



Brüsszel, 2021. november 26.
(OR. en)

14337/21

Intézményközi referenciaszám:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

FELJEGYZÉS

Küldi:	a Tanács Főtitkársága
Címzett:	a Tanács
Előző dok. sz.:	9583/2/21, 11724/21
Biz. dok. sz.:	14150/20
Tárgy:	Javaslat – Az Európai Parlament és a Tanács irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről – Általános megközelítés

I. BEVEZETÉS

1. A Bizottság 2020. december 16-án elfogadta az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről szóló irányelvre irányuló javaslatot (a felülvizsgált NIS-irányelv vagy „NIS 2 irányelv”)¹ azzal a céllal, hogy az felváltsa a hálózati és információs rendszerek biztonságáról szóló jelenlegi irányelvet (NIS-irányelv)².

¹ 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.

² 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.

A javaslat egyike volt a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiában³ előirányzott cselekvéseknek, amelyek célja annak biztosítása, hogy a polgárok és az üzleti vállalkozások megbízható digitális technológiák előnyeit élvezzék.

2. Az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikkén alapuló javaslat célja, hogy tovább javítsa az állami és magánszervezetek, az illetékes hatóságok és az egész Unió rezilienciáját és kiberbiztonsági eseményekre való reagálási képességét.
3. Az Európai Parlamentben az Ipari, Kutatási és Energiaügyi Bizottság (ITRE) felelős a javaslatért. Az ITRE bizottság 2021. október 28-án fogadta el az előadó jelentését.
4. Az Európai Gazdasági és Szociális Bizottság 2021. április 28-án fogadta el véleményét.
5. Az Állandó Képviselők Bizottsága 2021. február 3-án úgy határozott, hogy konzultál a Régiók Európai Bizottságával a javaslatról⁴. A Régiók Európai Bizottsága eddig még nem nyilvánított véleményt.
6. Az európai adatvédelmi biztos 2021. március 11-én nyilvánított véleményt⁵.
7. A digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról szóló, 2021. március 22-i következtetésekben⁶ a Tanács nyugtázta az új javaslatot, amely a kiberbiztonsági irányelvre épül, és ismételten hangsúlyozta, hogy támogatja a nemzeti kiberbiztonsági keretek megerősítését és harmonizálását, valamint a tagállamok közötti tartós együttműködést.
8. Az Európai Tanács a 2021. október 21–22-i következtetéseiben felszólított a NIS-irányelvre vonatkozó javaslattal kapcsolatos munka előmozdítására.

³ 14133/20.

⁴ 5573/21.

⁵ 5/2021. sz. vélemény a kiberbiztonsági stratégiáról és a NIS 2.0 irányelvről.

⁶ 6722/21.

II. A TANÁCS ELŐKÉSZÍTŐ SZERVEI KERETÉBEN VÉGZETT MUNKA

9. A Tanácsban a javaslat vizsgálatára a kiberkérdésekkel foglalkozó horizontális munkacsoport (a továbbiakban: HWPCI) keretében került sor. A javaslat vizsgálata a portugál elnökség alatt, január 19-én kezdődött a javaslat alapos átolvasásával, amelynek keretében a tagállamoknak lehