kell cserélniük minden releváns kérdésben az adatvédelmi hatóságokkal és a felügyeleti hatóságokkal.
- (59) A doménnevek és a nyilvántartási adatok (ún. 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 Unión belüli egységesen magas szintű kiberbiztonsághoz. Amennyiben a feldolgozás személyes adatokat is tartalmaz, az említett feldolgozásnak meg kell felelnie az uniós adatvédelmi jogszabályoknak.
- (60) Ezen adatok rendelkezésre állása és időben történő hozzáférhetősége a hatóságok – ideértve a bűncselekmények megelőzése, kivizsgálása vagy büntetőeljárás alá vonása céljából az uniós vagy nemzeti jogszabályok alapján illetékes hatóságokat, a CERT-eket (CSIRT-eket) –, valamint ügyfelek adatai tekintetében az elektronikus hírközlő hálózatok szolgáltatói, valamint az említett ügyfelek nevében eljáró, kiberbiztonsági technológiák és szolgáltatások szolgáltatói számára elengedhetetlen a doménnévrendszerrel való visszaélések megelőzéséhez és felszámolásához, különösen a kiberbiztonsági események megelőzéséhez, felderítéséhez és azok elhárításához. Az említett hozzáférésnek meg kell felelnie az uniós adatvédelmi jogszabályoknak, amennyiben az személyes adatokhoz kapcsolódik.
- (61) A pontos és teljes doménnév-nyilvántartási adatok rendelkezésre állásának biztosítása érdekében a legfelső szintű doménnév-nyilvántartóknak és a TLD-hez doménnév-nyilvántartási szolgáltatást nyújtó szervezeteknek (ügynevezett regisztrátoroknak) össze kell gyűjteniük a doménnevek nyilvántartási adatait és garantálniuk kell azok

integritását és elérhetőségét. Különösen a legfelső szintű doménnév-nyilvántartóknak és a TLD-hez doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteknek szabályzatokat és eljárásokat kell kidolgozniuk a pontos és teljes nyilvántartási adatok összegyűjtése és vezetése, valamint az uniós adatvédelmi szabályokkal összhangban a pontatlan nyilvántartási adatok megelőzése és kijavítása céljából.

- (62) A legfelső szintű doménnév-nyilvántartóknak és a számukra doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteknek nyilvánosan hozzáférhetővé kell tenniük az uniós adatvédelmi szabályok hatályán kívül eső doménnév-nyilvántartási adatokat, például a jogi személyeket érintő adatokat²⁵. A legfelső szintű doménnév-nyilvántartóknak és a TLD-hez doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteknek az uniós adatvédelmi jogszabályokkal összhangban lehetővé kell tenniük a jogosult hozzáférés-igénylők számára a természetes személyekre vonatkozó meghatározott doménnév-nyilvántartási adatokhoz való jogszerű hozzáférést is. A tagállamoknak biztosítaniuk kell, hogy a legfelső szintű doménnév-nyilvántartók és a számukra doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek indokolatlan késedelem nélkül reagáljanak a jogosult hozzáférés-igénylők kérésére a doménnév-nyilvántartási adatok nyilvánosságra hozatalára. A legfelső szintű doménnév-nyilvántartóknak és a számukra 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. A hozzáférési eljárás magában foglalhatja egy interfész, portál vagy más technikai eszköz használatát is, hogy hatékony rendszert lehessen biztosítani a nyilvántartási adatok lekérésére és elérésére. A Bizottság a belső piacon a harmonizált gyakorlatok előmozdítása érdekében iránymutatásokat fogadhat el az említett eljárásokról, az Európai Adatvédelmi Testület hatáskörének sérelme nélkül.
- (63) Az ezen irányelv alapján lényeges és fontos minden szervezetnek annak a tagállamnak a joghatósága alá kell tartoznia, ahol szolgáltatásait nyújtja. Ha a szervezet több tagállamban nyújt szolgáltatásokat, 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.
- (64) A DNS-szolgáltatók szolgáltatásainak és műveleteinek határokon átnyúló jellegének figyelembevétele érdekében a legfelső szintű doménnév-nyilvántartók, tartalomszolgáltató hálózati szolgáltatók, felhőszolgáltatók, adatközpont-szolgáltatók és digitális szolgáltatók esetében csak egy tagállamnak lehet joghatósága e szervezetek felett. A joghatóságot annak a tagállamnak kell tulajdonítani, amelyben az adott szervezet üzleti tevékenységének fő helye az Unióban 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

²⁵

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, a (14) preambulumbekzdés értelmében „(e) rendelet hatálya nem terjed ki az olyan személyes adatkezelésre, amely jogi személyekre, illetve amely különösen olyan vállalkozásokra vonatkozik, amelyeket jogi személyként hoztak létre, beleértve a jogi személy nevét és formáját, valamint a jogi személy elérhetőségére vonatkozó adatokat”.

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 annak a helynek kell lennie, ahol az Unióban meghozzák a kiberbiztonsági kockázatkezelési intézkedésekkel kapcsolatos döntéseket. Ez általában megfelel a vállalatok uniós központi ügyvezetése helyének. Ha ilyen döntéseket nem hoznak az Unióban, úgy kell tekinteni, hogy az üzleti tevékenység fő helye azokban a tagállamokban van, ahol a szervezetnek az Unióban a legmagasabb a munkavállalói létszáma. Ha a szolgáltatásokat vállalkozások csoportja végzi, az irányító vállalkozás üzleti tevékenysége fő helyét a vállalkozáscsoport üzleti tevékenysége fő helyének kell tekinteni.

- (65) Olyan esetekben, amikor az Unión belül kínál szolgáltatásokat az Unióban nem letelepedett DNS-szolgáltató, legfelső szintű doménnév-nyilvántartó, tartalomszolgáltató hálózati szolgáltató, felhőszolgáltató, adatközpont-szolgáltató és digitális szolgáltató, ki kell jelölnie egy képviselőt. Annak eldöntése érdekében, hogy az említett szervezet kínál-e szolgáltatásokat az Unión belül, meg kell győződni arról, hogy nyilvánvaló-e, hogy a szervezet tervezi-e egy vagy több tagállamban tartózkodó személyek szolgáltatások kínálását. A szervezet vagy a közvetítő webhelyének, az e-mail-címnek és más elérhetőségeknek az Unióban való pusztán elérhetősége, vagy a szervezet alapítása szerinti harmadik országban általánosan használt nyelv használata önmagában nem elegendő információ az említett szándék megállapításához. Azonban olyan tényezők, mint például egy vagy több tagállamban általánosan használt nyelv vagy pénznem használata, a szolgáltatások adott másik nyelven történő megrendelésének lehetősége, vagy az Unióban tartózkodó ügyfelek vagy felhasználók megemlézése nyilvánvalóvá teheti, hogy a szervezet tervezi az Unión belüli szolgáltatások kínálását. A képviselőnek a szervezet nevében kell eljárnia, és az illetékes hatóságoknak vagy a CSIRT-eknek lehetővé kell tenni, hogy kapcsolatba lépjenek a képviselővel. A képviselőt a szervezet írásbeli meghatalmazásával kifejezetten ki kell jelölni, hogy a szervezet nevében eljárjon az utóbbi ezen irányelv szerinti kötelezettségei tekintetében, ideértve az események jelentését is.
- (66) Amennyiben a nemzeti vagy az uniós jogszabályok szerint minősítettnek minősülő információkat ezen irányelv rendelkezései alapján kicserélik, jelentik vagy más módon megosztják, a minősített információk kezelésére vonatkozó különös szabályokat alkalmazni kell.
- (67) A kiberfenyegetések bonyolultabbá és kifinomultabbá válásával a jó észlelési és megelőzési intézkedések nagymértékben függenek a szervezetek között a fenyegetésekre és biztonsági résekre vonatkozó információk rendszeres megosztásától. Az információmegosztás hozzájárul a kiberfenyegetésekkel kapcsolatos tudatosság erősítéséhez, ami viszont fokozza a szervezetek azon képességét, hogy megakadályozzák a fenyegetések valós eseménnyé válását, és lehetővé teszi a szervezetek számára, hogy jobban visszaszorítsák az események hatásait és a hatékonyabb helyreállítást. Uniós szintű útmutatás hiányában úgy tűnik, hogy számos tényező gátolta az említett információmegosztást, nevezetesen a verseny- és felelősségi szabályokkal való összeegyeztethetőség bizonytalansága.
- (68) A szervezeteket ösztönözni kell arra, hogy stratégiai, taktikai és operatív szinten együttesen hasznosítsák egyéni tudásukat és gyakorlati tapasztalataikat annak érdekében, hogy javítsák képességeiket a kiberfenyegetések megfelelő felmérésére, nyomon követésére, az ellenük való védekezésre és azok elhárítására. Ezért lehetővé kell tenni az önkéntes információmegosztási megállapodások uniós szintű

mechanizmusainak megjelenését. Ennek érdekében a tagállamoknak aktívan támogatniuk és ösztönözniük kell az ezen irányelv hatálya alá nem tartozó érintett szervezeteket is, hogy vegyenek részt az említett információmegosztási mechanizmusokban. Ezeket a mechanizmusokat az Unió versenyszabályaival, valamint az adatvédelmi uniós jogszabályokkal teljes összhangban kell végrehajtani.

- (69) A személyes adatok feldolgozásának – a hálózati és információbiztonság szervezeti egységek, hatóságok, CERT-ek, CSIRT-ek, valamint a biztonsági technológiák és szolgáltatások szolgáltatói általi biztosítása érdekében a feltétlenül szükséges és arányos mértékben – az érintett adatkezelő jogos érdekét kell képeznie, az (EU) 2016/679 rendeletben említettek szerint. Ennek ki kell terjednie az események megelőzésével, felderítésével, elemzésével és az azok elhárításával kapcsolatos intézkedésekre, a konkrét kiberfenyegetésekkel kapcsolatos tudatosság növelésére, a biztonsági rés elhárításával és az összehangolt nyilvánosságra hozattal kapcsolatos információmegosztásra, valamint az ezekre az eseményekre, valamint a kiberfenyegetésekre és biztonsági résekre, a kompromisszummutatókra, taktikákra, technikákra és eljárásokra, kiberbiztonsági figyelmeztetésekre és konfigurációs eszközökre vonatkozó önkéntes információmegosztásra. Az említett intézkedések megkövetelhetik a következő típusú személyes adatok feldolgozását: IP-címek, egységes forrásazonosítók (URL-ek), doménnevek és e-mail-címek.
- (70) 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 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 mind a szervezetek, mind 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 vonatkozik. Ez utóbbi esetben ez azt jelenti, hogy a fontos szervezeteknek nem kell módszeresen dokumentálniuk a kiberbiztonsági kockázatkezelési követelményeknek való megfelelést, míg az illetékes hatóságoknak reaktív *utólagos* felügyeleti megközelítést kell alkalmazniuk, és ezért nem terheli azokat általános kötelezettség az említett szervezetek felügyeletére.
- (71) A végrehajtás hatásossága érdekében meg kell határozni az ezen irányelvben a kiberbiztonsági kockázatkezelési és jelentéstételi kötelezettségek megszegése esetére előírt adminisztratív szankciók minimumlistáját, az említett szankciók vonatkozásában az egész Unióban egyértelmű és következetes keretet létrehozva. Megfelelő figyelmet kell fordítani a jogsértés jellegére, súlyosságára és időtartamára, a ténylegesen okozott, illetve a lehetséges kárra vagy az elszenvedett veszteségekre, a jogsértés szándékos vagy gondatlan jellegére, az elszenvedett károk és/vagy veszteségek 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. Az adminisztratív bírságokat is beleértve a szankciók kiszabására megfelelő eljárási biztosítékoknak kell vonatkozniuk, az uniós jog általános elveivel és az Európai Unió Alapjogi Chartájával összhangban, ideértve a hatékony bírói jogvédelmet és a megfelelő eljárást.
- (72) Az ezen irányelvben megállapított kötelezettségek hatékony végrehajtásának biztosítása érdekében minden illetékes hatóságnak rendelkeznie kell hatáskörrel adminisztratív bírság kiszabására vagy kiszabására.

- (73) Ha egy vállalkozást közigazgatási bírsággal sújtanak, a vállalkozást az EUMSZ 101. és 102. cikkével összhangban kell e célból vállalkozásnak tekinteni. Amennyiben közigazgatási bírságokat szabnak ki vállalkozásnak nem minősülő személyekre, a bírság megfelelő összegének mérlegelésekor a felügyeleti hatóságnak figyelembe kell vennie a tagállam általános jövedelemszintjét, valamint a személy anyagi helyzetét. A tagállamok feladata annak meghatározása, hogy az állami hatóságokat sújtsák-e és milyen mértékben adminisztratív bírságokkal. A közigazgatási bírság kiszabása nem érinti az illetékes hatóságok egyéb hatásköreinek alkalmazását vagy az ezen irányelvet átültető nemzeti szabályokban megállapított egyéb szankciók alkalmazását.
- (74) A tagállamok megállapíthatják az ezen irányelvet átültető nemzeti szabályok megsértése esetén alkalmazandó büntetőjogi szankciók szabályait. Az említett nemzeti szabályok és a kapcsolódó közigazgatási szankciók megsértése esetén büntetőjogi szankciók kiszabása azonban nem ütközhet a kétszeres büntetés tilalmának (*ne bis in idem*) a Bíróság értelmezése szerinti elvébe.
- (75) Ha ez az irányelv nem harmonizálja az adminisztratív szankciókat, vagy szükség esetén más esetekben, például az ezen irányelvben megállapított kötelezettségek súlyos megsértése esetén, a tagállamoknak olyan rendszert kell bevezetniük, amely hatékony, arányos és visszatartó erejű szankciókat ír elő. Az említett büntetőjogi vagy közigazgatási szankciók jellegét a tagállami jognak kell meghatároznia.
- (76) Az ezen irányelv alapján megállapított kötelezettségek megsértése esetén alkalmazandó szankciók hatékonyságának és visszatartó erejének további erősítése érdekében az illetékes hatóságokat fel kell hatalmazni arra, hogy a tanúsítás vagy az engedély felfüggesztéséből álló, az alapvető szervezet által nyújtott összes szolgáltatásra vagy azok egy részére kiterjedő szankciókat alkalmazzanak, és ideiglenesen eltilthassanak természetes személyeket az irányítási feladatok ellátásától. Az említett szankciókat csak a jogsértés súlyosságával arányosan lehet alkalmazni – tekintettel azok súlyosságára és a szervezetek tevékenységére, és végső soron fogyasztóikra gyakorolt hatására –, figyelembe véve az egyes esetek sajátos körülményeit, beleértve a jogsértés szándékos vagy gondatlan jellegét, az elszenvedett károk és/vagy veszteségek megelőzése vagy enyhítése érdekében tett intézkedéseket. Ezeket a szankciókat csak végső megoldásként szabad alkalmazni, vagyis csak az ezen irányelvben megállapított egyéb vonatkozó végrehajtási intézkedések kimerítése után, és csak addig az időtartamig, amíg a szankcionált szervezetek megteszik a szükséges intézkedéseket a hiányosságok elhárítására vagy az illetékes hatóság szankcionált követelményeinek betartására. Az említett szankciók kiszabására megfelelő eljárási biztosítékok vonatkoznak, az uniós jog általános elveivel és az Európai Unió Alapjogi Chartájával összhangban, ideértve a hatékony bírói jogvédelmet, a tisztességes eljárást, az ártatlanság vélelmét és a védelemhez való jogot.
- (77) Ennek az irányelvnek az (EU) 2016/679 rendelettel összhangban meg kell határoznia az illetékes hatóságok és a felügyeleti hatóságok közötti együttműködési szabályokat a személyes adatokkal kapcsolatos jogsértések kezelése érdekében.
- (78) Ennek az irányelvnek a célja a kiberbiztonsági kockázatkezelési intézkedésekért és a jelentéstételi kötelezettségekért a magas szintű felelősség biztosítása a szervezetek szintjén. Ezen okok miatt az ezen irányelv hatálya alá tartozó szervezetek vezető testületeinek jóvá kell hagyniuk a kiberbiztonsági kockázatra vonatkozó intézkedéseket, és felügyelniük kell azok végrehajtását.

- (79) Be kell vezetni egy szakértői értékelési mechanizmust, amely lehetővé teszi a tagállamok által kijelölt szakértők számára a kiberbiztonsági politikák végrehajtásának értékelését, beleértve a tagállami képességek és rendelkezésre álló erőforrások szintjét.
- (80) Az új kiberfenyegetések, a technológiai fejlődés vagy az ágazati sajátosságok figyelembevétele érdekében a Bizottságot fel kell hatalmazni arra, hogy az EUMSZ 290. cikkével összhangban jogi aktusokat fogadjon el az ebben az irányelvben előírt kockázatkezelési intézkedésekkel kapcsolatos elemek tekintetében. A Bizottságot fel kell hatalmazni arra is, hogy felhatalmazáson alapuló jogi aktusokat fogadjon el annak meghatározására, hogy az alapvető szervezetek mely kategóriái esetében van szükség tanúsítvány megszerzésére, és melyik konkrét európai kiberbiztonsági tanúsítási rendszerek alapján. 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 megállapodásban²⁶ foglalt elvekkel összhangban kerüljön sor. A felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlament és a Tanács a tagállamok szakértőivel egyidejűleg megkap minden dokumentumot, és szakértőik rendszeresen részt vehetnek a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein.
- (81) Az ezen irányelv vonatkozó rendelkezéseinek az együttműködési csoport működéséhez szükséges eljárási szabályokra, a kockázatkezelési intézkedésekhez kapcsolódó technikai elemekre vagy az információk típusára, az eseménybejelentés formátumára és eljárására vonatkozó rendelkezések egységes végrehajtásának biztosítása érdekében a Bizottságot végrehajtási hatáskörökkel kell felruházni. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek²⁷ megfelelően kell gyakorolni.
- (82) A Bizottságnak rendszeresen felül kell vizsgálnia ezt az irányelvet, az érdekelt felekkel konzultálva, különösen a társadalmi, politikai, technológiai vagy piaci körülmények változásainak figyelembevételével történő módosítás szükségességének megállapítása céljából.
- (83) Mivel ezen irányelv célkitűzését, nevezetesen a kiberbiztonság Unión belüli egységesen magas szintjének elérését a tagállamok nem tudják kielégítően megvalósítani, hanem a fellépés hatásai miatt jobban megvalósíthatók uniós szinten, ezért az Unió intézkedéseket fogadhat el az Európai Unióról szóló szerződés 5. cikkében meghatározott szubszidiaritás elvével összhangban. Az említett cikkben foglalt arányossági elvnek megfelelően ez az irányelv nem lépi túl az e célok eléréséhez szükséges mértéket.
- (84) Ez az irányelv tiszteletben tartja az alapvető jogokat, és betartja az Európai Unió Alapjogi Chartája által elismert elveket, különösen a magánélet és a kommunikáció tiszteletben tartásához való jogot, a személyes adatok védelmét, a vállalkozás szabadságát, a tulajdonhoz való jogot, a bíróság előtti hatékony jogorvoslathoz való jogot és a meghallgatáshoz való jogot. Ezt az irányelvet az említett jogokkal és elvekkel összhangban kell végrehajtani,

²⁶ HL L 123., 2016.5.12., 1. o.

²⁷ 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.).

ELFOGADTA EZT AZ IRÁNYELVET:

I. FEJEZET

Általános rendelkezések

1. cikk

Tárgy

- (1) Ez az irányelv intézkedéseket határoz meg az Unión belüli egységesen magas szintű kiberbiztonság biztosítása érdekében.
- (2) Ennek érdekében ez az irányelv:
 - a) előír kötelezettségeket a tagállamok számára a nemzeti kiberbiztonsági stratégia elfogadására, az illetékes nemzeti hatóságok, az egyedüli kapcsolattartó pontok és a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) kijelölésére vonatkozóan;
 - b) kiberbiztonsági kockázatkezelési és jelentéstételi kötelezettségeket állapít MEG az I. mellékletben említett alapvető szervezetek és a II. mellékletben említett fontos szervezetek számára;
 - c) kötelezettségeket állapít meg a kiberbiztonsági információk megosztására vonatkozóan.

2. cikk

Hatály

- (1) Ezt az irányelvet az I. mellékletben alapvető szervezetként és a II. mellékletben fontos szervezetként említett állami és magánszervezetekre kell alkalmazni. Ez az irányelv nem vonatkozik azokra a szervezetekre, amelyek a 2003/361/EK bizottsági ajánlás²⁸ értelmében mikro- és kisvállalkozásnak minősülnek.
- (2) Méretüktől függetlenül azonban ez az irányelv az I. és II. mellékletben említett szervezetekre is vonatkozik, amennyiben:
 - a) a szolgáltatásokat a következő szervezetek valamelyike nyújtja:
 - i. az I. melléklet 8. pontjában említett nyilvános elektronikus hírközlő hálózatok vagy nyilvánosan elérhető elektronikus hírközlési szolgáltatások;
 - ii. az I. melléklet 8. pontjában említett bizalmi szolgáltatók;
 - iii. az I. melléklet 8. pontjában említett legfelső szintű doménnév-nyilvántartók és doménnévrendszer (DNS) szolgáltatók;

²⁸

A Bizottság 2003/361/EK ajánlása (2003. május 6.) a mikro-, kis- és középvállalkozások meghatározásáról (HL L 124., 2003.5.20., 36. o.).

- b) a szervezet a 4. cikk 23. pontjában meghatározott közigazgatási szerv;
- c) a szervezet egy tagállamban az egyetlen szolgáltató;
- d) a szervezet által nyújtott szolgáltatás esetleges zavara hatással lehet a közbiztonságra, a közbiztonságra vagy a közegészségre;
- e) a szervezet által nyújtott szolgáltatás esetleges zavara rendszerszintű kockázatokat idézhet elő, különösen azokban az ágazatokban, ahol az említett zavarnak határokon átnyúló hatása lehet;
- f) a szervezet kritikus, mivel regionális vagy nemzeti szinten különös fontossággal bír az adott ágazat vagy szolgáltatás típusa, vagy a tagállam más, kölcsönösen függő ágazatai szempontjából;
- g) a szervezetet az (EU) XXXX/XXXX európai parlamenti és tanácsi irányelv²⁹ [A kritikus szervezetek rezilienciájáról szóló irányelv] alapján kritikus szervezetként, vagy az említett irányelv 7. cikke alapján a kritikus szervezetekkel egyenértékű szervezetként azonosítják.

A tagállamok összeállítják a b) –f) pont alapján kijelölt szervezetek listáját, és azt [az átültetési határidő lejártá után 6 hónappal] benyújtják a Bizottsághoz. A tagállamok a listát rendszeresen, de az említett időpontot követően legalább kétfévente felülvizsgálják, és adott esetben frissítik.

- (3) Ez az irányelv nem érinti a tagállamok hatáskörét a közbiztonság, a védelem és a nemzetbiztonság uniós joggal összhangban történő fenntartásával kapcsolatban.
- (4) Ezt az irányelvet a 2008/114/EK tanácsi irányelv³⁰ és a 2011/93/EU³¹ és 2013/40/EU³² európai parlamenti és tanácsi irányelv sérelme nélkül kell alkalmazni.
- (5) Az EUMSZ 346. cikk sérelme nélkül, az uniós és nemzeti szabályok értelmében bizalmas információkat, például az üzleti titoktartási szabályokat, csak akkor lehet megosztani a Bizottsággal és más érintett hatóságokkal, ha az említett információmegosztás ezen irányelv alkalmazásához szükséges. A megosztott információnak csak arra kell korlátozódnia, amely releváns és megosztás céljával arányos. Az információmegosztás megőrzi ezen információk titkosságát, és védi az alapvető vagy fontos szervezetek biztonsági és kereskedelmi érdekeit.
- (6) Ha az uniós jogszabályok ágazatspecifikus jogi aktusainak rendelkezései megkövetelik, hogy az alapvető vagy fontos szervezetek kiberbiztonsági kockázatkezelési intézkedéseket fogadjanak el, vagy bejelentsék az eseményeket vagy jelentős kiberfenyegetéseket, és ha ezek a követelmények legalább egyenértékűek az ezen irányelvben meghatározott kötelezettségekkel, ezen irányelv vonatkozó rendelkezései – beleértve a VI. fejezetben a felügyeletre és a végrehajtásra vonatkozó rendelkezéseket – nem alkalmazhatók.

²⁹ [illessze be a teljes címet és a HL-kiadvány hivatkozását, amikor ismertté válik].

³⁰ A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (HL L 345., 2008.12.23., 75. o.).

³¹ 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.).

³² 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.).

3. cikk

Minimális harmonizáció

A tagállamok az uniós jogból eredő egyéb kötelezettségeik sérelme nélkül ezen irányelvnek megfelelően magasabb szintű kiberbiztonságot biztosító rendelkezéseket fogadhatnak el vagy tarthatnak fenn.

4. cikk

Fogalommeghatározások

Ezen irányelv alkalmazásában:

1. „hálózati és információs rendszer”:
 - a) az (EU) 2018/1725 irányelv 2. cikkének (1) bekezdése értelmében vett elektronikus hírközlő hálózat;
 - b) bármely eszköz vagy egymással összekapcsolt vagy kapcsolódó eszközök csoportja, amelyek közül egy vagy több egy program alapján a digitális adatok automatikus feldolgozását végzi;
 - c) az a) és b) pont hatálya alá tartozó elemek által tárolt, feldolgozott, visszakeresett vagy továbbított digitális adatok, azok működtetése, felhasználása, védelme és karbantartása céljából;
2. „hálózati és információs rendszerek biztonsága”: a hálózati és információs rendszerek azon képessége, hogy egy adott megbízhatósági szinten ellenálljanak minden olyan intézkedésnek, amely veszélyezteti a tárolt, továbbított vagy feldolgozott adatok vagy az e hálózati vagy információs rendszerek által vagy azokon keresztül elérhető kapcsolódó szolgáltatások elérhetőségét, hitelességét, integritását vagy titkosságát;
3. „kiberbiztonság”: az (EU) 2019/881 európai parlamenti és tanácsi rendelet³³ 2. cikkének (1) bekezdése szerinti kiberbiztonság;
4. „nemzeti kiberbiztonsági stratégia”: a tagállam koherens kerete, amely stratégiai célokat és prioritásokat határoz meg az adott tagállam hálózati és információs rendszereinek biztonságával kapcsolatban;
5. „esemény”: minden olyan esemény, amely veszélyezteti a tárolt, továbbított vagy feldolgozott adatok vagy a hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető kapcsolódó szolgáltatások elérhetőségét, hitelességét, integritását vagy titkosságát;
6. „esemény kezelése”: minden olyan tevékenység és eljárás, amelynek célja az esemény felderítése, elemzése, elszigetelése és az arra adott válasz;

³³

Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Unió Kiberbiztonsági Ügynökségéről) 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.).

7. „kiberfenyegetés”: az (EU) 2019/881 rendelet 2. cikkének (8) bekezdése értelmében vett kiberfenyegetés;
8. „biztonsági rés”: valamely eszköz, rendszer, folyamat vagy irányítás gyengesége, érzékenysége vagy hibája, amelyet egy kiberfenyegetés kihasználhat;
9. „képviselő”: az Unióban letelepedett bármely természetes vagy jogi személy, akit kifejezetten kijelöltek, hogy i. DNS-szolgáltató, legfelső szintű doménnév-nyilvántartó, felhőszolgáltató, adatközpont-szolgáltató nevében eljárjon; az I. melléklet 8. pontjában említett tartalomszolgáltató hálózati szolgáltató vagy ii. a II. melléklet 6. pontjában említett, az Unióban nem letelepedett szervezetek, amelyekhez a szervezet helyett egy illetékes nemzeti hatóság vagy egy CSIRT fordulhat a szervezet ezen irányelv szerinti kötelezettségei tekintetében;
10. „szabvány”: az 1025/2012/EU európai parlamenti és tanácsi rendelet³⁴ 2. cikkének (1) bekezdése értelmében vett szabvány;
11. „műszaki előírás”: az 1025/2012/EU rendelet 2. cikkének 4. pontja szerinti műszaki előírás;
12. „internetkapcsolódási pont (IXP)”: olyan hálózati létesítmény, amely több mint két, egymástól független hálózat (autonóm rendszerek) összekapcsolását teszi lehetővé, elsősorban az internetes forgalom cseréjének megkönnyítése céljából; egy internetkapcsolódási pont csak az autonóm rendszerek tekintetében biztosít összekapcsolást; egy internetkapcsolódási pont nem követeli meg, hogy a résztvevő bármely két autonóm rendszer között zajló internetes forgalom egy harmadik autonóm rendszeren is áthaladjon, továbbá nem változtatja meg az említett forgalmat és egyéb módon sem avatkozik be abba;
13. „doménnévrendszer (DNS)”: hierarchikusan felépülő elnevezési rendszer, amely lehetővé teszi a végfelhasználók számára, hogy az interneten szolgáltatásokat és erőforrásokat érjenek el;
14. „DNS-szolgáltató”: olyan szervezet, amely rekurzív vagy hiteles doménnév-feloldási szolgáltatásokat nyújt az internet végfelhasználóinak és más DNS-szolgáltatóknak;
15. „legfelső szintű doménnév-nyilvántartó”: olyan szervezet, amely egy meghatározott TLD-t kapott, és felelős egyrészt a TLD kezeléséért – ideértve a TLD alatti doménnevek nyilvántartásba vételét –, másrészt a TLD technikai üzemeltetéséért, amely magában foglalja a névszervereinek üzemeltetését, adatbázisainak karbantartását és a TLD zónafájlok elosztását a névszerverek között;
16. „digitális szolgáltatás”: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv³⁵ 1. cikke (1) bekezdésének b) pontja értelmében vett szolgáltatás;
17. „online piactér”: a 2005/29/EK európai parlamenti és tanácsi irányelv³⁶ 2. cikkének n) pontja értelmében vett digitális szolgáltatás;

³⁴ 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.).

³⁵ 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.).

18. „online keresőmotor”: az (EU) 2019/1150 európai parlamenti és tanácsi rendelet³⁷ 2. cikkének (5) bekezdése értelmében vett digitális szolgáltatás;
19. „felhőszolgáltatás”: olyan digitális szolgáltatás, amely igény szerinti adminisztrációt és kiterjedt távoli hozzáférést tesz lehetővé megosztható és decentralizált számítástechnikai erőforrások méretezhető és rugalmas készletéhez;
20. „adatközpont-szolgáltatás”: olyan szolgáltatások, 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 a villamosenergia-elosztás és a környezetvédelmi ellenőrzés összes létesítményével és infrastruktúrájával együtt;
21. „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;
22. „közösségi hálózati 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);
23. „közigazgatási szerv”: egy tagállam következő kritériumoknak megfelelő egysége:
- a) az általános érdekű szükségletek kielégítése céljából jött létre, és nincs ipari vagy kereskedelmi jellege;
 - b) jogi személyiséggel rendelkezik;
 - c) finanszírozását többnyire állam, regionális hatóság vagy más, közjog által szabályozott szervek végzik; az említett hatóságok vagy szervek irányítása alatt áll; vagy van olyan igazgatási, irányító vagy felügyelő testülete, amely tagjainak több mint felét az állam, a regionális hatóságok vagy más közjogi szerv nevezi ki;
 - d) hatásköre van a természetes vagy jogi személyekhez a személyek, áruk, szolgáltatások vagy tőke határokon átnyúló mozgásával kapcsolatos jogaikat érintő igazgatási vagy szabályozási határozatok intézésére.
- Nem tartoznak ide azok a közigazgatási szervek, amelyek a közbiztonság, a bűnüldözés, a védelem vagy a nemzetbiztonság területén folytatnak tevékenységet.
24. „szervezet”: minden 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;

³⁶ 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.).

³⁷ 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.).

25. „alapvető szervezet”: az I. mellékletben alapvető szervezetként említett típusú minden szervezet;
26. „fontos szervezet”: a II. mellékletben fontos szervezetként említett típusú minden szervezet.

II. FEJEZET

Összehangolt kiberbiztonsági szabályozási keretek

5. cikk

Nemzeti kiberbiztonsági stratégia

- (1) Minden tagállam a magas szintű kiberbiztonság elérése és fenntartása céljából elfogad nemzeti kiberbiztonsági stratégiát, meghatározva a stratégiai célokat, valamint a megfelelő szakpolitikai és szabályozási intézkedéseket. A nemzeti kiberbiztonsági stratégia különösen a következőket tartalmazza:
- a) a kiberbiztonságra vonatkozó tagállami stratégia céljainak és prioritásainak meghatározása;
 - b) irányítási keretrendszer e célok és prioritások elérése érdekében, ideértve a (2) bekezdésben említett szakpolitikákat, valamint az állami szervek és szervezetek, valamint más érintett szereplők szerepét és felelősségét;
 - c) értékelés az adott tagállamban a releváns eszközök és a kiberbiztonsági kockázatok azonosítására;
 - d) az eseményekre való felkészültséget, azok elhárítását és a helyreállítást biztosító intézkedések meghatározása, ideértve az állami és a magánszektor közötti együttműködést;
 - e) a nemzeti kiberbiztonsági stratégia végrehajtásában részt vevő különféle hatóságok és szereplők listája;
 - f) az illetékes hatóságok közötti, ezen irányelv és az (EU) XXXX/XXXX európai parlamenti és tanácsi irányelv³⁸ [A kritikus szervezetek rezilienciájáról szóló irányelv] szerinti, az eseményekkel és a kiberfenyegetésekkel kapcsolatos információk megosztását és a felügyeleti feladatok ellátását célzó, fokozott koordináció politikai kerete.
- (2) A nemzeti kiberbiztonsági stratégia részeként a tagállamok különösen a következő politikákat fogadják el:
- a) az alapvető és fontos szervezetek által szolgáltatásaik nyújtásához használt IKT-termékek és -szolgáltatások kiberbiztonságával foglalkozó politika;
 - b) iránymutatások az IKT-termékek és -szolgáltatások kiberbiztonsággal kapcsolatos követelményeinek a közbeszerzésekbe történő felvételére és meghatározására vonatkozóan;

³⁸

[illessze be a teljes címet és a HL-kiadvány hivatkozását, amikor ismertté válik].

- c) a biztonsági rés 6. cikk értelmében vett összehangolt közzétételének előmozdítását és megkönnyítését szolgáló politika;
 - d) a nyílt internet nyilvános magja általános elérhetőségének és integritásának fenntartásával kapcsolatos politika;
 - e) a kiberbiztonsági készségek népszerűsítésére és fejlesztésére, a figyelemfelkeltésre, valamint a kutatási és fejlesztési kezdeményezésekre vonatkozó politika;
 - f) a tudományos és kutatóintézetek kiberbiztonsági eszközök és biztonságos hálózati infrastruktúra fejlesztésében való támogatására vonatkozó politika;
 - g) a vállalatok közötti önkéntes kiberbiztonsági információmegosztás támogatására vonatkozó politika, a vonatkozó eljárások és megfelelő információmegosztási eszközök az uniós jognak megfelelően;
 - h) a kkv-k – különösen az ezen irányelv hatálya alól kizárt kkv-k – sajátos szükségleteivel foglalkozó politika, a kiberbiztonsági fenyegetésekkel szembeni rezilienciájuk javításában nyújtott útmutatással és támogatással kapcsolatban.
- (3) A tagállamok az elfogadástól számított három hónapon belül értesítik a Bizottságot nemzeti kiberbiztonsági stratégiájukról. A tagállamok kizárhatnak bizonyos információkat a bejelentés alól, annyiban és amennyiben ez a nemzetbiztonság megőrzéséhez feltétlenül szükséges.
- (4) A tagállamok a legfontosabb teljesítménymutatók alapján legalább négyévente értékelik nemzeti kiberbiztonsági stratégiáikat, és szükség esetén módosítják azokat. Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) kérésre segítséget nyújt a tagállamoknak egy nemzeti stratégia és a stratégia értékeléséhez szükséges fő teljesítménymutatók kidolgozásában.

6. cikk

Biztonsági rés összehangolt közzététele és egy európai biztonságirés-nyilvántartás

- (1) Minden tagállam kijelöli a 9. cikkben említett egyik CSIRT-jét koordinátorként a biztonsági rés összehangolt közzététele céljából. A kijelölt CSIRT megbízható közvetítőként jár el, szükség esetén megkönnyítve az adatszolgáltató szervezet és az IKT-termékek vagy IKT-szolgáltatások gyártója vagy szolgáltatója közötti kapcsolattartást. Ha a bejelentett biztonsági rés az IKT-termékek vagy IKT-szolgáltatások több gyártóját vagy szolgáltatóját érinti az egész Unióban, az érintett tagállamok kijelölt CSIRT-je együttműködik a CSIRT-hálózattal.
- (2) Az ENISA kidolgozza és fenntartja az európai biztonságirés-nyilvántartást. Ebből a célból az ENISA létrehozza és fenntartja a megfelelő információs rendszereket, szabályzatokat és eljárásokat, különösen annak érdekében, hogy a fontos és alapvető szervezetek és hálózati és információs rendszer szállítók számára lehetővé tegye az IKT-termékekben vagy az IKT-szolgáltatásokban található biztonsági résök nyilvánosságra hozatalát és nyilvántartását, valamint az összes érdekelt fél számára hozzáférést biztosít a nyilvántartásba vett biztonsági résekre vonatkozó információkhoz. A nyilvántartásnak tartalmaznia kell különösen a biztonsági részt, az érintett IKT-terméket vagy IKT-szolgáltatásokat, valamint a biztonsági rés

súlyosságát a kihasználható körülmények, a kapcsolódó javítások rendelkezésre állása és a javítás hiánya tekintetében, és elérhető javítás hiányában a biztonsági réssel érintett termékek és szolgáltatások felhasználóinak szóló útmutatás a nyilvánosságra hozott biztonsági résekből fakadó kockázatok csökkenthetőségének mikéntjéről.

7. cikk

Nemzeti kiberbiztonsági válságkezelési keretek

- (1) Minden tagállam kijelöl egy vagy több illetékes hatóságot, amely felelős a nagyszabású események és válságok kezeléséért. A tagállamok biztosítják, hogy az illetékes hatóságok megfelelő forrásokkal rendelkezzenek a rájuk ruházott feladatok hatékony és eredményes végrehajtásához.
- (2) Minden tagállam meghatározza azon képességeket, eszközöket és eljárásokat, amelyek válság esetén ezen irányelv alkalmazásában alkalmazhatók.
- (3) Minden tagállam elfogad egy nemzeti kiberbiztonsági esemény- és válságelhárítási tervet, amelyben meghatározza a nagyszabású kiberbiztonsági események és válságok kezelésének célkitűzéseit és módozatait. A tervnek különösen a következőket kell tartalmaznia:
 - a) a nemzeti felkészültségi intézkedések és tevékenységek célkitűzései;
 - b) az illetékes nemzeti hatóságok feladatai és felelősségei;
 - c) válságkezelési eljárások és információmegosztási csatornák;
 - d) felkészültségi intézkedések, beleértve a gyakorlatokat és a képzési tevékenységeket;
 - e) az érintett állami és magán érdekelt felek, valamint az érintett infrastruktúra;
 - 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 elhárításában és azt támogassa.
- (4) A tagállamok közlik a Bizottsággal az (1) bekezdésben említett illetékes hatóságaik kijelölését, és a (3) bekezdésben említett nemzeti kiberbiztonsági eseményekre és válságelhárítási terveiket a kijelöléstől és a tervek elfogadásától számított három hónapon belül benyújtják. A tagállamok kizárhatnak bizonyos információkat a tervből, annyiban és amennyiben ez nemzetbiztonságukhoz feltétlenül szükséges.

8. cikk

Az illetékes nemzeti hatóságok és az egyedüli kapcsolattartó pontok

- (1) Minden tagállam kijelöl egy vagy több illetékes, a kiberbiztonságért és az ezen irányelv VI. fejezetében említett felügyeleti feladatokért felelős hatóságot. A tagállamok e célból kijelölhetnek egy vagy több meglévő hatóságot.
- (2) Az (1) bekezdésben említett illetékes hatóságok nemzeti szinten figyelemmel kísérik ezen irányelv alkalmazását.

- (3) Minden tagállam kijelöl egy nemzeti kiberbiztonsági kapcsolattartó pontot („egyedüli kapcsolattartó pont”). Ha egy tagállam csak egy illetékes hatóságot jelöl ki, ez az illetékes hatóság az adott 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 illetékes hatóságaival, valamint hogy biztosítsák az ágazatok közötti együttműködést a tagállam más illetékes nemzeti hatóságaival.
- (5) A tagállamok biztosítják, hogy az (1) bekezdésben említett illetékes hatóságok és az egyedüli kapcsolattartó pontok megfelelő forrásokkal rendelkezzenek a rájuk ruházott feladatok hatékony és eredményes végrehajtásához, és ezáltal ezen irányelv célkitűzéseinek teljesítéséhez. A tagállamok biztosítják a 12. cikkben említett együttműködési csoport kijelölt képviselőinek hatékony, eredményes és biztonságos együttműködését.
- (6) Minden tagállam indokolatlan késedelem nélkül értesíti a Bizottságot az (1) bekezdésben említett illetékes hatóság és a (3) bekezdésben említett egyedüli kapcsolattartó pont kijelöléséről, feladataikról és azok minden későbbi változásáról. Minden tagállam nyilvánosságra hozza azok kijelölését. A Bizottság közzéteszi a kijelölt egyedüli kapcsolattartó pontok listáját.

9. cikk

Számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek)

- (1) Minden tagállam kijelöl egy vagy több CSIRT-et, amely megfelel a 10. cikk (1) bekezdésében meghatározott követelményeknek, és amely legalább az I. és II. mellékletben említett ágazatokra, alágazatokra vagy szervezetekre kiterjed, és felelős az események egy jól körülhatárolható folyamat szerinti kezeléséért. CSIRT létrehozható a 8. cikkben említett illetékes hatóságon belül.
- (2) A tagállamok biztosítják, hogy minden CSIRT megfelelő erőforrásokkal rendelkezzen a 10. cikk (2) bekezdésében meghatározott feladatai hatékony végrehajtásához.
- (3) A tagállamok biztosítják, hogy minden CSIRT rendelkezzen megfelelő, biztonságos és ellenálló kommunikációs és információs infrastruktúrával az alapvető és fontos szervezetekkel és más érintett érdekelt felekkel történő információmegosztáshoz. Ebből a célból a tagállamok biztosítják, hogy a CSIRT-ek részt vegyenek a biztonságos információmegosztó eszközök kiépítésében.
- (4) A CSIRT-ek együttműködnek, és adott esetben a 26. cikkel összhangban cserélnek releváns információkat az alapvető és fontos szervezetek megbízható ágazati vagy ágazatközi csoportjaival.
- (5) A CSIRT-ek részt vesznek a 16. cikkel összhangban szervezett szakértői értékelésekben.
- (6) A tagállamok biztosítják CSIRT-eik hatékony, eredményes és biztonságos együttműködését a 13. cikkben említett CSIRT-hálózatokban.
- (7) A tagállamok indokolatlan késedelem nélkül közlik a Bizottsággal az (1) bekezdéssel összhangban kijelölt CSIRT-eket, a 6. cikk (1) bekezdésével összhangban kijelölt

CSIRT-koordinátort, valamint az I. és II. Mellékletben említett szervezetekkel kapcsolatos feladataikat.

- (8) A tagállamok kérhetik az ENISA segítségét a nemzeti CSIRT-ek kidolgozásához.

10. cikk

A CSIRT-ek követelményei és feladatai

- (1) A CSIRT-eknek meg kell felelniük a következő követelményeknek:
- a) A CSIRT-eknek biztosítaniuk kell hírközlési szolgáltatásaik magas szintű elérhetőségét az egyetlen meghibásodási pont megelőzésével, és többféle eszközzel kell rendelkezniük a mindenkori elérhetőséghez és kapcsolattartáshoz. A CSIRT-ek egyértelműen meghatározzák a kommunikációs csatornákat, és közlik azokat a körzetükkel és az együttműködő partnerekkel;
 - b) A CSIRT-ek helyiségeinek és az azokat támogató információs rendszereknek biztonságos helyszínen kell lenniük;
 - c) A CSIRT-eket el kell ellátni a kérelmek kezeléséhez és továbbításához megfelelő rendszerrel, különösen a hatékony és eredményes átadás-átvétel megkönnyítése érdekében;
 - d) A CSIRT-eknek megfelelő személyzettel kell rendelkezniük a mindenkori elérhetőségük biztosítása érdekében;
 - e) A CSIRT-eket redundáns rendszerekkel és tartalék munkaterülettel kell ellátni a szolgáltatásuk folyamatosságának biztosítása érdekében;
 - f) A CSIRT-eknek lehetőségük van részt venni a nemzetközi együttműködési hálózatokban.
- (2) A CSIRT-ek a következő feladatokat látják el:
- a) a kiberfenyegetések, biztonsági rések és események figyelemmel kísérése nemzeti szinten;
 - b) korai előrejelzés, riasztások, bejelentések és információk terjesztése az alapvető és fontos szervezeteknek, valamint más érdekelt feleknek a kiberfenyegetésekkel, biztonsági résekkel és eseményekkel kapcsolatban;
 - c) események elhárítása;
 - d) dinamikus kockázat- és eseményelemzés, valamint a kiberbiztonsággal kapcsolatos helyzetismeret biztosítása;
 - e) valamely szervezet kérésére a szolgáltatások nyújtásához használt hálózati és információs rendszerek proaktív vizsgálatának biztosítása;
 - f) részvétel a CSIRT-hálózatban, és kérésükre kölcsönös segítségnyújtás a hálózat többi tagjának.
- (3) A CSIRT-ek együttműködési kapcsolatokat alakítanak ki a magánszektor érintett szereplőivel az irányelv célkitűzéseinek jobb elérése érdekében.

- (4) Az együttműködés megkönnyítése érdekében a CSIRT-ek előmozdítják a közös vagy szabványosított gyakorlatok, osztályozási rendszerek és rendszertanok elfogadását és alkalmazását a következők tekintetében:
- a) eseménykezelési rend;
 - b) kiberbiztonsági válságkezelés;
 - c) biztonsági rések összehangolt nyilvánosságra hozatala.

11. cikk

Együttműködés nemzeti szinten

- (1) Ha a 8. cikkben említett illetékes hatóságok, az egyedüli kapcsolattartó pont és ugyanazon tagállam CSIRT-je elkülönül egymástól, együttműködnek egymással az ezen irányelvben meghatározott kötelezettségek teljesítése tekintetében.
- (2) A tagállamok biztosítják, hogy az illetékes hatóságaik vagy a CSIRT-ek értesítést kapjanak az ezen irányelv alapján bejelentett eseményekről, jelentős kiberfenyegetésekről és majdnem bekövetkezett (near miss) eseményekről. Ha egy tagállam úgy dönt, hogy CSIRT-jei nem kapják meg az említett bejelentéseket, a CSIRT-eknek a feladataik ellátásához szükséges mértékben hozzáférést kell biztosítani az alapvető vagy fontos szervezetek által a 20. cikknek megfelelően bejelentett eseményekre vonatkozó adatokhoz.
- (3) Minden tagállam biztosítja, hogy illetékes hatóságai vagy CSIRT-jei tájékoztassák az egyedüli kapcsolattartó pontját az ezen irányelv alapján bejelentett eseményekről, jelentős kiberfenyegetésekről és majdnem bekövetkezett (near miss) eseményekről.
- (4) Az ebben az irányelvben meghatározott feladatok és kötelezettségek eredményes végrehajtásához szükséges mértékben a tagállamok biztosítják a megfelelő együttműködést az illetékes hatóságok, az egyedüli kapcsolattartó pontok és a bűnüldöző hatóságok, az adatvédelmi hatóságok és a kritikus infrastruktúráért az (EU) XXXX/XXXX irányelv (A kritikus szervezetek rezilienciájáról szóló irányelv) szerint felelős hatóságok, és az XXXX/XXXX/EU európai parlamenti és tanácsi rendeletnek³⁹ (a DORA rendelet) megfelelően kijelölt nemzeti pénzügyi hatóságok között az adott tagállamon belül.
- (5) A tagállamok biztosítják, hogy illetékes hatóságaik rendszeresen tájékoztatást nyújtsanak a(z) (EU) XXXX/XXXX irányelv (a kritikus szervezetek rezilienciájáról szóló irányelv) alapján kijelölt illetékes hatóságok számára a kritikusként azonosított alapvető szervezeteket vagy az (EU) XXXX/XXXX irányelv [A kritikus szervezetek rezilienciájáról szóló irányelv] szerint azokkal egyenértékű szervezeteket érintő kiberbiztonsági kockázatokról, a kiberfenyegetésekről és eseményekről, valamint az illetékes hatóságok által e kockázatokra és események elhárítására hozott intézkedésekről.

III. FEJEZET

³⁹

[illessze be a teljes címet és a HL-kiadvány hivatkozását, amikor ismertté válik].

12. cikk

Együttműködési csoport

- (1) Az irányelv alkalmazási körében a tagállamok közötti stratégiai együttműködés és információmegosztás támogatása és megkönnyítése érdekében együttműködési csoportot hoznak létre.
- (2) Az együttműködési csoport feladatait a (6) 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 (ESA-k) az (EU) XXXX/XXXX rendelet (a DORA-rendelet) 17. cikke (5) bekezdésének c) pontjával összhangban részt vehetnek az együttműködési csoport tevékenységeiben.

Adott esetben az együttműködési csoport meghívhatja az érdekelt felek képviselőit, hogy vegyenek részt munkájában.

A Bizottság biztosítja a titkárságot.

- (4) Az együttműködési csoport a következő feladatokat látja el:
 - a) útmutatás nyújtása az illetékes hatóságok számára ezen irányelv átültetésével és végrehajtásával kapcsolatban;
 - b) az ezen irányelv végrehajtásával kapcsolatos bevált gyakorlatok és információk cseréje, ideértve a kiberfenyegetéseket, az eseményeket, a biztonsági réseket, a majdnem bekövetkezett (near miss) eseményeket, a figyelemfelkeltő kezdeményezéseket, képzéseket, gyakorlatokat és készségeket, a kapacitásépítést, valamint a szabványokat és a műszaki előírásokat;
 - c) tanácsadás és együttműködés a Bizottsággal a kialakítás alatt álló kiberbiztonsági politikai kezdeményezésekkel kapcsolatban;
 - d) tanácsadás és együttműködés a Bizottsággal az ezen irányelv alapján elfogadott bizottsági végrehajtási vagy felhatalmazáson alapuló jogi aktusok tervezetével kapcsolatban;
 - e) bevált gyakorlatok és információk cseréje az érintett uniós intézményekkel, szervekkel, hivatalokkal és ügynökségekkel;
 - f) a 16. cikk (7) bekezdésében említett szakértői értékelésről szóló jelentések megvitatása;
 - g) a 34. cikkben említett, határokon átnyúló esetekben végzett közös felügyeleti tevékenységek eredményeinek megvitatása;
 - h) stratégiai útmutatás nyújtása a CSIRT-hálózat számára konkrét felmerülő kérdésekben;
 - i) hozzájárulás a kiberbiztonsági képességekhez az egész Unióban a nemzeti tisztviselők cseréjének megkönnyítésével a tagállamok illetékes hatóságai vagy CSIRT-ek munkatársait bevonó kapacitásépítő program révén;

- j) rendszeres közös megbeszélések szervezése az érintett magánérdekeltekkel az Unió egész területén, hogy megvitassák a csoport által végzett tevékenységeket, és információkat gyűjtsenek a felmerülő politikai kihívásokról;
 - k) a kiberbiztonsági gyakorlatokkal kapcsolatban vállalt munka megbeszélése, ideértve az ENISA által végzett munkát is.
- (5) Az együttműködési csoport műszaki jelentést kérhet a CSIRT hálózattól a kiválasztott témákról.
 - (6) Az együttműködési csoport-ig [24 hónappal ezen irányelv hatálybalépését követően], és ezt követően kétévente munkaprogramot készít az általa kitűzött célok és feladatok végrehajtása érdekében meghozandó intézkedésekre vonatkozóan. Az ezen irányelv alapján elfogadott első program időkeretét össze kell hangolni az (EU) 2016/1148 irányelv alapján elfogadott legutóbbi program időkeretével.
 - (7) A Bizottság végrehajtási jogi aktusokat fogadhat el, amelyek meghatározzák az együttműködési csoport működéséhez szükséges eljárási szabályokat. Ezeket a végrehajtási jogi aktusokat a 37. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.
 - (8) Az együttműködési csoport rendszeresen és évente legalább egy alkalommal ülésezik az (EU) XXXX/XXXX irányelv (a kritikus szervezetek rezilienciájáról szóló irányelv) alapján létrehozott, a kritikus szervezetek rezilienciájával foglalkozó csoporttal stratégiai együttműködés és az információmegosztás előmozdítása érdekében.

13. cikk

CSIRT-hálózat

- (1) A bizalom fejlődéséhez való hozzájárulás és a tagállamok közötti gyors és hatékony operatív együttműködés előmozdítása érdekében létrehozzák a nemzeti CSIRT-ek hálózatát.
- (2) A CSIRT-hálózat a tagállami CSIRT-ek és a CERT – EU képviselőiből áll. A Bizottság megfigyelőként vesz részt a CSIRT-hálózatban. Az ENISA biztosítja a titkárságot, és aktívan támogatja a CSIRT-ek közötti együttműködést.
- (3) A CSIRT-hálózat a következő feladatokat látja el:
 - a) információmegosztás a CSIRT-ek képességeiről;
 - b) releváns információk cseréje az eseményekről, a majdnem bekövetkezett (near miss) eseményekről, a kiberfenyegetésekről, a kockázatokról és a biztonsági résekről;
 - c) a CSIRT-hálózat esemény által potenciálisan érintett képviselőjének kérésére információmegosztás és -megbeszélés az eseményről és a kapcsolódó kiberfenyegetésekről, kockázatokról és biztonsági résekről;
 - d) a CSIRT-hálózat képviselőjének kérésére az adott tagállam joghatósága alatt azonosított eseményre vonatkozó összehangolt válasz megvitatása és lehetőség szerint végrehajtása;

- e) támogatás nyújtása a tagállamoknak a határokon átnyúló események ezen irányelv szerinti kezelése érdekében;
 - f) együttműködés és segítségnyújtás a 6. cikkben említett kijelölt CSIRT-ek számára a több felet érintő biztonsági rés összehangolt közzététele tekintetében a különböző tagállamokban létrehozott IKT-termékek, IKT-szolgáltatások és IKT-folyamatok több gyártóját vagy szolgáltatóját érintő biztonsági rések esetében;
 - g) az operatív együttműködés további formáinak megvitatása és meghatározása, beleértve a következőket:
 - i. a kiberfenyegetések és események kategóriái;
 - ii. korai figyelmeztetések;
 - iii. kölcsönös segítségnyújtás;
 - iv. a határokon átnyúló kockázatok és események elhárítása koordinálásának elvei és módozatai;
 - v. hozzájárulás a 7. cikk (3) bekezdésében említett nemzeti kiberbiztonsági eseményekhez és válságelhárítási tervhez;
 - h) az együttműködési csoport tájékoztatása tevékenységeiről és a g) pont szerint megvitatott operatív együttműködés további formáiról, szükség esetén útmutatás kérése ezzel kapcsolatban;
 - i) a kiberbiztonsági gyakorlatok számbavétele, beleértve az ENISA által szervezetteket is;
 - j) valamely CSIRT kérésére a CSIRT képességeinek és felkészültségének megvitatása;
 - k) együttműködés és információmegosztás a regionális és uniós szintű biztonsági műveleti központokkal (SOC) annak érdekében, hogy az egész Unióban javuljon az eseményekkel és fenyegetésekkel kapcsolatos közös helyzetismeret;
 - l) a 16. cikk (7) bekezdésében említett szakértői értékelési jelentések megvitatása;
 - m) iránymutatások kiadása az operatív gyakorlatok konvergenciájának megkönnyítése érdekében e cikk operatív együttműködésre vonatkozó rendelkezéseinek alkalmazása tekintetében.
- (4) A CSIRT-hálózat a 35. cikkben említett felülvizsgálat céljából és-ig [24 hónappal ezen irányelv hatálybalépését követően], majd ezt követően kétévente értékeli az operatív együttműködés terén elért előrehaladást és jelentést készít. A jelentés következtetéseket von le különösen a 16. cikkben említett, a nemzeti CSIRT-ekkel kapcsolatban végzett szakértői értékelések eredményeiről, beleértve az e cikk alapján követett következtetéseket és ajánlásokat. Ezt a jelentést az együttműködési csoportnak is be kell nyújtani.
- (5) A CSIRT elfogadja saját eljárási szabályzatát.

14. cikk

Az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (EU-CyCLONe)

- (1) A nagyszabású kiberbiztonsági események és válságok operatív szintű összehangolt kezelésének támogatása, valamint a tagállamok és az uniós intézmények, szervek és ügynökségek közötti rendszeres információmegosztás biztosítása érdekében ezennel létrejön az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (EU-CyCLONe).
- (2) Az EU-CyCLONe a tagállamok válságkezeléssel foglalkozó hatóságainak a 7. cikkel összhangban kijelölt képviselőiből, a Bizottságból és az ENISA-ból áll. Az ENISA biztosítja a hálózat titkárságát és támogatja a biztonságos információmegosztást.
- (3) Az EU-CyCLONe a következő feladatokat látja el:
 - a) a nagyszabású események és válságok kezelésére való felkészültség növelése;
 - b) a releváns kiberbiztonsági események közös helyzetismeretének fejlesztése;
 - c) a nagyszabású események és a válságkezelés összehangolása és az említett eseményekkel és válságokkal kapcsolatos politikai döntéshozatal támogatása;
 - d) a nemzeti kiberbiztonsági események és a 7. cikk (2) bekezdésében említett válságelhárítási tervek megvitatása.
- (4) Az EU-CyCLONe elfogadja eljárási szabályzatát.
- (5) Az EU-CyCLONe rendszeresen jelentést tesz az együttműködési csoportnak a kiberfenyegetésekkel, eseményekkel és trendekkel kapcsolatban, különös tekintettel az alapvető és fontos szervezetekre gyakorolt hatásukra.
- (6) Az EU-CyCLONe együttműködik a CSIRT-hálózattal egyeztetett eljárási szabályok alapján.

15. cikk

Jelentés az uniós kiberbiztonsági helyzetről

- (1) Az ENISA a Bizottsággal együttműködve kétéves jelentést ad ki az Unió kiberbiztonságának helyzetéről. A jelentés különösen a következők értékelését tartalmazza:
 - a) a kiberbiztonsági képességek fejlesztése az egész Unióban;
 - b) az illetékes hatóságok rendelkezésére álló technikai, pénzügyi és humán erőforrások, kiberbiztonsági politikák, valamint a felügyeleti és végrehajtási intézkedések végrehajtása a 16. cikkben említett szakértői értékelések eredményeire figyelemmel;
 - c) kiberbiztonsági index, amely a kiberbiztonsági képességek kiforrottságának összesített értékelését biztosítja.
- (2) A jelentésnek tartalmaznia kell konkrét szakpolitikai ajánlásokat a kiberbiztonság szintjének növelésére az Unió egész területén, valamint az Ügynökség adott időszakra vonatkozó megállapításainak összefoglalását az ENISA által az (EU) 2019/881 rendelet 7. cikkének (6) bekezdésével összhangban kiadott uniós kiberbiztonsági technikai helyzetjelentésekből.

16. cikk

Szakértői értékelés

- (1) A Bizottság az együttműködési csoporttal és az ENISA-val folytatott konzultációt követően, legkésőbb ezen irányelv hatálybalépésétől számított 18 hónapon belül meghatározza a tagállamok kiberbiztonsági politikája hatékonyságának értékelésére szolgáló szakértői értékelési rendszer módszertanát és tartalmát. Az értékelt tagállamtól eltérő tagállamokból érkező kiberbiztonsági technikai szakértők által végzett értékelések legalább a következőkre terjednek ki:
 - i. a 18. és 20. cikkben említett kiberbiztonsági kockázatkezelési követelmények és jelentéstételi kötelezettségek végrehajtásának hatékonysága;
 - ii. a képességek szintje, ideértve a rendelkezésre álló pénzügyi, technikai és humán erőforrásokat, valamint az illetékes nemzeti hatóságok feladatai ellátásának hatékonyságát;
 - iii. a CSIRT-ek műveleti képességei és hatékonysága;
 - iv. a 34. cikkben említett kölcsönös segítségnyújtás hatékonysága;
 - v. az ezen irányelv 26. cikkében említett információmegosztási keret hatékonysága.
- (2) A módszertannak objektív, megkülönböztetéstől mentes, igazságos és átlátható kritériumokat kell tartalmaznia, amelyek alapján a tagállamok kijelölik a szakértői értékelések elvégzésére jogosult szakértőket. Az ENISA és a Bizottság szakértőket jelöl ki, hogy megfigyelőként vegyenek részt a szakértői értékelésekben. A Bizottság az ENISA támogatásával az (1) bekezdésben említett módszertanon belül objektív, megkülönböztetéstől mentes, igazságos és átlátható rendszert hoz létre a szakértők kiválasztására és véletlenszerű kijelölésére az egyes szakértői értékelésekhez.
- (3) A szakértői értékelések szervezési szempontjairól a Bizottság dönt az ENISA támogatásával, és az együttműködési csoporttal folytatott konzultációt követően, és ezeknek az (1) bekezdésben említett módszertanban meghatározott kritériumokon kell alapulniuk. A szakértői értékelések során fel kell mérni az (1) bekezdésben említett szempontokat valamennyi tagállam és ágazat tekintetében, ideértve az egy vagy több tagállamra, vagy egy vagy több ágazatra jellemző, célzott kérdéseket is.
- (4) A szakértői értékeléseknek részét képezik tényleges vagy virtuális helyszíni látogatások és helyszínen kívüli találkozók. A jó együttműködés elvének figyelembevételével az értékelés alatt álló tagállamok a kijelölt szakértőknek megadják az értékelés alá vont szempontok értékeléséhez szükséges, kért információkat. A szakértői értékelési eljárás során kapott információkat kizárólag erre a célra szabad felhasználni. A szakértői értékelésben részt vevő szakértők semmilyen, az értékelés során kapott érzékeny vagy bizalmas információt nem közölhetnek harmadik személyekkel.
- (5) Egy adott tagállamban végzett szakértői értékelés lezárását követő két éven belül ugyanabban a tagállamban ugyanazokat a szempontokat nem lehet további szakértői értékelésnek alávetni, kivéve, ha a Bizottság másképp határoz az ENISA-val és az együttműködési csoporttal folytatott konzultációt követően.

- (6) A tagállamok biztosítják, hogy a kijelölt szakértőket érintő összeférhetlenség kockázatát indokolatlan késedelem nélkül feltárják a többi tagállam, a Bizottság és az ENISA számára.
- (7) A szakértői értékelésekben részt vevő szakértők jelentést készítenek az értékelések eredményeiről és következtetéseiről. A jelentéseket a Bizottságnak, az együttműködési csoportnak, a CSIRT-hálózatnak és az ENISA-nak kell benyújtani. A jelentéseket az együttműködési csoportban és a CSIRT-hálózaton belül vitatják meg. A jelentések közzétehetőek az együttműködési csoport erre a célra létrehozott weboldalán.

IV. FEJEZET

Kiberbiztonsági kockázatkezelési és jelentési kötelezettségek

I. SZAKASZ

Kiberbiztonsági kockázatkezelés és jelentéskészítés

17. cikk

Irányítás

- (1) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek vezető testületei jóváhagyják az e szervezetek által a 18. cikknek való megfelelés érdekében tett kiberbiztonsági kockázatkezelési intézkedéseket, felügyelik annak végrehajtását és elszámoltathatók legyenek a szervezetek által az e cikk szerinti kötelezettségek be nem tartásáért.
- (2) A tagállamok biztosítják, hogy az irányító testület tagjai rendszeresen speciális képzéseken vegyenek részt a kiberbiztonsági kockázatok és irányítási gyakorlatok, valamint azoknak a szervezet működésére gyakorolt hatása felderítéséhez és értékeléséhez elegendő ismeretek és készségek elsajátítása érdekében.

18. cikk

Kiberbiztonsági kockázatkezelési intézkedések

- (1) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek megfelelő és arányos technikai és szervezési intézkedéseket hozzanak annak a hálózati és információs rendszer biztonságára keltett kockázatok kezelésére, amelyeket e szervezetek a szolgáltatásaik nyújtása során használnak. Figyelembe véve a technika állását, ezeknek az intézkedéseknek biztosítaniuk kell a hálózati és információs rendszerek keltett kockázatnak megfelelő biztonsági szintjét.
- (2) Az (1) bekezdésben előírt jelentésnek legalább a következőket kell tartalmaznia:
- a) kockázatelemzés és az informatikai rendszerek biztonsági politikája;
 - b) eseménykezelés (megelőzés, felderítés és az események elhárítása);

- c) üzletmenet-folytonosság és válságkezelés;
 - d) az ellátási lánc biztonsága, ideértve az egyes szervezetek és beszállítóik vagy szolgáltatóik, például adattárolási és -feldolgozási szolgáltatások vagy felügyelt biztonsági szolgáltatások közötti kapcsolatok biztonságával kapcsolatos szempontokat;
 - e) biztonság a hálózati és információs rendszerek beszerzésében, fejlesztésében és karbantartásában, beleértve a biztonsági részek kezelését és közzétételét;
 - f) politikák és eljárások (tesztelés és ellenőrzés) a kiberbiztonsági kockázatkezelési intézkedések hatékonyságának értékelésére;
 - g) a rejtjelezés és a titkosítás használata.
- (3) A tagállamok biztosítják, hogy a (2) bekezdés d) pontjában említett megfelelő intézkedések mérlegelésekor a szervezetek figyelembe vegyék az egyes beszállítókra és szolgáltatókra jellemző biztonsági részeket, valamint a termékek általános minőségét, valamint beszállítóik és szolgáltatóik kiberbiztonsági gyakorlatát, beleértve a biztonságos fejlesztési eljárásaikat is.
- (4) A tagállamok biztosítják, hogy ha egy szervezet megállapítja, hogy szolgáltatásai vagy feladatai nem felelnek meg a (2) bekezdésben megállapított követelményeknek, indokolatlan késedelem nélkül megtegyen minden szükséges korrekciós intézkedést az érintett szolgáltatás megfelelőségének biztosítása érdekében.
- (5) A Bizottság végrehajtási jogi aktusokat fogadhat el a (2) bekezdésben említett elemek műszaki és módszertani előírásinak meghatározása érdekében. E jogi aktusok előkészítése során a Bizottság a 37. cikk (2) bekezdésében említett vizsgálóbizottsági eljárásnak megfelelően jár el, és a lehető legnagyobb mértékben követi a nemzetközi és európai szabványokat, valamint a vonatkozó műszaki előírásokat.
- (6) A Bizottság felhatalmazást kap arra, hogy a 36. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el a (2) bekezdésben megállapított elemek kiegészítésére az új kiberfenyegetések, a technológiai fejlődés vagy az ágazati sajátosságok figyelembevétele érdekében.

19. cikk

A kritikus ellátási láncok uniós koordinált kockázatértékelése

- (1) Az együttműködési csoport a Bizottsággal és az ENISA-val együttműködve összehangolt biztonsági kockázatértékeléseket végezhet a kritikus IKT-szolgáltatások, -rendszerek vagy -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 folytatott konzultációt követően meghatározza azokat a kritikus IKT-szolgáltatásokat, -rendszereket vagy -termékeket, amelyekre az (1) bekezdésben említett összehangolt kockázatértékelés vonatkozhat.

Jelentéstételi kötelezettségek

- (1) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek indokolatlan késedelem nélkül értesítsék az illetékes hatóságokat vagy a CSIRT-et a (3) és (4) bekezdéssel összhangban minden olyan eseményről, amely jelentős hatással van szolgáltatásaik nyújtására. Adott esetben ezek a szervezetek indokolatlan késedelem nélkül értesítik a szolgáltatásaikat igénybe vevőket azon eseményekről, amelyek valószínűleg hátrányosan érintik a szolgáltatás nyújtását. A tagállamok biztosítják, hogy ezek a szervezetek jelentsenek többek között minden olyan információt, amely lehetővé teszi az illetékes hatóságok vagy a CSIRT számára, hogy meghatározzák az esemény határokon átnyúló hatásait.
- (2) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek indokolatlan késedelem nélkül értesítsék az illetékes hatóságokat vagy a CSIRT-et minden olyan jelentős kiberfenyegetésről, amelyet e szervezetek azonosítanak, és amely potenciálisan jelentős eseményhez vezethetett.

Adott esetben ezek a szervezetek indokolatlan késedelem nélkül értesítik szolgáltatásaik jelentős kiberfenyegetéssel esetlegesen érintett igénybe vevőit azokról az intézkedésekről vagy jogorvoslatokról, amelyeket e címzettek a fenyegetés elhárítására megtehetnek. Adott esetben a szervezetek az igénybe vevőket magukról a fenyegetésekről is értesítik. A bejelentés következtében a bejelentő szervezetet többletfelelősség nem terhelheti.
- (3) Az esemény akkor tekinthető jelentősnek, ha:
 - a) az esemény jelentős működési zavart vagy pénzügyi veszteséget okozott vagy okozhat az érintett szervezet számára;
 - b) az esemény jelentős vagyoni vagy nem vagyoni veszteségek révén más természetes vagy jogi személyeket érintett vagy képes érinteni.
- (4) A tagállamok biztosítják, hogy az (1) bekezdés szerinti bejelentés céljából az érintett szervezetek benyújtanak az illetékes hatóságoknak vagy a CSIRT-nek:
 - a) egy első bejelentést, indokolatlan késedelem nélkül és minden esetben az esemény tudomására jutásától számított 24 órán belül, amelyben adott esetben fel kell tüntetni, hogy az eseményt vélhetően jogellenes vagy rosszindulatú cselekmény okozta-e;
 - b) az illetékes hatóság vagy a CSIRT kérésére közbenső jelentés a vonatkozó állapotfrissítésekről;
 - c) zárójelentés legkésőbb az a) pont szerinti jelentés benyújtását követő egy hónapon belül, amely tartalmazza legalább a következőket:
 - i. az esemény, annak súlyossága és hatása részletes leírása;
 - ii. az eseményt valószínűleg kiváltó fenyegetés vagy kiváltó ok típusa;
 - iii. alkalmazott és folyamatban lévő mérséklési intézkedések.

A tagállamok előírják, hogy kellően indokolt esetekben és az illetékes hatóságokkal vagy a CSIRT-tel egyetértésben az érintett szervezet eltérhet az a) és c) pontban meghatározott határidőktől.
- (5) Az illetékes nemzeti hatóságok vagy a CSIRT a (4) bekezdés a) pontjában említett első bejelentés kézhezvételétől számított 24 órán belül választ ad a bejelentő

szervezetnek, ideértve az eseményről szóló első visszajelzést, és a szervezet kérésére, útmutatást a lehetséges mérséklési intézkedések végrehajtásáról. Ha a CSIRT nem kapta meg az (1) bekezdésben említett bejelentést, az útmutatást az illetékes hatóság a CSIRT-tel együttműködve nyújtja. A CSIRT további technikai támogatást nyújt, ha az érintett szervezet ezt kéri. Ha az eseménnyel kapcsolatban bűncselekmény gyanúja felmerül, az illetékes nemzeti hatóságok vagy a CSIRT útmutatást ad az esemény bűnüldöző hatóságoknak történő bejelentésére vonatkozóan is.

- (6) Adott esetben, és különösen, ha az (1) bekezdésben említett esemény két vagy több tagállamot érint, az illetékes hatóság vagy a CSIRT tájékoztatja az eseményről a többi érintett tagállamot és az ENISA-t. Ennek során az illetékes hatóságoknak, a CSIRT-eknek és az egyedüli kapcsolattartó pontoknak az uniós joggal vagy az uniós jognak megfelelő nemzeti jogszabályokkal összhangban meg kell őrizniük a szervezet biztonsági és kereskedelmi érdekeit, valamint a nyújtott információk titkosságát.
- (7) Ha az esemény megelőzéséhez vagy egy folyamatban lévő esemény kezeléséhez lakossági tudatosítás szükséges, vagy ha az esemény nyilvánosságra hozatala egyébként közérdek, az illetékes hatóság vagy a CSIRT, és adott esetben a többi érintett tagállam hatóságai vagy CSIRT-je az érintett szervezettel folytatott konzultációt követően tájékoztathatja a nyilvánosságot az eseményről, vagy ezt megkövetelheti a szervezettől.
- (8) Az illetékes hatóság vagy a CSIRT kérésére az egyedüli kapcsolattartó pont az (1) és (2) bekezdés alapján kapott bejelentéseket továbbítja a többi érintett tagállam egyedüli kapcsolattartó pontjának.
- (9) Az egyedüli kapcsolattartó pont havonta összefoglaló jelentést nyújt be az ENISA-nak, amely névtelen és összesített adatokat tartalmaz az (1) és (2) bekezdéssel, valamint a 27. cikkkel összhangban bejelentett eseményekről, jelentős kiberfenyegetésekről és majdnem bekövetkezett (near miss) eseményekről. Az összehasonlítható információk szolgáltatásához való hozzájárulás érdekében az ENISA technikai útmutatást adhat ki az összefoglaló jelentésben szereplő információk paramétereiről.
- (10) Az illetékes hatóságok információt nyújtanak az (EU) XXXX/XXXX irányelv (A kritikus szervezetek rezilienciájáról szóló irányelv) alapján kijelölt illetékes hatóságoknak a kritikus szervezetként vagy az (EU) XXXX/XXXX irányelv (A kritikus szervezetek rezilienciájáról szóló irányelv) alapján a kritikus szervezetekkel egyenértékű szervezetként azonosított alapvető szervezetek által az (1) és (2) bekezdéssel összhangban bejelentett eseményekről és kiberfenyegetésekről.
- (11) A Bizottság végrehajtási jogi aktusokat fogadhat el, amelyek meghatározzák az (1) és (2) bekezdés alapján benyújtott bejelentés típusát, formátumát és eljárását. A Bizottság végrehajtási jogi aktusokat is elfogadhat azoknak az eseteknek a pontos meghatározása érdekében, amelyekben egy eseményt a (3) bekezdésben említettek szerint jelentősnek kell tekinteni. Ezeket a végrehajtási jogi aktusokat a 37. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

21. cikk

Az európai kiberbiztonsági tanúsítási rendszerek használata

- (1) A 18. cikk egyes követelményeinek való megfelelés igazolása érdekében a tagállamok megkövetelhetik az alapvető és fontos szervezetektől, hogy tanúsítsanak bizonyos IKT-termékeket, IKT-szolgáltatásokat és IKT-folyamatokat az (EU) 2019/881 rendelet 49. cikke alapján elfogadott európai kiberbiztonsági tanúsítási rendszerek keretében. A tanúsítás tárgyát képező termékeket, szolgáltatásokat és folyamatokat egy alapvető vagy fontos szervezet fejlesztheti, vagy azok beszerezhetők harmadik felektől.
- (2) A Bizottság felhatalmazást kap felhatalmazáson alapuló jogi aktusok elfogadására, amelyek meghatározzák, hogy az alapvető szervezetek mely kategóriái kötelesek tanúsítványt szerezni, és az (1) bekezdés szerinti mely konkrét európai kiberbiztonsági tanúsítási rendszerek alapján. A felhatalmazáson alapuló jogi aktusokat a 36. cikkel összhangban kell elfogadni.
- (3) A Bizottság felkérheti az ENISA-t, hogy készítse egy javasolt tanúsítási rendszert az (EU) 2019/881 rendelet 48. cikkének (2) bekezdése alapján azokban az esetekben, amikor a (2) bekezdés alkalmazásában nincs megfelelő európai kiberbiztonsági tanúsítási rendszer.

22. cikk

Szabványosítás

- (1) A 18. 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 vagy nemzetközileg elfogadott szabványok és előírások alkalmazását.
- (2) Az ENISA a tagállamokkal együttműködve tanácsokat és iránymutatásokat dolgoz ki az (1) bekezdéssel összefüggésben mérlegelendő technikai területekről, valamint a már meglévő szabványokról – beleértve a tagállamok nemzeti szabványait is – amelyek lehetővé tennék e területek lefedését.

23. cikk

Doménnevek és nyilvántartási adatok adatbázisai

- (1) A DNS biztonságához, stabilitásához és rezilienciájához való hozzájárulás céljából a tagállamok biztosítják, hogy a legfelső szintű doménnév-nyilvántartók és a TLD-hez doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek a személyes adatnak minősülő adatok tekintetében az uniós adatvédelmi jogszabályoknak megfelelően kellő gondossággal, egy erre kijelölt adatbázis-létesítményben gyűjtsék és gondozzák a pontos és teljes doménnév-nyilvántartási adatokat.
- (2) A tagállamok biztosítják, hogy az (1) bekezdésben említett doménnév-nyilvántartási adatok adatbázisai tartalmazzák a releváns információkat a doménnevek tulajdonosai és a TLD-k alatt bejegyzett doménneveket kezelő kapcsolattartó pontok azonosításához és a velük való kapcsolatfelvételhez.
- (3) A tagállamok biztosítják, hogy a legfelső szintű doménnév-nyilvántartók és a TLD-hez doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek rendelkezzenek szabályzatokkal és eljárásokkal annak biztosítására, hogy az adatbázisok pontos és

teljes információkat tartalmazzanak. A tagállamok biztosítják, hogy az említett szabályzatokat és eljárásokat nyilvánosan hozzáférhetővé tegyék.

- (4) A tagállamok biztosítják, hogy a legfelső szintű doménnév-nyilvántartók és a TLD-hez doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek a doménnév-nyilvántartásba vétele után indokolatlan késedelem nélkül közzétegyék azokat a domén-nyilvántartási adatokat, amelyek nem személyes adatok.
- (5) A tagállamok biztosítják, hogy a legfelső szintű doménnév-nyilvántartók és a TLD-hez doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek jogszerű és kellően indokolt kérésére az uniós adatvédelmi jogszabályokkal összhangban betekintést biztosítsanak meghatározott doménnév-nyilvántartási adatokba a jogosult hozzáférés-igénylők számára. A tagállamok biztosítják, hogy a legfelső szintű doménnév-nyilvántartók és a TLD-hez doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek indokolatlan késedelem nélkül megválaszoljanak minden hozzáférési kérelmet. A tagállamok biztosítják, hogy az említett adatok közzétételére vonatkozó szabályzatokat és eljárásokat nyilvánosan hozzáférhetővé tegyék.

II. szakasz

Joghatóság és nyilvántartás

24. cikk

Joghatóság és területi elv

- (1) A DNS-szolgáltatókat, a legfelső szintű doménnév-nyilvántartókat, a felhőszolgáltatókat, az adatközpont-szolgáltatókat és az I. melléklet 8. pontjában említett tartalomszolgáltató hálózati szolgáltatókat, valamint a II. melléklet 6. pontjában említett digitális szolgáltatókat annak a tagállamnak a joghatósága alá tartozónak kell tekinteni, amelyben az Unióban üzleti tevékenységük fő helye található.
- (2) Ezen irányelv alkalmazásában úgy kell tekinteni, hogy az (1) bekezdésben említett szervezetek üzleti tevékenységének fő helye az Unióban abban a tagállamban van, ahol a kiberbiztonsági kockázatkezelési intézkedésekkel kapcsolatos döntéseket hozzák. Ha ilyen döntéseket az Unióban egyetlen telephelyen sem hoznak, akkor az üzleti tevékenység fő helyét abban a tagállamban levőnek kell tekinteni, ahol a szervezeteknek az Unióban a legmagasabb munkavállalói létszámmal rendelkező telephelyük van.
- (3) Ha az (1) bekezdésben említett szervezet székhelye nem az Unióban van, 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 említett szervezetet a képviselő letelepedése szerinti tagállam joghatósága alá tartozónak kell tekinteni. E cikk alapján az Unióban kijelölt képviselő hiányában bármely olyan tagállam, amelyben a szervezet szolgáltatást nyújt, jogi lépéseket tehet a szervezet ellen az ezen irányelvből eredő kötelezettségek be nem tartása miatt.
- (4) A képviselő (1) bekezdésben említett szervezet általi kijelölése nem érinti azokat a jogi lépéseket, amelyek maga a szervezet ellen kezdeményezhetők.

Az alapvető és fontos szervezetek nyilvántartása

- (1) Az ENISA nyilvántartást hoz létre és vezet a 24. cikk (1) bekezdésében említett alapvető és fontos szervezetekről. A szervezeteknek a következő információkat kell benyújtaniuk az ENISA-nak [legkésőbb az irányelv hatálybalépésétől számított 12 hónapon belül]:
 - a) a szervezet neve;
 - b) üzleti tevékenysége fő helyének és egyéb Unión belüli jogszerű telephelyének, vagy ha az Unióban nem letelepedett, a 24. cikk (3) bekezdése szerint kijelölt képviselőjének a címe;
 - c) naprakész kapcsolattartási adatok, beleértve a szervezetek e-mail-címét és telefonszámát.
- (2) Az (1) bekezdésben említett szervezetek haladéktalanul, de minden esetben a változás hatálybalépésétől számított három hónapon belül értesítik az ENISA-t az (1) bekezdés alapján benyújtott adatok minden változásáról.
- (3) Az (1) bekezdés szerinti információk kézhezvétele után az ENISA továbbítja azokat az egyedüli kapcsolattartó pontoknak, az egyes szervezetek üzleti tevékenysége fő helyétől, vagy ha az Unióban nem letelepedett, kijelölt képviselőjének megjelölt helyétől függően. Ha az (1) bekezdésben említett szervezetnek az unióbeli üzleti tevékenység fő helyén kívül további telephelyei vannak más tagállamokban, az ENISA tájékoztatja ezen tagállamok egyedüli kapcsolattartó pontját is.
- (4) Ha a szervezet nem veteti nyilvántartásba tevékenységét vagy nem nyújtja be a vonatkozó információkat az (1) bekezdésben meghatározott határidőn belül, bármely tagállam, ahol a szervezet szolgáltatást nyújt, illetékes annak biztosítására, hogy a szervezet betartsa az ezen irányelvben meghatározott kötelezettségeket.

V. FEJEZET

Információmegosztás

Kiberbiztonsági információmegosztási megállapodások

- (1) Az (EU) 2016/679 rendelet sérelme nélkül a tagállamok biztosítják, hogy az alapvető és fontos szervezetek megoszthassák egymással a vonatkozó kiberbiztonsági információkat, ideértve a kiberfenyegetésekre, a biztonsági résekre, a kompromisszummutatókra, a taktikákra, a technikákra és az eljárásokra, a kiberbiztonsági figyelmeztetésekre és a konfigurációs eszközökre vonatkozó információkat, amennyiben az említett információmegosztás:
 - a) célja az események megelőzése, felderítése, elhárítása vagy mérséklése;
 - b) növeli a kiberbiztonság szintjét, különösen azáltal, hogy felhívja a figyelmet a kiberfenyegetésekre, korlátozza vagy gátolja az említett fenyegetések terjedési képességét, támogatja a védelmi képességek széles skáláját, a biztonsági rés

elhárítását és nyilvánosságra hozatalát, a fenyegetésészlelési technikákat, a mérséklési stratégiákat vagy az elhárítási és helyreállítást szakaszt.

- (2) A tagállamok biztosítják, hogy az információmegosztás alapvető és fontos szervezetek megbízható közösségei között történjen. Az említett megosztást információmegosztás-megállapodások útján kell végrehajtani a megosztott információk potenciálisan érzékeny jellegét tiszteletben tartva, és az (1) bekezdésben említett uniós jogi szabályoknak megfelelően.
- (3) A tagállamok meghatározzák azokat a szabályokat, amelyek meghatározzák a (2) bekezdésben említett információmegosztási megállapodások eljárását, működési elemeit (ideértve a dedikált IKT-platformok használatát), tartalmát és feltételeit. Az említett szabályoknak tartalmazniuk kell a hatóságok részvételének részleteit az említett megállapodásokban, valamint az operatív elemeket, ideértve a dedikált informatikai platformok használatát is. A tagállamok támogatást nyújtanak az említett megállapodások alkalmazásához az 5. cikk (2) bekezdésének g) pontjában említett politikájukkal összhangban.
- (4) Az alapvető és fontos szervezetek az említett megállapodások megkötésekor értesítik az illetékes hatóságokat a (2) bekezdésben említett információmegosztási megállapodásokban való részvételükről, vagy adott esetben az említett megállapodások felmondásáról, a felmondás hatálybalépésekor.
- (5) Az uniós joggal összhangban az ENISA a bevált gyakorlatok és útmutatás nyújtásával támogatja a (2) bekezdésben említett kiberbiztonsági információmegosztási megállapodások létrehozását.

27. cikk

A releváns információk önkéntes bejelentése

A tagállamok biztosítják, hogy a 3. cikk sérelme nélkül az ezen irányelv hatályán kívül eső szervezetek önkéntes alapon bejelentést nyújthassanak be jelentős eseményekről, kiberfenyegetésekről vagy majdnem bekövetkezett (near miss) eseményekről. A bejelentések feldolgozása során a tagállamok a 20. cikkben megállapított eljárásnak megfelelően járnak el. A tagállamok előnyben részesíthetik a kötelező bejelentések feldolgozását az önkéntes bejelentésekkel szemben. Az önkéntes adatszolgáltatás nem eredményezhet az adatszolgáltatóra olyan további kötelezettségeket, amelyek nem vonatkoztak volna rá, ha nem nyújtja be a bejelentést.

VI. FEJEZET

Felügyelet és végrehajtás

28. cikk

A felügyelet és a végrehajtás általános szempontjai

- (1) A tagállamok biztosítják, hogy az illetékes hatóságok ténylegesen figyelemmel kísérik és megtegyék az ezen irányelvnek, különösen a 18. és 20. cikkben meghatározott kötelezettségeknek való megfelelés biztosításához szükséges intézkedéseket.

- (2) Az illetékes hatóságok szorosan együttműködnek az adatvédelmi hatóságokkal a személyes adatok megsértését eredményező események kezelése során.

29. cikk

Felügyelet és végrehajtás az alapvető szervezetek esetében

- (1) A tagállamok biztosítják, hogy az alapvető szervezetekre az ezen irányelvben meghatározott kötelezettségek teljesítése érdekében 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 az alábbiakat:
- a) helyszíni ellenőrzések és távoli ellenőrzés, ideértve a véletlenszerű ellenőrzéseket is;
 - b) rendszeres ellenőrzések;
 - c) célzott biztonsági auditok, a kockázatértékelések vagy a kockázattal kapcsolatban rendelkezésre álló információk alapján;
 - d) objektív, megkülönböztetéstől mentes, méltányos és átlátható kockázatértékelési kritériumokon alapuló biztonsági vizsgálatok;
 - e) a szervezet által elfogadott kiberbiztonsági intézkedések értékeléséhez szükséges tájékoztatás kérése, ideértve a dokumentált kiberbiztonsági politikákat, valamint az ENISA-nak a 25. cikk (1) és (2) bekezdése szerinti bejelentési kötelezettség betartását;
 - f) a felügyeleti feladataik ellátásához szükséges adatokhoz, dokumentumokhoz vagy bármilyen információhoz való hozzáférés iránti kérelem;
 - g) a kiberbiztonsági politikák végrehajtására vonatkozó bizonyítékok, például a minősített ellenőr által végzett biztonsági ellenőrzések eredményei és a vonatkozó mögöttes bizonyítékok iránti kérelmek.
- (3) A (2) bekezdés e) –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 hatóságok az alapvető szervezetekkel kapcsolatos végrehajtási hatáskörök gyakorlása során hatáskörrel rendelkezzenek az alábbiakra:
- a) figyelmeztetés kiadása, ha a szervezetek nem tartják be az ezen irányelvben meghatározott kötelezettségeket;
 - b) kötelező erejű utasítások vagy végzés kiadása, amelyek előírják az említett szervezetek számára, hogy orvosolják a feltárt hiányosságokat vagy az ezen irányelvben megállapított kötelezettségek megsértését;
 - c) a szervezetek kötelezése arra, hogy szüntessék meg az ebben az irányelvben meghatározott kötelezettségeknek meg nem felelő magatartást, és tartózkodjanak a magatartás ismételt elkövetésétől;

- d) a szervezetek kötelezése arra, hogy kockázatkezelési intézkedéseiket és/vagy jelentési kötelezettségeiket a 18. és 20. cikkben meghatározott kötelezettségeknek megfelelően, meghatározott módon és határidőn belül hozzák összhangba;
 - e) a szervezetek kötelezése arra, hogy tájékoztassák azon természetes vagy jogi személy(eke)t, akiknek szolgáltatásokat nyújtanak vagy tevékenységeket végeznek, és amelyeket a jelentős kiberfenyegetés érinthet, minden lehetséges védelmi vagy helyreállítási intézkedésről, amelyet e természetes vagy jogi személy(ek) megtehetnek a fenyegetés elhárítására;
 - f) a 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 a 18. és 20. cikkben előírt kötelezettségeik teljesítésének felügyeletére;
 - h) a szervezetek kötelezése arra, hogy az ezen irányelvben meghatározott kötelezettségek be nem tartásának szempontjait meghatározott módon hozzák nyilvánosságra;
 - i) nyilvános nyilatkozat megtétele, amely meghatározza az ebben az irányelvben meghatározott kötelezettségek megsértéséért felelős jogi és természetes személy(eke)t, valamint a jogsértés jellegét;
 - j) a 31. cikk szerinti közigazgatási bírság kiszabása vagy annak kérése az illetékes szervektől vagy bíróságoktól a nemzeti jogszabályok szerint, az e bekezdés a)–i) pontjában említett intézkedések mellett vagy azok helyett, a konkrét eset körülményeitől függően.
- (5) Ha a (4) bekezdés a)–d) és f) pontja alapján elfogadott végrehajtási intézkedések hatástalannak bizonyulnak, a tagállamok biztosítják, hogy az illetékes hatóságok jogosultak legyenek határidőt tűzni, amikor felkérlik az alapvető szervezetet a szükséges intézkedések a hiányosságok elhárítására vagy az említett hatóságok követelményeinek való megfelelésre. Ha a kért intézkedést a kitűzött határidőn belül nem hozzák meg, a tagállamok biztosítják, hogy az illetékes hatóságok hatáskörrel rendelkezzenek a következőkre:
- a) a tanúsítás vagy az engedély felfüggesztése egy alapvető szervezet által nyújtott szolgáltatások vagy tevékenységek egészére vagy egy részére vonatkozóan, vagy a tanúsító vagy engedélyező szervezet erre való felkérése;
 - b) az adott szervezetnél vezetői funkciók gyakorlásától ideiglenes eltiltás előírása vagy ennek kérése az illetékes szervektől vagy bíróságoktól a nemzeti jogszabályok szerint, az alapvető szervezet ügyvezető tisztségviselői vagy törvényes képviseleti szintű vezetői feladatokat ellátó személyek és a jogsértésért felelős bármely más természetes személy ellen.
- Ezeket a szankciókat csak addig kell alkalmazni, amíg a szervezet megteszi a szükséges intézkedéseket a hiányosságok elhárítására, vagy eleget tesz az illetékes hatóság azon követelményeinek, amelyre az említett szankciókat alkalmazták.
- (6) A tagállamok biztosítják, hogy minden alapvető szervezetért felelős vagy annak képviseletében képviseleti joga, a nevében történő döntéshozatal vagy az irányítás gyakorlásának joga alapján eljáró természetes személy hatáskörrel rendelkezzen az ezen irányelvben megállapított kötelezettségeknek való megfelelés biztosítására. A

tagállamok biztosítják, hogy ezeket a természetes személyeket felelősségre vonhassák az ezen irányelvben meghatározott kötelezettségek betartásának biztosítását szolgáló köteleességeik megsértéséért.

- (7) A végrehajtási intézkedések bármelyikének meghozatala vagy a (4) és (5) bekezdés szerinti szankciók alkalmazása esetén az illetékes hatóságoknak tiszteletben kell tartaniuk a védelemhez való jogot, és figyelembe kell venniük a konkrét esetek körülményeit, és legalább kellően figyelembe kell venniük az alábbiakat:
- a) a jogsértés súlyossága és a megsértett rendelkezések fontossága. A jogsértések közül súlyosnak tekintendők az alábbiak: ismételt jogsértések, jelentős bomlasztó hatású események bejelentésének vagy elhárításának elmaradása, a hiányosságok orvoslásának elmaradása az illetékes hatóságok kötelező erejű utasításait követően, a jogsértés megállapítását követően az illetékes hatóság által elrendelt ellenőrzések vagy ellenőrzési tevékenységek akadályozása, hamis vagy súlyosan pontatlan információk közlése a kockázatkezeléssel kapcsolatban a 18. és 20. cikkben meghatározott követelmények vagy jelentéstételi kötelezettségekkel kapcsolatban.
 - b) a jogsértés időtartama, ideértve az ismételt jogsértések elemét;
 - c) a ténylegesen okozott kár vagy a felmerült veszteségek, vagy a kiváltható lehetséges károk vagy veszteségek, amennyiben meghatározhatók. E szempont értékelésekor figyelembe kell venni többek között a tényleges vagy lehetséges pénzügyi vagy gazdasági veszteségeket, az egyéb szolgáltatásokra gyakorolt hatásokat, az érintett vagy potenciálisan érintett felhasználók számát;
 - d) a jogsértés szándékos vagy gondatlan jellege;
 - e) a szervezet által a kár és/vagy veszteség megelőzésére vagy enyhítésére tett intézkedések;
 - f) a jóváhagyott magatartási kódexek vagy jóváhagyott tanúsítási mechanizmusok betartása;
 - g) a felelősnek tartott természetes vagy jogi személy(ek) illetékes hatóságokkal való együttműködésének szintje.
- (8) Az illetékes hatóságok részletesen indokolják végrehajtási döntéseiket. Az említett döntések meghozatala előtt az illetékes hatóságok értesítik az érintett szervezeteket előzetes megállapításaikról, és észszerű időt biztosítanak az említett szervezetek számára észrevételek benyújtására.
- (9) A tagállamok biztosítják, hogy illetékes hatóságaik tájékoztassák az érintett tagállam (EU) XXXX/XXXX irányelv (a kritikus szervezetek rezilienciájáról szóló irányelv) alapján kijelölt érintett illetékes hatóságait, amennyiben gyakorolják azon felügyeleti és végrehajtási hatásköreiket, amelyek célja az ezen irányelv szerinti kötelezettségek egy kritikusként vagy az (EU) XXXX/XXXX irányelv (A kritikus szervezetek rezilienciájáról szóló irányelv) alapján a kritikus szervezettel egyenértékű szervezetként azonosított alapvető szervezet általi betartásának biztosítása. Az (EU) XXXX/XXXX irányelv (a kritikus szervezetek rezilienciájáról szóló irányelv) alapján illetékes hatóságok kérésére az illetékes hatóságok gyakorolhatják felügyeleti és végrehajtási hatásköreiket a kritikusnak vagy azzal egyenértékűnek nyilvánított alapvető szervezetek tekintetében.

Felügyelet és végrehajtás fontos szervezetek esetében

- (1) Ha bizonyítékokat vagy jelzést kapnak arról, hogy egy fontos szervezet nem teljesíti az ezen irányelvben és különösen a 18. és 20. cikkben meghatározott kötelezettségeket, a tagállamok biztosítják, hogy az illetékes hatóságok szükség esetén utólagos felügyeleti intézkedések révén intézkedjenek.
- (2) A tagállamok biztosítják, hogy az illetékes hatóságok a fontos szervezetekkel kapcsolatos felügyeleti feladataik ellátása során hatáskörrel rendelkezzenek arra, hogy ezeknél a szervezeteknél elvégezzék az alábbiakat:
 - a) utólagos helyszíni ellenőrzés és távoli ellenőrzés;
 - b) célzott biztonsági auditok, a kockázatértékelések vagy a kockázattal kapcsolatban rendelkezésre álló információk alapján;
 - c) objektív, igazságos és átlátható kockázatértékelési kritériumokon alapuló biztonsági vizsgálatok;
 - d) a kiberbiztonsági intézkedések utólagos értékeléséhez szükséges tájékoztatás kérése, ideértve a dokumentált kiberbiztonsági politikákat, valamint az ENISA-nak a 25. cikk (1) és (2) bekezdése szerint történő bejelentés kötelezettségének való megfelelést;
 - e) a felügyeleti feladatok ellátásához szükséges adatokhoz, dokumentumokhoz és/vagy információkhoz való hozzáférés iránti kérelmek.
- (3) Hatásköreik (2) bekezdés d) vagy e) 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 hatáskörük gyakorlásakor hatáskörrel rendelkezzenek a következőkre:
 - a) figyelmeztetés kiadása, ha a szervezetek nem tartják be az ezen irányelvben meghatározott kötelezettségeket;
 - b) kötelező erejű utasítások vagy végzés kiadása, amelyek előírják az említett szervezetek számára, hogy orvosolják a feltárt hiányosságokat vagy az ezen irányelvben megállapított kötelezettségek megsértését;
 - c) a szervezetek kötelezése arra, hogy szüntessék meg az ebben az irányelvben meghatározott kötelezettségeknek meg nem felelő magatartást, és tartózkodjanak a magatartás ismételt elkövetésétől;
 - d) a szervezetek kötelezése arra, hogy kockázatkezelési intézkedéseiket vagy jelentési kötelezettségeiket a 18. és 20. cikkben meghatározott kötelezettségeknek megfelelően, meghatározott módon és határidőn belül hozzák összhangba;
 - e) a szervezetek kötelezése arra, hogy tájékoztassák azon természetes vagy jogi személy(ek)e)t, akiknek szolgáltatásokat nyújtanak vagy tevékenységeket végeznek, és amelyeket a jelentős kiberfenyegetés érinthet, minden lehetséges védelmi vagy helyreállítási intézkedésről, amelyet e természetes vagy jogi személy(ek) megtehetnek a fenyegetés elhárítására;
 - f) a szervezetek kötelezése arra, hogy észszerű határidőn belül hajtsák végre a biztonsági ellenőrzés eredményeként adott ajánlásokat;

- g) a szervezetek kötelezése arra, hogy az ezen irányelvben meghatározott kötelezettségeik be nem tartásának szempontjait meghatározott módon hozzák nyilvánosságra;
 - h) nyilvános nyilatkozat megtétele, amely meghatározza az ebben az irányelvben meghatározott kötelezettségek megsértéséért felelős jogi és természetes személy(ek)e, valamint a jogsértés jellegét;
 - i) a 31. cikk szerinti közigazgatási bírság kiszabása vagy annak kérése az illetékes szervektől vagy bíróságoktól a nemzeti jogszabályok szerint, az e bekezdés a)–h) pontjában említett intézkedések mellett vagy azok helyett, a konkrét eset körülményeitől függően.
- (5) A 29. cikk (6)–(8) bekezdését alkalmazni kell az e cikkben a II. mellékletben felsorolt fontos szervezetekre vonatkozóan előírt felügyeleti és végrehajtási intézkedésekre is.

31. cikk

Közigazgatási bírság alapvető és fontos szervezetekre történő kiszabásának általános feltételei

- (1) A tagállamok biztosítják, hogy az ezen irányelvben megállapított kötelezettségek megsértése esetén az alapvető és fontos szervezetekre az e cikk szerint kiszabott adminisztratív bírságok minden esetben hatékonyak, arányosak és visszatartó erejűek legyenek.
- (2) Közigazgatási bírságot a konkrét esetek körülményeitől függően a 29. cikk (4) bekezdésének a)–i) pontjában, a 29. cikk (5) bekezdésében és a 30. cikk (4) bekezdésének a)–h) pontjában említett intézkedések mellett vagy helyett kell kiszabni.
- (3) A konkrét esetekben közigazgatási bírság kiszabásának és annak összegének eldöntésekor kellő figyelmet kell fordítani legalább a 29. cikk (7) bekezdésében előírt elemekre.
- (4) A tagállamok biztosítják, hogy a 18. vagy a 20. cikkben megállapított kötelezettségek megsértését e cikk (2) és (3) bekezdésével összhangban legalább 10 000 000 EUR vagy, ha ez magasabb, azon vállalkozás globális éves forgalma teljes összege 2 %-ának megfelelő maximális összegű közigazgatási bírsággal sújtsák, amelyhez az előző pénzügyi évben az alapvető vagy fontos szervezet tartozik.
- (5) A tagállamok rendelkezhetnek időszakos kényszerítő bírság kiszabásának hatásköréről annak érdekében, hogy egy alapvető vagy fontos szervezetet az illetékes hatóság korábbi határozatával összhangban a jogsértés megszüntetésére kényszerítsenek.
- (6) Az illetékes hatóságok 29. és 30. cikk szerinti hatáskörének sérelme nélkül minden tagállam meghatározhat szabályokat, hogy adminisztratív bírság kiszabható-e és milyen mértékben a 4. cikk 23. pontjában említett, az ezen irányelvben előírt kötelezettségek hatálya alatt álló közigazgatási szervekre.

32. cikk

A személyes adatok megsértésével járó jogsértések

- (1) Ha az illetékes hatóságoknak jelzik, hogy a 18. és 20. cikkben megállapított kötelezettségek lényeges vagy fontos szervezet általi megsértése személyes adatok megsértésével jár az (EU) 2016/679 rendelet 4. cikkének (12) bekezdésében meghatározottak szerint, amelyet az említett rendelet 33. cikke alapján be kell jelenteni, észszerű időn belül tájékoztatják az említett rendelet 55. és 56. cikke alapján illetékes felügyeleti hatóságokat.
- (2) Ha az (EU) 2016/679 rendelet 55. és 56. cikkével összhangban illetékes felügyeleti hatóságok úgy határoznak, hogy az említett rendelet 58. cikkének i. pontja alapján gyakorolják hatásköreiket és közigazgatási bírságot szabnak ki, az illetékes hatóságok ugyanazon jogsértés miatt nem szabhatnak ki közigazgatási bírságot ezen irányelv 31. cikke szerint. Az illetékes hatóságok azonban alkalmazhatnak végrehajtási intézkedéseket vagy gyakorolhatják az ezen irányelv 29. cikke (4) bekezdésének a)–i) pontjában, 29. cikke (5) bekezdésében és 30. cikke (4) bekezdésének a)–h) pontjában előírt szankcionálási hatásköröket.
- (3) Ha az (EU) 2016/679 rendelet alapján illetékes felügyeleti hatóság az illetékes hatóságtól eltérő tagállamban található, az illetékes hatóság tájékoztathatja az ugyanabban a tagállamban letelepedett felügyeleti hatóságot.

33. cikk

Szankciók

- (1) A tagállamok megállapítják az ezen irányelv alapján elfogadott nemzeti rendelkezések megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és megtesznek minden szükséges intézkedést azok végrehajtásának biztosítására. Az így elrendelt szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük.
- (2) A tagállamok ezen irányelv hatálybalépésétől számított [két] éven belül értesítik a Bizottságot ezekről a szabályokról és intézkedésekről, és indokolatlan késedelem nélkül értesítik a Bizottságot azok minden későbbi módosításáról.

34. cikk

Kölcsönös segítségnyújtás

- (1) Ha egy alapvető vagy fontos szervezet több tagállamban nyújt szolgáltatásokat, vagy ha üzleti tevékenységének fő helye vagy képviselője egy tagállamban van, de hálózatának és információs rendszerei egy vagy több másik tagállamban találhatóak, az üzleti tevékenység fő helye vagy más telephely vagy a képviselője tagállamának illetékes hatósága, valamint e többi tagállam 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 vele a megtett

felügyeleti és végrehajtási intézkedésekről és azok nyomon követéséről, a 29. és 30. cikkel összhangban;

- b) az illetékes hatóság felkérhet egy másik illetékes hatóságot a 29. és 30. cikkben említett felügyeleti vagy végrehajtási intézkedések megtételére;
 - c) az illetékes hatóság egy másik illetékes hatóságtól származó indokolt kérelem kézhezvétele után segítséget nyújt a másik illetékes hatóság számára annak érdekében, hogy a 29. és 30. cikkben említett felügyeleti vagy végrehajtási intézkedéseket hatékonyan, eredményesen és következetesen lehessen végrehajtani. az említett kölcsönös segítségnyújtás kiterjedhet a tájékoztatás kérésére és a felügyeleti intézkedésekre, ideértve a helyszíni ellenőrzések vagy a távoli felügyelet vagy célzott biztonsági ellenőrzések elvégzésére irányuló kéréseket is. Az az illetékes hatóság, amelyhez segítségnyújtás iránti kérelmet nyújtanak be, nem utasíthatja el ezt a kérelmet, kivéve, ha a többi érintett hatósággal, az ENISA-val és a Bizottsággal folytatott eszmecsere követően megállapítást nyer, hogy a hatóság nem illetékes a kért segítség nyújtására, vagy a kért segítségnyújtás nem arányos az illetékes hatóság 29. vagy 30. cikkel összhangban végzett felügyeleti feladataival.
- (2) Adott esetben és közös megegyezéssel különböző tagállamok illetékes hatóságai végezhetik a 29. és 30. cikkben említett közös felügyeleti intézkedéseket.

VII. FEJEZET

Átmeneti és záró rendelkezések

35. cikk

Felülvizsgálat

A Bizottság rendszeresen felülvizsgálja ezen irányelv működését, és jelentést tesz az Európai Parlamentnek és a Tanácsnak. A jelentés különösen azt értékeli, hogy az I. és II. mellékletben említett ágazatok, alágazatok, a szervezetek mérete és típusa mennyire releváns a gazdaság és a társadalom működése szempontjából a kiberbiztonsággal kapcsolatban. Ebből a célból és 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. Az első jelentést ... -ig [54 hónappal ezen irányelv hatálybalépését követően] kell benyújtani.

36. cikk

Felhatalmazás gyakorlása

- (1) A Bizottság felhatalmazást kap felhatalmazáson alapuló jogi aktusok elfogadására, az e cikkben meghatározott feltételek mellett.
- (2) A 18. cikk (6) bekezdésében és a 21. cikk (2) bekezdésében említett, felhatalmazáson alapuló jogi aktusok elfogadására vonatkozó felhatalmazást a Bizottságnak [...]tól/-től számított ötéves időtartamra adják át.

- (3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 18. cikk (6) bekezdésében és a 21. cikk (2) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti a határozatban meghatározott hatáskör átruházását. Ez a határozat az *Európai Unió Hivatalos Lapjában* való közzétételét követő napon vagy a határozatban meghatározott későbbi időpontban lép hatályba. Ez nem érinti a már hatályban lévő felhatalmazáson alapuló jogi aktusok érvényességét.
- (4) Felhatalmazáson alapuló jogi aktus elfogadása előtt a Bizottság konzultál az egyes tagállamok által kijelölt szakértőkkel a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban meghatározott elvekkel összhangban.
- (5) Felhatalmazáson alapuló jogi aktus elfogadásakor a Bizottság erről egyidejűleg értesíti az Európai Parlamentet és a Tanácsot.
- (6) A 18. cikk (6) bekezdése és a 21. cikk (2) bekezdése alapján elfogadott felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha sem az Európai Parlament, sem a Tanács nem emelt kifogást az Európai Parlament és a Tanács említett jogi aktusról történő értesítésétől számított két hónapon belül, vagy ha ezen időszak lejártá előtt az Európai Parlament és a Tanács egyaránt tájékoztatta a Bizottságot, hogy nem emel kifogást. Ezt az időszakot az Európai Parlament vagy a Tanács kezdeményezésére két hónappal meghosszabbítják.

37. cikk

Bizottsági eljárás

- (1) A Bizottság munkáját 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.

38. cikk

Átültetés

- (1) A tagállamok ... -ig [18 hónappal ezen irányelv hatálybalépését követően] elfogadják és kihirdetik az ezen irányelvnek való megfeleléshez szükséges törvényi, rendeleti és közigazgatási rendelkezéseket. A tagállamok erről haladéktalanul tájékoztatják a Bizottságot. Ezeket az intézkedéseket... -tól [az első albekezdésben említett időpontot követő egy nappal] alkalmazzák.
- (2) Amikor a tagállamok elfogadják ezeket az intézkedéseket, azokban hivatkozni kell erre az irányelvre, vagy azokhoz hivatalos kihirdetésük alkalmával ilyen hivatkozást kell fűzni. A hivatkozás módját a tagállamok határozzák meg.

39. cikk

A 910/2014/EU rendelet módosításai

A 910/2014/EU rendelet 19. cikkét el kell hagyni.

40. cikk

Az (EU) 2018/1972 irányelv módosítása

Az (EU) 2018/1972 irányelv 40. és 41. cikkét el kell hagyni.

41. cikk

Hatályon kívül helyezés

Az (EU) 2016/1148 irányelv ... [az irányelv átültetésének határideje]-től/-től hatályát veszti.

Az (EU) 2016/1148 irányelvre történő hivatkozásokat erre az irányelvre való hivatkozásként kell értelmezni, és a III. mellékletben található megfelelési táblázattal összhangban kell olvasni.

42. cikk

Hatálybalépés

Ez az irányelv az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

43. cikk

Címzettek

Ennek az irányelvnek a tagállamok a címzettjei.

Kelt Brüsszelben, -án/-én.

*az Európai Parlament részéről
az elnök*

*a Tanács részéről
az elnök*

PÉNZÜGYI KIMUTATÁS

Tartalom

1.	A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI	4
1.1.	A javaslat/kezdemenyezes címe.....	4
1.2.	Az érintett szakpolitikai terület(ek) (<i>Programklaszter</i>)	4
1.3.	A javaslat/kezdemenyezes a ketvekezoire irányul:.....	4
1.4.	A javaslat/kezdemenyezes indokolása	4
1.4.1.	Rövid vagy hosszú távon kielégítendő szükséglet(ek) a kezdeményezés végrehajtásának részletes ütemtervével	4
1.4.2.	Az uniós részvétel hozzáadott értéke (különböző tényezőkből fakadhat, pl. koordinációs nyereség, jogbiztonság, nagyobb hatékonyság vagy kiegészítő jelleg). E pont alkalmazásában az „uniós részvétel hozzáadott értéke” az uniós beavatkozásból származó érték, amely kiegészíti azt az értéket, amelyet egyébként a tagállamok egyedül hoztak volna létre.	4
1.4.3.	Hasonló korábbi tapasztalatok tanulsága	5
1.4.4.	Egyéb releváns eszközökkel való összeegyeztethetőség és lehetséges szinergia	5
1.5.	Időtartam és pénzügyi hatás	6
1.6.	Tervezett irányítási módszer(ek).....	6
2.	IRÁNYÍTÁSI INTÉZKEDÉSEK	8
2.1.	A nyomon követésre és a jelentéstételre vonatkozó rendelkezések.....	8
2.2.	Irányítási és kontrollrendszer(ek).....	8
2.2.1.	Az irányítási módszer(ek), a finanszírozás végrehajtási mechanizmusai, a kifizetési módok és a javasolt kontrollstratégia indokolása.....	8
2.2.2.	A felismert kockázatokkal és a csökkentésükre létrehozott belső kontrollrendszerekkel kapcsolatos információk.....	8
2.2.3.	A kontroll költség hatékonyságának becslése és indokolása (a „kontroll költségei ÷ a kezelt kapcsolódó források értéke” hányados) és a hibakockázat várható szintjeinek értékelése (kifizetéskor és záráskor)	8
2.3.	A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések	8
3.	A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA	9
3.1.	A többéves pénzügyi keret érintett fejezete és a költségvetésben javasolt új kiadási sor.....	9
3.2.	A kiadásokra gyakorolt becsült hatás.....	10
3.2.1.	A kiadásokra gyakorolt becsült hatás összefoglalása.....	10
3.2.2.	Az igazgatási jellegű előirányzatokra gyakorolt becsült hatás összefoglalása	13
3.2.3.	Harmadik felek részvétele a finanszírozásban	15
3.3.	A bevételre gyakorolt becsült hatás	15

1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdeményezés címe

Irányelvre irányuló javaslat az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről

1.2. Az érintett szakpolitikai terület(ek) (Programklaszter)

Hírközlési hálózatok, tartalom és technológia

1.3. A javaslat/kezdeményezés a következőre irányul:

☐ új intézkedés

☐ kísérleti projektet/előkészítő intézkedést követő új intézkedés⁴⁰

☒ jelenlegi intézkedés meghosszabbítása

☐ egy vagy több intézkedés összevonása vagy átalakítása egy másik/új intézkedéssé

1.4. A javaslat/kezdeményezés indokolása

1.4.1. Rövid vagy hosszú távon kielégítendő szükséglet(ek) a kezdeményezés végrehajtásának részletes ütemtervével

A felülvizsgálat célja az Európai Unióban működő vállalkozások átfogó csoportja kiberrezilienciájának növelése az összes releváns ágazatban, az irányelv által már lefedett ágazatokban a belső piacon tapasztalható reziliencia következtelenségeinek csökkentése és a közös helyzetismeret szintjének és a felkészülés és az elhárítás kollektív képességének javítása.

1.4.2. Az uniós részvétel hozzáadott értéke (különböző tényezőkből fakadhat, pl. koordinációs nyereség, jogbiztonság, nagyobb hatékonyság vagy kiegészítő jelleg). E pont alkalmazásában az „uniós részvétel hozzáadott értéke” az uniós beavatkozásból származó érték, amely kiegészíti azt az értéket, amelyet egyébként a tagállamok egyedül hoztak volna létre.

A kiberreziliencia nem lehet tényleges az Unió egészében, ha azt nemzeti vagy regionális adatsílókon keresztül eltérő módon közelítik meg. A hálózat- és információbiztonsági irányelv ennek a hiányosságnak az orvoslásával volt hivatott rendezni a hálózati és információs rendszerek biztonságát nemzeti és uniós szinten. A kiberbiztonsági irányelv első időszakos felülvizsgálata azonban számos eredendő hibára mutatott rá, amelyek végül jelentős különbségeket eredményeztek a tagállamokban a képességek, a tervezés és a védelem szintje tekintetében, amelyek egyidejűleg befolyásolják hasonló vállalatok számára az egyenlő versenyfeltételeket a belső piacon.

A kiberbiztonsági irányelv jelenlegi intézkedésein túlmutató uniós beavatkozást elsősorban a következők indokolják: i. a probléma határokon átnyúló vonatkozásai; ii. az uniós fellépés lehetőségei a hathatós nemzeti politikák javítására és megkönnyítésére; iii. összehangolt és együttműködő hálózati és információs

⁴⁰

A költségvetési rendelet 58. cikke (2) bekezdésének a) vagy b) pontja szerint.

rendszerekkel kapcsolatos szakpolitikai fellépések a hatékony adatvédelem és a magánélet védelme céljából.

A megfogalmazott célkitűzések tehát jobban elérhetők uniós szintű fellépéssel, mintsem egyedül a tagállamok által.

1.4.3. *Hasonló korábbi tapasztalatok tanulsága*

A kiberbiztonsági irányelv az első horizontális belső piaci eszköz, amelynek célja a hálózatok és rendszerek kiberbiztonsági kockázatokkal szembeni rezilienciájának javítása az Unióban. Ez már nagyban hozzájárult a kiberbiztonság közös szintjének emeléséhez a tagállamok körében. Az irányelv működésének és végrehajtásának felülvizsgálata azonban számos hiányosságra mutatott rá, amelyeket az egyre növekvő digitalizáció és a naprakészebb reagálás szükségessége mellett felülvizsgált jogi aktusban kell kezelni.

1.4.4. *Egyéb releváns eszközökkel való összeegyeztethetőség és lehetséges szinergia*

Az új javaslat teljes mértékben következetes és koherens más kapcsolódó kezdeményezésekkel, például a pénzügyi ágazat digitális működési rezilienciájáról szóló rendeletre irányuló javaslattal (DORA) és az alapvető szolgáltatásokat nyújtó kritikus szereplők rezilienciájáról szóló irányelvre irányuló javaslattal. Összhangban van az Európai Elektronikus Hírközlési Szabályzattal, az Általános Adatvédelmi Rendelettel és az eIDAS-rendelettel is.

A javaslat a biztonsági unióra vonatkozó uniós stratégia lényeges részét képezi.

1.5. Időtartam és pénzügyi hatás

☐ határozott időtartam

- ☐ hatályos ÉÉÉÉ [NN/HH] és [NN/HH] ÉÉÉÉ között
- ☐ Pénzügyi hatás: ÉÉÉÉ-től/től ÉÉÉÉ-ig a kötelezettségvállalási előirányzatok esetében és ÉÉÉÉ-től/től ÉÉÉÉ-ig a kifizetési előirányzatok esetében.

☒ határozatlan időtartam

- beindítási időszak: 2022-től 2025-ig
- azt követően: rendes ütem.

1.6. Tervezett irányítási módszer(ek)⁴¹

Bizottság általi közvetlen irányítás

- ☒ a Bizottság szervezeti egységein keresztül, ideértve az uniós küldöttségek személyzetét

- ☐ végrehajtó ügynökségen keresztül

☐ Megosztott irányítás a tagállamokkal

☐ **Közvetett irányítás** a költségvetés végrehajtásával kapcsolatos feladatoknak a következőkre történő átruházásával:

- ☐ harmadik országok vagy az általuk kijelölt szervek;
- ☐ nemzetközi szervezetek és ügynökségek (nevezze meg);
- ☐ az EBB és az Európai Beruházási Alap;
- ☒ a költségvetési rendelet 70. és 71. cikkben említett szervek;
- ☐ közjogi szervek;
- ☐ magánjog alapján működő, közfeladatot ellátó szervek, olyan mértékben, amennyiben megfelelő pénzügyi garanciákat nyújtanak;
- ☐ a valamely tagállam magánjoga alapján működő, köz- és magánszféra közötti partnerség végrehajtásával megbízott és megfelelő pénzügyi garanciákat nyújtó szervek;
- ☐ az EUSZ V. címének értelmében a KKBP terén konkrét fellépések végrehajtásával megbízott, és a vonatkozó alap-jogiaktusban meghatározott személyek.
- *Egynél több irányítási módszer feltüntetése esetén kérjük, adjon részletes felvilágosítást a „Megjegyzések” rovatban.*

Megjegyzések

Az Európai Unió Kiberbiztonsági Ügynöksége, az ENISA, amelynek a kiberbiztonsági jogszabály új állandó megbízatást adott, segítséget nyújtana a tagállamoknak és a Bizottságnak a felülvizsgált kiberbiztonsági irányelv végrehajtásában.

⁴¹

Az egyes irányítási módszerek ismertetése, valamint a költségvetési rendeletre való megfelelő hivatkozások megtalálhatók a Költségvetési Főigazgatóság honlapján:
<https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>

A felülvizsgált kiberbiztonsági irányelv eredményeként 2022/23-tól az ENISA további cselekvési területekkel rendelkezik. Jóllehet ezekre a cselekvési területeket megbízatása alapján lefedik az ENISA általános feladatai, ezek további munkaterhet jelentenek az ügynökség számára. Pontosabban, a jelenlegi cselekvési területein túl, a felülvizsgált kiberbiztonsági irányelvre irányuló bizottsági javaslat értelmében az ENISA-nak munkaprogramjába külön be kell építenie többek között a következő intézkedéseket: i. európai biztonságírás-nyilvántartás kidolgozása és fenntartása (a javaslat 6. cikkének (2) bekezdése), ii. az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (CyCLONe) titkárságának biztosítása (a javaslat 14. cikke), valamint éves jelentés kiadása a kiberbiztonság helyzetéről az EU-ban (a javaslat 15. cikke), iii. a tagállamok körében szakértői értékelések megszervezésének támogatása (a javaslat 16. cikke), iv. összesített eseményadatok összegyűjtése a tagállamoktól és technikai útmutatás kiadása (a javaslat 20. cikkének (9) bekezdése), v. nyilvántartás létrehozása és vezetése a határokon átnyúló szolgáltatásokat nyújtó szervezetek vonatkozásában (a javaslat 25. cikke).

Ezért 2022-től 5 kiegészítő teljes munkaidős egyenértéket igényelnek, amelynek megfelelő költségvetése évi körülbelül 0,61 millió EUR ezen új álláshelyek fedezésére (lásd az ügynökségek külön pénzügyi kimutatását).

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

Gyakoriság és feltételek.

A Bizottság rendszeresen felülvizsgálja az irányelv működését, és jelentést tesz az Európai Parlamentnek és a Tanácsnak, először három évvel a hatálybalépés után.

A Bizottság értékeli az irányelv helyes tagállami átültetését is.

2.2. Irányítási és kontrollrendszer(ek)

2.2.1. Az irányítási módszer(ek), a finanszírozás végrehajtási mechanizmusai, a kifizetési módok és a javasolt kontrollstratégia indokolása

A DG CNECT szakpolitikai területért felelős egysége irányítja az irányelv végrehajtását.

2.2.2. A felismert kockázatokkal és a csökkentésükre létrehozott belső kontrollrendszerekkel kapcsolatos információk

Nagyon alacsony a kockázat, mivel a kiberbiztonsági irányelv ökoszisztémája már működik.

2.2.3. A kontroll költséghatékonyságának becslése és indokolása (a „kontroll költségei ÷ a kezelt kapcsolódó források értéke” hányados) és a hibakockázat várható szintjeinek értékelése (kifizetéskor és záráskor)

Nem releváns. Csak adminisztratív költségvetés felhasználása („Teljes keret”).

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

Tüntesse fel a meglévő vagy tervezett megelőző és védintézkedéseket, pl. a csalás elleni stratégiából.

Nem releváns. Csak adminisztratív költségvetés felhasználása („Teljes keret”).

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

3.1. A többéves pénzügyi keret érintett fejezete és a költségvetésben javasolt új kiadási sor

A többéves pénzügyi keret fejezete	Költségvetési sor	Kiadás típusa	Hozzájárulás			
	Szám [Fejezet...7.....]	diff./nem diff. ⁴²	EFTA- országoktól ⁴³	tagjelölt országoktól ⁴⁴	harmadi k országok tól	a költségvetési rendelet [21. cikke (2) bekezdésének b) pontja] értelmében
	20 02 06 igazgatási kiadások					
	20 02 06	Nem diff	NEM	NEM	NEM	NEM

⁴² Diff. = Differenciált előirányzatok/Nem diff. = Nem differenciált előirányzatok.

⁴³ EFTA: Európai Szabadkereskedelmi Társulás.

⁴⁴ Tagjelölt országok és adott esetben a nyugat-balkáni potenciális tagjelölt országok.

3.2. A kiadásokra gyakorolt becsült hatás

3.2.1. A kiadásokra gyakorolt becsült hatás összefoglalása

millió EUR (három tizedesjegyre)

A többéves pénzügyi keret fejezete	<...>	[Fejezet.....]
---	-------	----------------

			2021	2022	2023	2024	2025	2026	2027	2027 után	ÖSSZESEN
Működési előirányzatok (a 3.1. pontban felsorolt költségvetési sorok szerint felosztva)	Kötelezettségvállalási előirányzatok	1.									
	Kifizetési előirányzatok	2.									
A program keretéből finanszírozott igazgatási előirányzatok ⁴⁵	Kötelezettségvállalási előirányzatok = Kifizetési előirányzatok	3.									
ÖSSZES előirányzat a program keretére	Kötelezettségvállalási előirányzatok	=1+3									
	Kifizetési előirányzatok	=2+3									

A többéves pénzügyi keret fejezete	7	„Igazgatási kiadások” Ülések: a kiberbiztonsági együttműködési csoport plenáris üléseire általában évente négy alkalommal kerül sor. A Bizottság fedezi a 27 tagállam képviselőinek étkezési
---	---	---

⁴⁵ Technikai és/vagy igazgatási segítségnyújtás, valamint az uniós programok és/vagy fellépések végrehajtásának támogatására fordított kiadások (korábbi „BA” sorok), közvetett kutatás, közvetlen kutatás.

		és utazási költségeit (tagállamonként egy képviselő). Egy találkozó költsége elérheti a 15 000 EUR-t. Küldöttségek: A küldöttségek a kiberbiztonsági irányelv végrehajtásának nyomon követésére irányulnak. Példa: Egy év alatt (2019. május – 2020. július) úgynevezett „kiberbiztonsági országlátogatásokat” kellett szerveznünk, és meglátogattuk mind a 27 tagállamot, hogy megvitassuk a kiberbiztonsági irányelv EU-ban történő végrehajtását.
--	--	--

Ezt a szakaszt az „igazgatási jellegű költségvetési adatok” felhasználásával kell kitölteni, amelyet először be kell vezetni [A pénzügyi kimutatás melléklete](#) dokumentumba, amelyet a DECIDE szolgálatok közötti konzultációs célokra tölt fel.

millió EUR (három tizedesjegyre)

		2021	2022	2023	2024	2025	2026	2027	2027 után	ÖSSZESEN
Humánerőforrás		1,14	1,14	1,14	1,14	1,14	1,14	1,14		7,98
Egyéb igazgatási kiadások		0,09	0,09	0,09	0,09	0,09	0,09	0,09		0,63
A többéves pénzügyi keret 7. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN	(Összes kötelezettségvállalási előirányzat = Összes kifizetési előirányzat)	1,23	1,23	1,23	1,23	1,23	1,23	1,23		8,61

millió EUR (három tizedesjegyre)

		2021	2022	2023	2024	2025	2026	2027	2027 után	ÖSSZESEN
A többéves pénzügyi keret több FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN	Kötelezettségvállalási előirányzatok									
	Kifizetési előirányzatok									

3.2.2. Az igazgatási jellegű előirányzatokra gyakorolt becsült hatás összefoglalása

- ☐ A javaslat/kezdeményezés nem vonja maga után igazgatási előirányzatok felhasználását.
- ☒ A javaslat/kezdeményezés az alábbi igazgatási előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyig)

Évek	2021	2022	2023	2024	2025	2026	2027	ÖSSZESEN
------	------	------	------	------	------	------	------	----------

A többéves pénzügyi keret 7. FEJEZETE								
Humán erőforrás	1,14	1,14	1,14	1,14	1,14	1,14	1,14	7,98
Egyéb igazgatási kiadások	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,63
Részösszeg – A többéves pénzügyi keret 7. FEJEZETE	1,23	1,23	1,23	1,23	1,23	1,23	1,23	8,61

7. FEJEZETEN kívül⁴⁶ of the multiannual financial framework								
Humán erőforrás								
Egyéb igazgatási jellegű kiadások								
Részösszeg – a többéves pénzügyi keret 7. FEJEZETÉN kívül								

ÖSSZESEN	1,23	1,23	1,23	1,23	1,23	1,23	1,23	8,61
-----------------	------	------	------	------	------	------	------	------

A humán erőforrásokra és egyéb igazgatási jellegű kiadásokra szükséges előirányzatokat az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt és/vagy az adott főigazgatóságon belül átcsoportosított előirányzatokkal biztosítják. Az előirányzatok szükség szerint a meglévő költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további juttatásokkal.

⁴⁶

Technikai és/vagy igazgatási segítségnyújtás, valamint az uniós programok és/vagy fellépések végrehajtásának támogatására fordított kiadások (korábbi „BA” sorok), közvetett kutatás, közvetlen kutatás.

3.2.2.1. Becsült humánerőforrás-szükségletek

- ☐ A javaslat/kezdeményezés nem igényel humánerőforrást.
- ☒ A javaslat/kezdeményezés az alábbi humánerőforrás-igénnyel jár:

A becsléseket teljes munkaidős egyenértékben kell kifejezni

Évek	2021	2022	2023	2024	2025	2026	2027
• A létszámtervben szereplő álláshelyek (tisztviselők és ideiglenes alkalmazottak)							
A központban és a bizottsági képviselőket	6	6	6	6	6	6	6
a küldöttségeknél							
Kutatás							
• Külső munkatársak teljes munkaidős egyenértékben (FTE) kifejezve: – AC, AL, END, INT és JED ⁴⁷							
7. fejezet							
A többéves pénzügyi keret 7. FEJEZETÉBŐL finanszírozva	– a központban	3	3	3	3	3	3
	– a küldöttségeknél						
A programkeretből finanszírozva ⁴⁸	– a központban						
	– a küldöttségeknél						
Kutatás							
Egyéb (kérjük megnevezni)							
ÖSSZESEN		9	9	9	9	9	9

A humánerőforrás-igényeknek az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt és/vagy az adott főigazgatóságban belül átcsoportosított személyzettel kell eleget tenni. A források adott esetben a meglévő költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további juttatásokkal.

Az elvégzendő feladatok leírása:

Tisztviselők és ideiglenes alkalmazottak	- Felhatalmazáson alapuló jogi aktusok előkészítése a 18. cikk (6) bekezdésének, a 21. cikk (2) bekezdésének és a 36. cikknek megfelelően; - Végrehajtási jogi aktusok előkészítése a 12. cikk (8) bekezdésének, a 18. cikk (5) bekezdésének és a 20. cikk (11) bekezdésének megfelelően; - Titkárság biztosítása a kiberbiztonsági együttműködési csoport számára; - a kiberbiztonsági együttműködési csoport plenáris üléseinek és munkafolyamat-üléseinek szervezése; - A tagállamok munkájának összehangolása a különféle dokumentumok (iránymutatások, eszköztárak stb.) terén; - Kapcsolattartás más bizottsági szolgálatokkal, az ENISA-val és a nemzeti hatóságokkal a kiberbiztonsági irányelv végrehajtása érdekében; - A kiberbiztonsági irányelv végrehajtásával kapcsolatos nemzeti módszerek és bevált gyakorlatok elemzése.
Külső munkatársak	Szükség esetén az összes fenti feladat támogatása

⁴⁷ AC = szerződéses alkalmazott; AL = helyi alkalmazott; END = kirendelt nemzeti szakértő; INT = kölcsönmunkaerő (átmeneti alkalmazott); JPD = küldöttségi pályakezdő szakértő.

⁴⁸ Az operatív előirányzatokból finanszírozott külső munkatársakra vonatkozó részleges felső határérték (korábban: BA-tételek).

3.2.3. Harmadik felek részvétele a finanszírozásban

A javaslat/kezdemenyezés

- ☒ nem irányoz elő harmadik felek általi társfinanszírozást
- ☐ az alábbi becsült társfinanszírozást irányozza elő:

előirányzatok, millió EUR (három tizedesjegyre)

Évek	2021	2022	2023	2024	2025	2026	2027	ÖSSZESEN
Adja meg a társfinanszírozó szervet								
Társfinanszírozott előirányzatok ÖSSZESEN								

3.3. A bevételre gyakorolt becsült hatás

- ☒ A javaslatnak/kezdemenyezésnek nincs pénzügyi hatása a bevételre.
- ☐ A javaslatnak/kezdemenyezésnek van pénzügyi hatása – a bevételre gyakorolt hatása a következő:
 - ☐ a javaslat a saját forrásokra gyakorol hatást
 - ☐ a javaslat más bevételre gyakorol hatást

kérjük adja meg, hogy a bevétel kiadási sorhoz van-e rendelve ☐

millió EUR (három tizedesjegyre)

Bevételi költségvetési sor:	A javaslat/kezdemenyezés hatása ⁴⁹						
	2021	2022	2023	2024	2025	2026	2027
... jogcímcsoport							

A címzett bevételek esetében tüntesse fel az érintett kiadáshoz tartozó költségvetési sor(oka)t.

Egyéb megjegyzések (pl. a bevételre gyakorolt hatás számítására használt módszer/képlet vagy egyéb információ).

⁴⁹

A tradicionális saját források (vámok, cukorilletékek) tekintetében nettó összegeket, vagyis a 20 %-kal (beszedési költségek) csökkentett bruttó összegeket kell megadni.

MELLÉKLET **a PÉNZÜGYI KIMUTATÁSHOZ**

A javaslat/kezdemenyezés címe

A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i (EU) 2016/1148 európai parlamenti és tanácsi irányelv felülvizsgálatáról szóló irányelvre irányuló javaslat

- (1) SZÜKSÉGESNEK ÍTÉLT HUMÁNERŐFORRÁSOK SZÁMA és KÖLTSÉGE
- (2) Az EGYÉB IGAZGATÁSI KIADÁSOK KÖLTSÉGE
- (3) A KÖLTSÉGEK BECSLÉSÉRE HASZNÁLT SZÁMÍTÁSI MÓDSZER
 - 3,1 Humán erőforrás
 - 3,2 Egyéb igazgatási kiadások

Ezt a mellékletet, amelyet a javaslatban/kezdemenyezésben részt vevő egyes főigazgatóságoknak/szolgálatoknak kell kitölteniük, csatolni kell a pénzügyi kimutatáshoz a szolgálatközi konzultáció megindításakor.

Az adattáblázatokat használták forrásként a pénzügyi kimutatásba foglalt táblázatokhoz. A táblázatok kizárólag a Bizottságon belüli belső használatra készültek.

1. A humánerőforrás-szükségletek költsége

☐ A javaslat/kezdeményezés nem igényel humánerőforrást

☒ A javaslat/kezdeményezés az alábbi humánerőforrás-igénnyel jár:

millió EUR (három tizedesjegyig)

A többéves pénzügyi keret 7. FEJEZETE		2021		2022		2023		2024		2025		2026		2027		ÖSSZESEN	
		FTE	Előirányzatok	FTE	Előirányzatok	FTE	Előirányzatok	FTE	Előirányzatok	FTE	Előirányzatok	FTE	Előirányzatok	FTE	Előirányzatok	FTE	Előirányzatok
• A létszámtervben szereplő álláshelyek (tisztviselők és ideiglenes alkalmazottak)																	
A központban és a bizottsági képviseleteken	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
Uniós küldöttségeknél	AD																
	AST																
• Külső személyzet ⁵⁰ 0,24																	
Teljes keret	AC	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	END																
	INT																
Uniós küldöttségeknél	AC																
	AL																
	END																

50

AC = szerződéses alkalmazott; AL = helyi alkalmazott; END = kirendelt nemzeti szakértő; INT = kölcsönmunkaerő (átmeneti alkalmazott); JPD = küldöttségi pályakezdő szakértő.

	INT																
	JPD																
Egyéb költségvetési sor (<i>kérjük megnevezni</i>)																	
Részösszeg – A többéves pénzügyi keret 7. FEJEZETE		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

A humánerőforrás-igényeknek az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt és/vagy az adott főigazgatóságon belül átcsoportosított személyzettel kell eleget tenni. A források adott esetben a meglévő költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további juttatásokkal.

A többéves pénzügyi keret 7. FEJEZETÉN kívül		2021		2022		2023		2024		2025		2025		2025		ÖSSZESEN	
		FTE	Előirányzatok	FTE	Előirányzatok	FTE	Előirányzatok	FTE	Előirányzatok	FTE	Előirányzatok	FTE	Előirányzatok	FTE	Előirányzatok	FTE	Előirányzatok
• A létszámtervben szereplő álláshelyek (tisztviselők és ideiglenes alkalmazottak)																	
Kutatás	AD																
	AST																
• Külső munkatársak ⁵¹																	
Az operatív előirányzatokból finanszírozott külső munkatársak (korábban: BA-tételek).	– a központban	AC															
		END															
		INT															
	– uniós küldöttségeknél	AC															
		AL															
		END															
		INT															
		JPD															
Kutatás	AC																
	END																
	INT																
Egyéb költségvetési sor (kérjük)																	

⁵¹

AC = szerződéses alkalmazott; AL = helyi alkalmazott; END =kirendelt nemzeti szakértő; INT =kölcsonmunkaerő (átmeneti alkalmazott); JPD = küldöttségi pályakezdő szakértő.

megnevezni)																	
Részösszeg – A többéves pénzügyi keret 7. FEJEZETÉN kívül																	

A humánerőforrás-igényeknek az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt és/vagy az adott főigazgatóságon belül átcsoportosított személyzettel kell eleget tenni. A források adott esetben a meglévő költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további juttatásokkal.

Az ENISA humánerőforrására gyakorolt becsült hatás

Az Európai Unió Kiberbiztonsági Ügynöksége, az ENISA, amelynek a kiberbiztonsági jogszabály új állandó megbízatást adott, segítséget nyújtana a tagállamoknak és a Bizottságnak a felülvizsgált kiberbiztonsági irányelv végrehajtásában.

A felülvizsgált kiberbiztonsági irányelv eredményeként 2022/23-tól az ENISA további cselekvési területekkel rendelkezik. Jóllehet ezekre a cselekvési területeket megbízatása alapján lefedik az ENISA általános feladatai, ezek további munkaterhet jelentenek az ügynökség számára. Pontosabban, a jelenlegi cselekvési területein túl, a felülvizsgált kiberbiztonsági irányelvre irányuló bizottsági javaslat értelmében az ENISA-nak munkaprogramjába külön be kell építenie többek között a következő intézkedéseket: i. európai biztonságirés-nyilvántartás kidolgozása és fenntartása (a javaslat 6. cikkének (2) bekezdése), ii. az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (CyCLONE) titkárságának biztosítása (a javaslat 14. cikke), valamint éves jelentés kiadása a kiberbiztonság helyzetéről az EU-ban (a javaslat 15. cikke), iii. a tagállamok körében szakértői értékelések megszervezésének támogatása (a javaslat 16. cikke), iv. összesített eseményadatok összegyűjtése a tagállamoktól és technikai útmutatás kiadása (a javaslat 20. cikkének (9) bekezdése), v. nyilvántartás létrehozása és vezetése a határokon átnyúló szolgáltatásokat nyújtó szervezetek vonatkozásában (a javaslat 25. cikke).

Ezért 2022-től 5 kiegészítő teljes munkaidős egyenértéket igényelnek, amelynek megfelelő költségvetése évi körülbelül 0,61 millió EUR ezen új álláshelyek fedezésére (lásd az ügynökségek külön pénzügyi kimutatását).

Ezért 2022-től 5 kiegészítő FTE-t igényelnek a megfelelő költségvetéssel ezen új álláshelyek fedezésére.

- ☐ A javaslat/kezdeményezés nem vonja maga után igazgatási előirányzatok felhasználását
- ☒ A javaslat/kezdeményezés az alábbi igazgatási előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyig)

	Év N ⁵² 2022	Év N+1 2023	Év N+2 2024	Év N+3 2025	Adjon meg annyi évet, amennyi szükséges a hatás időtartamának megjelenítéséhez (lásd az 1.6. pontot)	ÖSSZES EN
--	-------------------------------	-------------------	-------------------	-------------------	--	--------------

Ideiglenes alkalmazottak (AD fokozat)	0,450	0,450	0,450	0,450	0,450	0,450		2,7
---------------------------------------	-------	-------	-------	-------	-------	-------	--	-----

⁵² Az N. év a javaslat/kezdeményezés végrehajtásának kezdete. Kérjük, cserélje ki az „N” értéket a megvalósítás várható első évére (például: 2021). Ugyanez a következő években is.

Ideiglenes alkalmazottak (AST fokozat)								
Szerződéses alkalmazottak	0,160	0,160	0,160	0,160	0,160	0,160		
Kirendelt nemzeti szakértők								0,96

ÖSSZESEN	0,61	0,61	0,61	0,61	0,61	0,61		3,66
-----------------	-------------	-------------	-------------	-------------	-------------	-------------	--	-------------

Személyi követelmények (FTE):

	Év N ⁵³ 2022	Év N+1 2023	Év N+2 2024	Év N+3 2025	Adjon meg annyi évet, amennyi szükséges a hatás időtartamának megjelenítéséhez (lásd az 1.6. pontot)	ÖSSZESEN
--	-------------------------------	-------------------	-------------------	-------------------	--	----------

Ideiglenes alkalmazottak (AD fokozat)	3	3	3	3	3	3		18
Ideiglenes alkalmazottak (AST fokozat)								
Szerződéses alkalmazottak	2	2	2	2	2	2		12

⁵³ Az N. év a javaslat/kezdeményezés végrehajtásának kezdete. Kérjük, cserélje ki az „N” értéket a megvalósítás várható első évére (például: 2021). Ugyanez a következő években is.

Kirendelt nemzeti szakértők								
-----------------------------	--	--	--	--	--	--	--	--

ÖSSZESEN	5	5	5	5	5	5		30
----------	---	---	---	---	---	---	--	----

2. Az egyéb igazgatási kiadások költsége

- ☐ A javaslat/kezdeményezés nem vonja maga után igazgatási előirányzatok felhasználását
☒ A javaslat/kezdeményezés az alábbi igazgatási előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyig)

A többéves pénzügyi keret 7. FEJEZETE	2021	2022	2023	2024	2025	2026	2027	Összesen
<u>A központban:</u>								
Kiküldetési és reprezentációs költségek	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,21
Konferenciákkal és ülésekkel kapcsolatos költségek	0,06	0,06	0,06	0,06	0,06	0,06	0,06	0,42
Bizottságok ⁵⁴								
Tanulmányok és konzultációk								
Informatikai és irányítási rendszerek								

⁵⁴ Nevezze meg a bizottság típusát és azt a csoportot, amelyhez a bizottság tartozik.

IKT-berendezések és -szolgáltatások ⁵⁵								
Egyéb költségvetési sor <i>(kérjük megnevezni)</i>								
Uniók küldöttségeknél								
Kiküldetési, konferencia- és reprezentációs költségek								
A személyzet továbbképzése								
Vásárlás, bérlet és ezzel kapcsolatos kiadások								
Berendezés, felszerelés, készletek és szolgáltatások								
Részösszeg – A többéves pénzügyi keret 7. FEJEZETE	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,63

⁵⁵

IKT: Információs és kommunikációs technológiák: az Informatikai Főigazgatósággal konzultálni kell.

millió EUR (három tizedesjegyre)

A többéves pénzügyi keret 7. FEJEZETÉN kívül	2021	2022	2023	2024	2025	2026	2027	Összesen
Technikai és igazgatási segítségnyújtás kiadása (a külső munkatársakat <u>nem számítva</u>) az operatív előirányzatokból (korábbi BA-tételek)								
– a központban								
– uniós küldöttségeknél								
Egyéb igazgatási kiadások a kutatás területén								
Egyéb költségvetési sor (kérjük megnevezni)								
Részösszeg – A többéves pénzügyi 7. FEJEZETÉN kívül								

ÖSSZESEN A többéves pénzügyi keret 7. FEJEZETE és 7. FEJEZETÉN kívül	1,23	1,23	1,23	1,23	1,23	1,23	1,23	8,61
---	------	------	------	------	------	------	------	-------------

A szükséges igazgatási előirányzatokat a fellépés irányításához rendelt és/vagy az adott főigazgatóságon belül átcsoportosított előirányzatokkal biztosítják. Az előirányzatok adott esetben a meglévő költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további juttatásokkal.

3. A költségek becslésére használt számítási módszer

3,1 Humánerőforrás

Ez a rész ismerteti a szükségesnek tartott humánerőforrás becslésére használt számítási módszert (a munkateherre vonatkozó feltevések, beleértve a konkrét álláshelyeket (Sysper 2 munkakörök), a személyzeti kategóriákat és az azoknak megfelelő átlagos költségeket)

A többéves pénzügyi keret 7. FEJEZETE

Megjegyzés: A központban foglalkoztatott egyes személyzeti kategóriák átlagköltségei a BudgWeb oldalon érhetők el:

https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx

• Tisztviselők és ideiglenes alkalmazottak

6 FTE tisztviselő (átlagos költsége 0,150) = 0,9 évenként

- Felhatalmazáson alapuló jogi aktusok előkészítése a 18. cikk (6) bekezdésének, a 21. cikk (2) bekezdésének és a 36. cikknek megfelelően;
- Végrehajtási jogi aktusok előkészítése a 12. cikk (8) bekezdésének, a 18. cikk (5) bekezdésének és a 20. cikk (11) bekezdésének megfelelően;
- Titkárság biztosítása a kiberbiztonsági együttműködési csoport számára;
- a kiberbiztonsági együttműködési csoport plenáris üléseinek és munkafolyamat-üléseinek szervezése;
- A tagállamok munkájának összehangolása a különféle dokumentumok (iránymutatások, eszköztárak stb.) terén;
- Kapcsolattartás más bizottsági szolgálatokkal, az ENISA-val és a nemzeti hatóságokkal a kiberbiztonsági irányelv végrehajtása érdekében;
- A kiberbiztonsági irányelv végrehajtásával kapcsolatos nemzeti módszerek és bevált gyakorlatok elemzése.

• Külső munkatársak

3 AC (átlagos költség 0,08) = 0,24 évenként

- Szükség esetén az összes fenti feladat támogatása

A többéves pénzügyi keret 7. FEJEZETÉN kívül

•Csak a kutatási költségvetésből finanszírozott álláshelyek

• Külső munkatársak

3,2 Egyéb igazgatási kiadások

Adja meg az egyes költségvetési sorok esetében alkalmazott számítási módszer részleteit, és különösen az azokat alátámasztó feltételezéseket (pl. ülések száma évente, átlagköltségek stb.)

A többéves pénzügyi keret 7. FEJEZETE
--

Ülések: a kiberbiztonsági együttműködési csoport plenáris üléseire általában évente négy alkalommal kerül sor. A Bizottság fedezi a 27 tagállam képviselőinek étkezési és utazási költségeit (tagállamonként egy képviselő). Egy találkozó költségei elérhetik a 15 000 EUR-t, ami évi 60 000 EUR-t jelent.
--

Küldöttségek: A küldöttségek a kiberbiztonsági irányelv végrehajtásának nyomon követésére irányulnak. Példa: Egy év alatt (2019. május – 2020. július) úgynevezett „kiberbiztonsági országlátogatásokat” kellett szerveznünk, és meglátogattuk mind a 27 tagállamot, hogy megvitassuk
--

a kiberbiztonsági irányelv EU-ban történő végrehajtását.

A többéves pénzügyi keret 7. FEJEZETÉN kívül

7. MELLÉKLET

A BIZOTTSÁG HATÁROZATA

az Európai Unió általános költségvetésének végrehajtására vonatkozó belső szabályokról (az Európai Bizottság szakasza) a Bizottság szervezeti egységei számára

„ÜGYNÖKSÉGEK” PÉNZÜGYI KIMUTATÁSA

Ez az LFS fedezi azt a kérést, hogy 2022-től 5 FTE-vel növeljék az ENISA személyzetét a kiberbiztonsági irányelv végrehajtásával kapcsolatos kiegészítő tevékenységek végzése érdekében. Ezekre a tevékenységekre már vonatkozik az ENISA megbízása.

Tartalom

1.	A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI	17
1.1.	A javaslat/kezdemenyezés címe.....	17
1.2.	Az érintett szakpolitikai terület(ek).....	17
1.3.	A javaslat/kezdemenyezés a következőre irányul:.....	17
1.4.	Célkitűzés(ek):	17
1.4.1.	Általános célkitűzés(ek).....	17
1.4.2.	Egyedi célkitűzés(ek)	17
1.4.3.	Várható eredmény(ek) és hatás	19
1.4.4.	Teljesítménymutatók.....	20
1.5.	A javaslat/kezdemenyezés indokolása	21
1.5.1.	Rövid vagy hosszú távon kielégítendő szükséglet(ek) a kezdemenyezés végrehajtásának részletes ütemtervével	21
1.5.2.	Az uniós részvétel hozzáadott értéke (különböző tényezőkből fakadhat, pl. koordinációs nyereség, jogbiztonság, nagyobb hatékonyság vagy kiegészítő jelleg). E pont alkalmazásában az „uniós részvétel hozzáadott értéke” az uniós beavatkozásból származó érték, amely kiegészíti azt az értéket, amelyet egyébként a tagállamok egyedül hoztak volna létre.21	
1.5.3.	Hasonló korábbi tapasztalatok tanulsága	21
1.5.4.	A többéves pénzügyi kerettel való összeegyeztethetőség és lehetséges szinergiák a többi megfelelő eszközzel	21
1.5.5.	A rendelkezésre álló különböző finanszírozási lehetőségek értékelése, ideértve az átcsoportosítás lehetőségét is	22
1.6.	A javaslat/kezdemenyezés tartama és becsült pénzügyi hatása	23
1.7.	Tervezett irányítási módszer(ek).....	23
2.	IRÁNYÍTÁSI INTÉZKEDÉSEK	25
2.1.	A nyomon követésre és a jelentéstételre vonatkozó rendelkezések.....	25
2.2.	Irányítási és kontrollrendszer(ek).....	25
2.2.1.	Az irányítási módszer(ek), a finanszírozás végrehajtási mechanizmusai, a kifizetési módok és a javasolt kontrollstratégia indokolása	25
2.2.2.	A felismert kockázatokkal és a csökkentésükre létrehozott belső kontrollrendszerekkel kapcsolatos információk	25
2.2.3.	A kontroll költség hatékonyságának becslése és indokolása (a „kontroll költségei ÷ a kezelt kapcsolódó források értéke” hányados) és a hibakockázat várható szintjeinek értékelése (kifizetéskor és záráskor)	25
2.3.	A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések.....	26
3.	A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA	26

3.1.	A többéves pénzügyi keret érintett fejezete(i) és a költségvetésben javasolt új kiadási sor(ok)	26
3.2.	A kiadásokra gyakorolt becsült hatás.....	28
3.2.1.	A kiadásokra gyakorolt becsült hatás összefoglalása	28
3.2.2.	A [testület] előirányzataira gyakorolt becsült hatás	31
3.2.3.	Az ENISA humánerőforrására gyakorolt becsült hatás	33
3.2.4.	Összeegyeztethetőség a folyó többéves pénzügyi kerettel	36
3.2.5.	Harmadik felek részvétele a finanszírozásban	36
3.3.	A bevételre gyakorolt becsült hatás	37

1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdemenyezes címe

Iránylevire irányuló javaslat az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről

1.2. Az érintett szakpolitikai terület(ek)

Hírközlési hálózatok, tartalom és technológia

1.3. A javaslat/kezdemenyezes a következore irányul:

☐ új intézkedés

☐ kísérleti projektet/előkészítő intézkedést követő új intézkedés⁵⁶

☒ jelenlegi intézkedés meghosszabbítása

☐ egy vagy több intézkedés összevonása vagy átalakítása egy másik/új intézkedéssé

1.4. Célkitűzés(ek):

1.4.1. Általános célkitűzés(ek)

A felülvizsgálat célja az Európai Unióban működő vállalkozások átfogó csoportja kiberrezilienciájának növelése az összes releváns ágazatban, az irányelv által már lefedett ágazatokban a belső piacon tapasztalható reziliencia következtelenségeinek csökkentése és a közös helyzetismeret szintjének és a felkészülés és az elhárítás kollektív képességének javítása.

1.4.2. Egyedi célkitűzés(ek)

Az Európai Unióban működő vállalkozások alacsony szintű kiberrezilienciája problémájának kezelése érdekében konkrét célkitűzés annak biztosítása, hogy minden ágazatban azok a szervezetek, amelyek függenek a hálózati és információs rendszerektől, és amelyek kulcsfontosságú szolgáltatásokat nyújtanak a gazdaság és a társadalom egésze számára, kiberbiztonsági intézkedések meghozatalára és az események bejelentésére legyenek kötelesek annak érdekében, hogy az egész belső piacon növelni lehessen a kiberreziliencia általános szintjét.

A tagállamok és az ágazatok rezilienciája terén tapasztalt következtelenségek problémájának kezelése érdekében konkrét célkitűzés annak biztosítása, hogy minden olyan szervezetre, amely a kiberbiztonsági irányelv jogi keretének hatálya alá tartozó ágazatokban tevékenykedik, és hasonló méretű és hasonló szerepet tölt be, ugyanazon szabályozási rendszer alá tartozzon (a hatályon belül vagy azon kívül), függetlenül attól, hogy melyik tagállam joghatósága alá tartozik az EU-n belül.

Annak biztosítása érdekében, hogy a kiberbiztonsági irányelv jogi keretének hatálya alá tartozó ágazatokban tevékenykedő valamennyi szervezet köteles legyen ugyanazokat a kötelezettségeket betartani a kockázatkezelés koncepciója alapján a biztonsági intézkedéseket illetően, és minden eseményt egységes kritériumok alapján legyen köteles jelenteni, konkrét

⁵⁶

A költségvetési rendelet 58. cikke (2) bekezdésének a) vagy b) pontja szerint.

célkitűzés annak biztosítása, hogy az illetékes hatóságok összehangolt felügyeleti és végrehajtási intézkedések révén hatékonyabban hajtsák végre a jogi eszköz által megállapított szabályokat, és hogy az illetékes hatóságok számára elkülönített források összehasonlítható szintűek legyenek a tagállamokban, ami lehetővé teszi számukra a kiberbiztonsági irányelv kerete által meghatározott alapvető feladatok teljesítését.

A közös helyzetismeret és a közös válságelhárítás hiánya problémájának kezelése érdekében konkrét cél az alapvető információk tagállamok közötti megosztásának biztosítása azáltal, hogy egyértelmű kötelezettségeket vezetnek be az illetékes hatóságok számára az információmegosztásra és az együttműködésre a kiberfenyegetések tekintetében, és fejlesztik az Unió közös operatív válságelhárítási képességét.

1.4.3. Várható eredmény(ek) és hatás

Adja meg, hogy a javaslatnak/kezdeményezésnek milyen hatásai lehetnek a megcélzott kedvezményezettekre/csoporthoz.

A javaslat várhatóan jelentős előnyökkel jár: becslések szerint 11,3 milliárd EUR-val csökkentheti a kiberbiztonsági események költségeit. Az ágazati hatókör jelentősen kibővülne a hálózati és információs rendszerek biztonsági keretén belül, de a fenti előnyök mellett a hálózati és információs rendszerek biztonsági követelményei által előidézhető teher – nevezetesen a felügyelet szempontjából – kiegyensúlyozásra kerülne mind a hatály alá újonnan bekerülő szervezetek, mind az illetékes hatóságok esetében. A hálózati és információs rendszerek új biztonsági kerete kétrétegű megközelítést vezetne be, amelynek középpontjában a nagy és kulcsfontosságú szervezetek, valamint a felügyeleti rendszer differenciálása áll, amely csak utólagos felügyeletet tesz lehetővé nagy számú, nevezetesen azon szervezetek esetében, amelyeket „fontosnak”, de nem „alapvetőnek” tekintenek.

Összességében a javaslat hatékony kompromisszumokat és szinergiákat eredményezne, az összes elemzett szakpolitikai alternatíva közül a lehető legjobb lehetne annak biztosítása érdekében, hogy a kulcsfontosságú szervezetek magasabb és következetes szintű kiberbiztonsági szintje az egész Unióban biztosítható legyen, ami végül költségmegtakarításhoz vezetne mind a vállalkozások, mind a társadalom számára.

A javaslat bizonyos megfelelési és végrehajtási költségekhez is vezetne az érintett tagállami hatóságok számára (a források összességében mintegy 20–30 %-os növekedését becsülték). Az új keret ugyanakkor jelentős előnyökkel járna a kulcsfontosságú vállalkozások jobb áttekintése és az azokkal való interakció, a határokon átnyúló operatív együttműködés fokozása, valamint a kölcsönös segítségnyújtás és a szakértői értékelési mechanizmusok révén is. Ez a tagállamokban a kiberbiztonsági képességek általános növekedését eredményezné.

Becslések szerint azoknak a vállalatoknak, amelyek a hálózati és információs rendszerek biztonsági keretének hatálya alá tartoznának, a hálózati és információs rendszerek új biztonsági keretének bevezetését követő első években a jelenlegi IKT-biztonsági kiadásaik legfeljebb 22 %-os növelésére lenne szükségük (ez 12 % a már a kiberbiztonsági irányelv hatálya alá tartozó vállalatok esetében). Az IKT-biztonsági kiadások ezen átlagos növekedése azonban az említett beruházások arányos hasznát eredményezné, elsősorban a kiberbiztonsági események költségeinek jelentős (becslések szerint tíz év alatt 118 milliárd EUR értékű) csökkenése miatt.

A kis- és mikrovállalkozások mentesülnének a hálózati és információs rendszerek biztonsági keretének hatálya alól. A középvállalkozások esetében várható, hogy a hálózati és információs rendszerek új biztonsági keretének bevezetését követő első években emelkedni fog az IKT-biztonsági kiadások szintje. Ugyanakkor az e szervezetekre vonatkozó biztonsági követelmények emelése ösztönözné kiberbiztonsági képességeiket és elősegítené IKT-kockázatkezelésük javítását.

Lesz hatás a tagállamok költségvetésére és közigazgatására: a források esetében körülbelül 20–30 %-os becsült növekedés várható rövid és középtávon.

Egyéb jelentős negatív hatás nem várható. A javaslat várhatóan erőteljesebb kiberbiztonsági képességekhez vezet, és ennek következtében jelentősebb mérséklő hatása lesz az események – ideértve az adatokkal való visszaéléseket is – száma és súlyossága vonatkozásában. Valószínűleg pozitív hatása lesz az egyenlő versenyfeltételek biztosítása tekintetében a

tagállamokban a kiberbiztonsági irányelv hatálya alá tartozó valamennyi szervezet számára, és csökkenti a kiberbiztonsági információk aszimmetriáit.

1.4.4. Teljesítménymutatók

Adja meg az előrehaladás és az eredmények nyomon követésének mutatóit.

A mutatók értékelését a Bizottság végzi az ENISA és az együttműködési csoport támogatásával, a hálózati és információs rendszerek biztonságáról szóló új jogi aktus hatálybalépésétől számított három év elteltével kezdődően. Néhány olyan nyomonkövetési mutató, amelynek alapján a kiberbiztonsági irányelv felülvizsgálatának sikerét értékelni fogják, a következő:

- Az események jobb kezelése: A kiberbiztonsági intézkedések meghozatalával a vállalatok nemcsak az egyes események teljes elkerülésének képességét javítják, hanem az eseményelhárítási képességüket is. A siker mércéje tehát: i. az esemény észleléséhez szükséges átlagos idő csökkentése, ii. az az idő, amelyre a szervezeteknek átlagosan szükségük van egy eseményből való felépüléshez, és iii. az esemény által okozott kár átlagos költsége.
- A kiberbiztonsági kockázatok nagyobb ismerete a vállalatok felső vezetése részéről: azáltal, hogy a vállalatoktól intézkedéseket követel meg, a felülvizsgált kiberbiztonsági irányelv hozzájárul a kiberbiztonsággal kapcsolatos kockázatok tudatosításához a felső vezetés körében. Ezt lehet mérni annak tanulmányozásával, hogy a kiberbiztonsági irányelv hatálya alá tartozó vállalatok milyen mértékben helyezik előtérbe a kiberbiztonságot a belső vállalati politikákban és folyamatokban, a belső dokumentáció, a releváns képzési programok és a munkavállalók tudatossági tevékenységei, valamint a biztonsággal kapcsolatos IKT-beruházások előtérbe helyezése által bizonyítottan. Valamennyi alapvető és fontos szervezet vezetőségének tisztában kell lennie a kiberbiztonsági irányelv által megállapított szabályokkal.
- Az ágazatspecifikus kiadások kiegyenlítése: Az IKT-biztonságra fordított kiadások jelentősen eltérnek az uniós ágazatokban. Azáltal, hogy a több ágazatban működő vállalatoktól intézkedéseket követelnek meg, csökkennie kell az összes IKT-kiadás százalékában az ágazatspecifikus IKT-biztonsági kiadások ágazatok és a tagállamok közötti átlagos eltéréseinek.
- Erősebb illetékes hatóságok és fokozott együttműködés: A felülvizsgált a kiberbiztonsági irányelv további feladatokat ruházhat az illetékes hatóságokra. Ennek mérhető hatása lesz a kiberbiztonsági ügynökségek számára nemzeti szinten elkülönített pénzügyi és humán erőforrásokra, és pozitív hatással lesz az illetékes hatóságok proaktív együttműködésre való képességére is, és ezáltal növeli azoknak az eseteknek a számát, amikor az illetékes hatóságok egymást határokon átnyúló események kezelése vagy közös felügyeleti tevékenységek végzése céljából bevonják.
- Fokozott információmegosztás: A hálózati és információs rendszerek biztonságáról szóló felülvizsgált irányelv javítja az információk megosztását a vállalatok között és az illetékes hatóságokkal is. A felülvizsgálat egyik célja lehet az információmegosztás különféle formáiban részt vevő szervezetek számának növelése.

1.5. A javaslat/kezdeményezés indokolása

1.5.1. Rövid vagy hosszú távon kielégítendő szükséglet(ek) a kezdeményezés végrehajtásának részletes ütemtervével

A javaslat célja az Európai Unióban működő vállalkozások átfogó csoportja kiberrezilienciájának növelése az összes releváns ágazatban, az irányelv által már lefedett ágazatokban a belső piacon tapasztalható reziliencia következtetlenségeinek csökkentése és a közös helyzetismeret szintjének és a felkészülés és az elhárítás kollektív képességének javítása. Az elmúlt 4 évben az (EU) 2016/1148 irányelv végrehajtásával elértre épít.

1.5.2. Az uniós részvétel hozzáadott értéke (különböző tényezőkből fakadhat, pl. koordinációs nyereség, jogbiztonság, nagyobb hatékonyság vagy kiegészítő jelleg). E pont alkalmazásában az „uniós részvétel hozzáadott értéke” az uniós beavatkozásból származó érték, amely kiegészíti azt az értéket, amelyet egyébként a tagállamok egyedül hoztak volna létre.

A kiberreziliencia nem lehet tényleges az Unió egészében, ha azt nemzeti vagy regionális adatsílokon keresztül eltérő módon közelítik meg. A hálózat- és információbiztonsági irányelv ennek a hiányosságnak az orvoslásával volt hivatott rendezni a hálózati és információs rendszerek biztonságát nemzeti és uniós szinten. A kiberbiztonsági irányelv első időszakos felülvizsgálata azonban számos eredendő hibára mutatott rá, amelyek végül jelentős különbségeket eredményeztek a tagállamokban a képességek, a tervezés és a védelem szintje tekintetében, amelyek egyidejűleg befolyásolják hasonló vállalatok számára az egyenlő versenyfeltételeket a belső piacon.

A kiberbiztonsági irányelv jelenlegi intézkedéseinek túlmutató uniós beavatkozást elsősorban a következők indokolják: i. a probléma határokon átnyúló vonatkozásai; ii. az uniós fellépés lehetőségei a hathatós nemzeti politikák javítására és megkönnyítésére; iii. összehangolt és együttműködő hálózati és információs rendszerekkel kapcsolatos szakpolitikai fellépések a hatékony adatvédelem és a magánélet védelme céljából.

A megfogalmazott célkitűzések tehát jobban elérhetők uniós szintű fellépéssel, mintsem egyedül a tagállamok által.

1.5.3. Hasonló korábbi tapasztalatok tanulsága

A kiberbiztonsági irányelv az első horizontális belső piaci eszköz, amelynek célja a hálózatok és rendszerek kiberbiztonsági kockázatokkal szembeni rezilienciájának javítása az Unióban. 2016-os hatálybalépése óta már nagyban hozzájárult a kiberbiztonság közös szintjének emeléséhez a tagállamok körében. Az irányelv működésének és végrehajtásának felülvizsgálata azonban számos hiányosságra mutatott rá, amelyeket az egyre növekvő digitalizáció és a naprakészebb reagálás szükségessége mellett felülvizsgált jogi aktusban kell kezelni.

1.5.4. A többéves pénzügyi kerettel való összeegyeztethetőség és lehetséges szinergiák a többi megfelelő eszközzel

Az új javaslat teljes mértékben következetes és koherens más kapcsolódó kezdeményezésekkel, például a pénzügyi ágazat digitális működési rezilienciájáról szóló rendeletre irányuló javaslattal (DORA) és az alapvető szolgáltatásokat nyújtó kritikus szereplők rezilienciájáról szóló irányelvre irányuló javaslattal. Összhangban van az Európai

Elektronikus Hírközlési Szabályzattal, az Általános Adatvédelmi Rendelettel és az eIDAS-rendelettel is.

A javaslat a biztonsági unióra vonatkozó uniós stratégia lényeges részét képezi.

1.5.5. *A rendelkezésre álló különböző finanszírozási lehetőségek értékelése, ideértve az átcsoportosítás lehetőségét is*

Ezeknek a feladatoknak az ENISA általi irányítása speciális profilokat és kiegészítő munkaterhet tesz szükségessé, amelyek nem megoldhatóak a humánerőforrások növelése nélkül.

1.6. A javaslat/kezdeményezés tartama és becsült pénzügyi hatása

☐ **határozott időtartam**

- ☐ A javaslat/kezdeményezés hatályos: [NN/HH] ÉÉÉÉ és [NN/HH] ÉÉÉÉ
- ☐ Pénzügyi hatás ÉÉÉÉ-től ÉÉÉÉ-ig

☒ **határozatlan időtartam**

- beindítási időszak: 2022-től 2025-ig
- azt követően: rendes ütem

1.7. Tervezett irányítási módszer(ek)⁵⁷

☒ Bizottság általi **közvetlen irányítás**

a

- ☐ végrehajtó ügynökségeken keresztül

☐ **Megosztott irányítás** a tagállamokkal

☒ **Közvetett irányítás** a költségvetés végrehajtásával kapcsolatos feladatoknak a következőkre történő átruházásával:

- ☐ nemzetközi szervezetek és ügynökségeik (nevezze meg);
- ☐ az EBB és az Európai Beruházási Alap;
- ☒ a 70. és 71. cikkben említett szervek;
- ☐ közjogi szervek;
- ☐ magánjog alapján működő, közfeladatot ellátó szervek, olyan mértékben, amennyiben megfelelő pénzügyi garanciákat nyújtanak;
- ☐ a valamely tagállam magánjoga alapján működő, köz- és magánszféra közötti partnerség végrehajtásával megbízott és megfelelő pénzügyi garanciákat nyújtó szervek;
- ☐ az EUSZ V. címének értelmében a KKBP terén konkrét fellépések végrehajtásával megbízott, és a vonatkozó alap-jogiaktusban meghatározott személyek.

Megjegyzések

Az Európai Unió Kiberbiztonsági Ügynöksége, az ENISA, amelynek a kiberbiztonsági jogszabály új állandó megbízatást adott, segítséget nyújtana a tagállamoknak és a Bizottságnak a felülvizsgált kiberbiztonsági irányelv végrehajtásában.

A felülvizsgált kiberbiztonsági irányelv eredményeként 2022/23-tól az ENISA további cselekvési területekkel rendelkezik. Jóllehet ezekre a cselekvési területeket megbízatása alapján lefedik az ENISA általános feladatai, ezek további munkaterhet jelentenek az ügynökség számára. Pontosabban, a jelenlegi cselekvési területein túl, a felülvizsgált kiberbiztonsági irányelvre irányuló bizottsági javaslat értelmében az ENISA-nak munkaprogramjába külön be kell építenie többek között a következő intézkedéseket: i. európai biztonságírás-nyilvántartás kidolgozása és fenntartása (a javaslat 6. cikkének

⁵⁷

Az egyes irányítási módszerek ismertetése, valamint a költségvetési rendeletre való megfelelő hivatkozások megtalálhatók a Költségvetési Főigazgatóság honlapján: <https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>

(2) bekezdése), ii. az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (CyCLONe) titkárságának biztosítása (a javaslat 14. cikke), valamint éves jelentés kiadása a kiberbiztonság helyzetéről az EU-ban (a javaslat 15. cikke), iii. a tagállamok körében szakértői értékelések megszervezésének támogatása (a javaslat 16. cikke), iv. összesített eseményadatok összegyűjtése a tagállamoktól és technikai útmutatás kiadása (a javaslat 20. cikkének (9) bekezdése), v. nyilvántartás létrehozása és vezetése a határokon átnyúló szolgáltatásokat nyújtó szervezetek vonatkozásában (a javaslat 25. cikke).

Ezért 2022-től 5 kiegészítő teljes munkaidős egyenértéket igényelnek, amelynek megfelelő költségvetése évente körülbelül 0,61 millió EUR az új álláshelyek fedezésére.

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

Gyakoriság és feltételek

A Bizottság rendszeresen felülvizsgálja az irányelv működését, és jelentést tesz az Európai Parlamentnek és a Tanácsnak, először három évvel a hatálybalépés után.

A Bizottság értékeli az irányelv helyes tagállami átültetését is.

A javaslat nyomon követése és a beszámolás az (EU) 2019/881 RENDELET (kiberbiztonsági jogszabály) értelmében az ENISA állandó megbízatásában felvázolt elveket követi.

A tervezett nyomon követéshez használt adatforrások többnyire az ENISA-tól, az együttműködési csoporttól, a CSIRT-hálózattól és a tagállamok hatóságaitól származnak. Az ENISA, az együttműködési csoport és a CSIRT Hálózat jelentéseiből (ideértve az éves tevékenységi jelentéseket is) gyűjtött adatok mellett szükség esetén speciális adatgyűjtő eszközök is használhatók (például felmérések a nemzeti hatóságoknál, az Eurobarométer és a kiberbiztonsági hónap kampánya, valamint a páneurópai gyakorlatok jelentései).

2.2. Irányítási és kontrollrendszer(ek)

2.2.1. *Az irányítási módszer(ek), a finanszírozás végrehajtási mechanizmusai, a kifizetési módok és a javasolt kontrollstratégia indokolása*

A DG CNECT szakpolitikai területért felelős egysége irányítja az irányelv végrehajtását.

Ami az ENISA vezetését illeti, a kiberbiztonsági jogszabály 15. cikke részletes felsorolást tartalmaz az ENISA igazgatóságának ellenőrzési funkcióiról.

A kiberbiztonsági jogszabály 31. cikke értelmében az ENISA ügyvezető igazgatója felel az ENISA költségvetésének végrehajtásáért, és a Bizottság belső ellenőre ugyanolyan hatáskörrel rendelkezik az ENISA felett, mint a Bizottság szervezeti egységei felett. Az ENISA igazgatósága véleményt nyilvánít az ENISA végleges beszámolójáról.

2.2.2. *A felismert kockázatokkal és a csökkentésükre létrehozott belső kontrollrendszerekkel kapcsolatos információk*

Nagyon alacsony kockázatú, mivel a kiberbiztonsági irányelv ökoszisztémája már működik, és már lefedi az ENISA-t, amelynek állandó megbízatása van a kiberbiztonsági jogszabály 2019-es hatálybalépése után.

2.2.3. *A kontroll költséghatékonyságának becslése és indokolása (a „kontroll költségei ÷ a kezelt kapcsolódó források értéke” hányados) és a hibakockázat várható szintjeinek értékelése (kifizetéskor és záráskor)*

A kért költségvetési emelés az 1. címet alkalmazza, és célja a fizetések finanszírozása. Ez nagyon alacsony hibakockázatot jelent kifizetési szinten.

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

Tüntesse fel a meglévő vagy tervezett megelőző és védintézkedéseket, pl. a csalás elleni stratégiából.

Az ENISA megelőzési és védintézkedéseit kell alkalmazni, különösen az alábbiakat:

- A kért szolgáltatások vagy vizsgálatok kifizetéseit az ügynökség személyzete a kifizetés előtt ellenőrzi, figyelembe véve a szerződéses kötelezettségeket, a gazdasági elveket és a helyes pénzügyi vagy irányítási gyakorlatot. A csalás elleni rendelkezéseket (felügyelet, jelentéstételi követelmények stb.) az ügynökség és az esetleges kifizetések címzettjei között megkötött valamennyi megállapodás és szerződés tartalmazza.
- A csalás, a korrupció és más jogellenes tevékenységek elleni küzdelem érdekében az Európai Csalás Elleni Hivatal (OLAF) által lefolytatott vizsgálatokról szóló, 1999. május 25-i 883/2013/EU, Euratom európai parlamenti és tanácsi rendelet rendelkezéseit korlátozás nélkül alkalmazni kell.
- A CSA 33. cikke értelmében az ENISA 2019. december 28-ig csatlakozott az Európai Parlament, az Európai Unió Tanácsa és az Európai Községek Bizottsága között az Európai Csaláselleni Hivatal (OLAF) belső vizsgálatairól szóló, 1999. május 25-i intézményközi megállapodáshoz. Az ENISA haladéktalanul kiadja az ügynökség összes alkalmazottjára vonatkozó megfelelő rendelkezéseket.

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

3.1. A többéves pénzügyi keret érintett fejezete(i) és a költségvetésben javasolt új kiadási sor(ok)

- Meglévő költségvetési sorok

A többéves pénzügyi keret fejezeteinek és költségvetési tételeinek rendjében.

A többéves pénzügyi keret fejezete	Költségvetési sor	Kiadás típusa	Hozzájárulás			
	Szám	diff./nem diff. ⁵⁸	EFTA-országoktól ⁵⁹	tagjelölt országoktól ⁶⁰	harmadik országoktól	a költségvetési rendelet 21. cikke (2) bekezdésének b) pontja értelmében
2	02 10 04	/Nem diff.	IGEN	NEM	NEM	/NEM

- Kért új költségvetési tételek

A többéves pénzügyi keret fejezeteinek és költségvetési tételeinek rendjében.

A többéves pénzügyi keret fejezete	Költségvetési sor	A kiadás típusa	Hozzájárulás			
	Szám	diff./nem	EFTA-	tagjelölt	harmadik	a költségvetési rendelet 21. cikke

⁵⁸ Diff. = Differenciált előirányzatok/Nem diff. = Nem differenciált előirányzatok.

⁵⁹ EFTA: Európai Szabadkereskedelmi Társulás.

⁶⁰ Tagjelölt országok és adott esetben a nyugat-balkáni potenciális tagjelölt országok.

		diff.	országoktól	országoktól	országoktól	(2) bekezdésének b) pontja értelmében
	[XX.YY.YY.YY]		IGEN/NE EM	IGEN/NE M	IGEN/NE EM	IGEN/NEM

3.2. A kiadásokra gyakorolt becsült hatás

3.2.1. A kiadásokra gyakorolt becsült hatás összefoglalása

millió EUR (három tizedesjegyig)

A többéves pénzügyi keret fejezete	Szám	[Fejezet...2 gazdaság.....]	Egységes	piac,	innováció	és	digitális
------------------------------------	------	--------------------------------	----------	-------	-----------	----	-----------

[Testület]: <... ENISA....>			Év N ⁶¹ 2022	Év N+1 2023	Év N+2 2024	Év N+3 2025	Adjon meg annyi évet, amennyi szükséges a hatás időtartamának megjelenítéséhez (lásd az 1.6. pontot)			ÖSSZESEN
							2026	2027		
1. cím:	Kötelezettségvál lási előirányzatok	1.	0,61	0,61	0,61	0,61	0,61	0,61		3,66
	Kifizetési előirányzatok	2.	0,61	0,61	0,61	0,61	0,61	0,61		3,66
2. cím:	Kötelezettségvál lási előirányzatok	(1a)								
	Kifizetési előirányzatok	(2a)								
3. cím:	Kötelezettségvál lási előirányzatok	(3a)								
	Kifizetési előirányzatok	(3b)								
A [testület] ÖSSZES előirányzata <ENISA.....>	Kötelezettségvál lási előirányzatok	=1+1a +3a	0,61	0,61	0,61	0,61	0,61	0,61		3,66
	Kifizetési előirányzatok	=2+2a	0,61	0,61	0,61	0,61	0,61	0,61		3,66

⁶¹ Az N. év a javaslat/kezdemenyezés végrehajtásának kezdete. Kérjük, cserélje ki az „N” értéket a megvalósítás várható első évére (például: 2021). Ugyanez a következő években is.

		+3b								
--	--	-----	--	--	--	--	--	--	--	--

A többéves pénzügyi keret fejezete	5	„Igazgatási kiadások”
---	----------	-----------------------

millió EUR (három tizedesjegyig)

		Év N	Év N+1	Év N+2	Év N+3	Adjon meg annyi évet, amennyi szükséges a hatás időtartamának megjelenítéséhez (lásd az 1.6. pontot)		ÖSSZESEN
Főigazgatóság: <.....>								
• Humánerőforrás								
• Egyéb igazgatási kiadások								
Főigazgatóság ÖSSZESEN <.....>	Előirányzatok							

A többéves pénzügyi keret 5. FEJEZETE szerinti ÖSSZES előirányzat	(Összes kötelezettségvállalási előirányzat = Összes kifizetési előirányzat)								
--	--	--	--	--	--	--	--	--	--

millió EUR (három tizedesjegyig)

		Év N ⁶² 2022	Év N+1 2023	Év N+2 2024	Év N+3 2025	Adjon meg annyi évet, amennyi szükséges a hatás időtartamának megjelenítéséhez (lásd az 1.6. pontot)		ÖSSZESEN
						2026	2027	
Előirányzatok ÖSSZESEN a többéves pénzügyi keret 1–5. FEJEZETE alatt	Kötelezettségvállalási előirányzatok	0,61	0,61	0,61	0,61	0,61	0,61	3,66
	Kifizetési előirányzatok	0,61	0,61	0,61	0,61	0,61	0,61	3,66

⁶² Az N. év a javaslat/kezdemenyezés végrehajtásának kezdete. Kérjük, cserélje ki az „N” értéket a megvalósítás várható első évére (például: 2021). Ugyanez a következő években is.

3.2.2. A [testület] előirányzataira gyakorolt becsült hatás

- ☒ A javaslat/kezdeményezés nem vonja maga után operatív előirányzatok felhasználását
- ☐ A javaslat/kezdeményezés az alábbi operatív előirányzatok felhasználását vonja maga után:

kötelezettségvállalási előirányzatok, millió EUR (három tizedesjegyig)

Adja meg a célokat és a teljesítéseket			Év N		Év N+1		Év N+2		Év N+3		Adjon meg annyi évet, amennyi szükséges a hatás időtartamának megjelenítéséhez (lásd az 1.6. pontot)								ÖSSZESEN	
	TELJESÍTÉSEK																			
	↓	Típus ₆₃	Átlag költség	Szám	Költsé g	Szám	Költsé g	Szám	Költsé g	Szám	Költsé g	Szám	Költsé g	Szám	Költsé g	Szám	Költsé g	Összes szám	Összes költség	
1. sz. KONKRÉT CÉLKITŰZÉS ⁶⁴ ...																				
– Teljesítés																				
– Teljesítés																				
– Teljesítés																				
Az 1. sz. konkrét célkitűzés részösszege																				
2. sz. KONKRÉT CÉLKITŰZÉS ...																				
– Teljesítés																				
A 2. sz. konkrét célkitűzés részösszege																				

⁶³ A teljesítések a nyújtandó termékek és szolgáltatások (pl.: finanszírozott diákcserék száma, megépített utak km-száma stb.).

⁶⁴ Az 1.4.2. pontban leírtak szerint. „Egyedi célkitűzés(ek)...”

ÖSSZES KÖLTSÉG																
----------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

3.2.3. Az ENISA humánerőforrására gyakorolt becsült hatás

3.2.3.1. Összegzés

A felülvizsgált kiberbiztonsági irányelv eredményeként 2022/23-tól az ENISA-nak további feladatai lesznek. Noha ezekre a feladatokra az ENISA megbízása vonatkozik, ezek további munkaterhet jelentenek az ügynökség számára. Pontosabban, a jelenlegi feladatai mellett, a felülvizsgált kiberbiztonsági irányelvre vonatkozó bizottsági javaslat alapján az ENISA feladata lesz többek között i. egy európai biztonságirés-nyilvántartás kidolgozása és fenntartása (6. cikk (2) bekezdés), ii. az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (CyCLONe) titkárságának biztosítása (14. cikk), valamint éves jelentés kiadása az EU kiberbiztonságának helyzetéről (15. cikk), iii. a tagállamok közötti szakértői értékelések megszervezésének támogatása (16. cikk), iv. összesített eseményadatok összegyűjtése a tagállamoktól és műszaki útmutatás kiadása (20. cikk (9) bekezdés), v. a határon átnyúló szolgáltatásokat nyújtó szervezetek nyilvántartásának létrehozása és vezetése (25. cikk).

Ezért 2022-től 5 kiegészítő FTE-t igényelnek a megfelelő költségvetéssel ezen új álláshelyek fedezésére.

- ☐ A javaslat/kezdeményezés nem vonja maga után igazgatási előirányzatok felhasználását
- ☒ A javaslat/kezdeményezés az alábbi igazgatási előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyre)

	Év N ⁶⁵ 2022	Év N+1 2023	Év N+2 2024	Év N+3 2025	Adjon meg annyi évet, amennyi szükséges a hatás időtartamának megjelenítéséhez (lásd az 1.6. pontot)		ÖSSZES EN
					2026	2027	

Ideiglenes alkalmazottak (AD fokozat)	0,450	0,450	0,450	0,450	0,450	0,450	2,7
Ideiglenes alkalmazottak (AST fokozat)							
Szerződéses alkalmazottak	0,160	0,160	0,160	0,160	0,160	0,160	0,96
Kirendelt nemzeti szakértők							

⁶⁵

Az N. év a javaslat/kezdeményezés végrehajtásának kezdete. Kérjük, cserélje ki az „N” értéket a megvalósítás várható első évére (például: 2021). Ugyanez a következő években is.

ÖSSZESEN	0,61	0,61	0,61	0,61	0,61	0,61		3,66
-----------------	-------------	-------------	-------------	-------------	-------------	-------------	--	-------------

Személyi követelmények (FTE):

	Év N ⁶⁶ 2022	Év N+1 2023	Év N+2 2024	Év N+3 2025	Adjon meg annyi évet, amennyi szükséges a hatás időtartamának megjelenítéséhez (lásd az 1.6. pontot)			ÖSSZESEN
					2026	2027		

Ideiglenes alkalmazottak (AD fokozat)	3	3	3	3	3	3		18
Ideiglenes alkalmazottak (AST fokozat)								
Szerződéses alkalmazottak	2	2	2	2	2	2		12
Kirendelt nemzeti szakértők								

ÖSSZESEN	5	5	5	5	5	5		30
-----------------	----------	----------	----------	----------	----------	----------	--	-----------

3.2.3.2. Becsült humánerőforrás-szükséglet a gazda főigazgatóság számára

- ☐ A javaslat/kezdeményezés nem igényel humánerőforrást.
- ☐ A javaslat/kezdeményezés az alábbi humánerőforrás-igénnyel jár:

A becslés teljes összegben (vagy legfeljebb egy tizedesjegyig) kell kifejezni

	Év N	Év N+1	N+2 év	N+3 év	Adjon meg annyi évet, amennyi szükséges a hatás időtartamának megjelenítéséhez (lásd az 1.6. pontot)		
• A létszámtervben szereplő álláshelyek (tisztviselők és ideiglenes alkalmazottak)							
XX 01 01 01 (A központban és a bizottsági képviselőket)							
XX 01 01 02 (Képviselők)							

⁶⁶

Az N. év a javaslat/kezdeményezés végrehajtásának kezdete. Kérjük, cserélje ki az „N” értéket a megvalósítás várható első évére (például: 2021). Ugyanez a következő években is.

XX 01 05 01 (Közvetett kutatás)							
10 01 05 01 (Közvetlen kutatás)							
• Külső munkatársak teljes munkaidős egyenértékben (FTE) kifejezve⁶⁷:							
XX 01 02 01 (AC, END, INT a „teljes keretből”)							
XX 01 02 02 (AC, AL, END, INT és JPD a küldöttségeknél)							
XX 01 04 yy⁶⁸	– a központban ⁶⁹						
	– a küldöttségeknél						
XX 01 05 02 (AC, END, INT – közvetett kutatás)							
10 01 05 02 (AC, END, INT – közvetlen kutatás)							
Egyéb költségvetési sor (kérjük megnevezni)							
ÖSSZESEN							

XX az érintett szakpolitikai terület vagy költségvetési cím.

A humánerőforrás-igényeknek az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt és/vagy az adott főigazgatóságon belül átcsoportosított személyzettel kell eleget tenni. A források adott esetben a meglévő költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további juttatásokkal.

Az elvégzendő feladatok leírása:

Tisztviselők és ideiglenes alkalmazottak	
Külső munkatársak	

Az FTE egységek költségének kiszámítását az V. melléklet 3. szakaszában kell feltüntetni.

⁶⁷ AC = szerződéses alkalmazott; AL = helyi alkalmazott; END = kirendelt nemzeti szakértő; INT = kölcsönmunkaerő (átmeneti alkalmazott); JPD = küldöttségi pályakezdő szakértő.

⁶⁸ Az operatív előirányzatokból finanszírozott külső munkatársakra vonatkozó részleges felső határérték (korábban: BA-tételek).

⁶⁹ Főleg a strukturális alapok, az Európai Mezőgazdasági Vidékfejlesztési Alap (EMVA) és az Európai Halászati Alap (EHA) esetében.

3.2.4. Összeegyeztethetőség a folyó többéves pénzügyi kerettel

- ☒ A javaslat/kezdeményezés összeegyeztethető a jelenlegi többéves pénzügyi kerettel.
- ☐ A javaslat/kezdeményezés a többéves pénzügyi keret vonatkozó fejezetének átprogramozását vonja maga után.

Magyarázza el, mi szükséges az újraprogramozáshoz, megadva az érintett költségvetési sorokat és a hozzájuk tartozó összegeket.

A javaslat összeegyeztethető a 21/27-es többéves pénzügyi kerettel.

Az ENISA humán erőforrás-növekedésének fedezésére kért költségvetés ellentételezése a Digitális Európa Program (DEP) költségvetésének ugyanezzel az összeggel történő csökkentésével történik.

- ☐ A javaslat/kezdeményezés a rugalmassági eszköz alkalmazását vagy a többéves pénzügyi keret felülvizsgálatát igényli⁷⁰.

Magyarázza el, hogy mire van szükség, részletezve az érintett fejezeteket és költségvetési sorokat, valamint a hozzájuk tartozó összegeket.

3.2.5. Harmadik felek részvétele a finanszírozásban

- A javaslat/kezdeményezés nem irányoz elő harmadik felek általi társfinanszírozást
- A javaslat/kezdeményezés az alábbiak szerinti becsült társfinanszírozást ír elő:

millió EUR (három tizedesjegyig)

	Év N	Év N+1	Év N+2	Év N+3	Adjon meg annyi évet, amennyi szükséges a hatás időtartamának megjelenítéséhez (lásd az 1.6. pontot)			Összesen
Adja meg a társfinanszírozó szervet								
Társfinanszírozott előirányzatok ÖSSZESEN								

⁷⁰

Lásd a 2014–2020-as időszakra vonatkozó többéves pénzügyi keretről szóló, 2013. december 2-i 1311/2013/EU, Euratom tanácsi rendelet, 11. és 17. cikk.

3.3. A bevételre gyakorolt becsült hatás

- ☐ A javaslatnak/kezdemenyezésnek nincs pénzügyi hatása a bevételre.
- ☐ A javaslatnak/kezdemenyezésnek van pénzügyi hatása – a bevételre gyakorolt hatása a következő:
 - ☐ a javaslat a saját forrásokra gyakorol hatást
 - ☐ a javaslat más bevételre gyakorol hatást
 - ☐ kérjük adja meg, hogy a bevétel kiadási sorhoz van-e rendelve

millió EUR (három tizedesjegyig)

Bevételi költségvetési sor:	A folyó pénzügyi évre rendelkezésre álló előirányzatok	A javaslat/kezdemenyezés hatása ⁷¹						
		Év N	Év N+1	Év N+2	Év N+3	Adjon meg annyi évet, amennyi szükséges a hatás időtartamának megjelenítéséhez (lásd az 1.6. pontot)		
... jogcímcsoport								

A címzett bevételek esetében tüntesse fel az érintett kiadáshoz tartozó költségvetési sor(oka)t.

--

Adja meg a bevételre gyakorolt hatás kiszámításának módszerét.

--

⁷¹

A tradicionális saját források (vámok, cukorilletékek) tekintetében nettó összegeket, vagyis a 20 %-kal (beszedési költségek) csökkentett bruttó összegeket kell megadni.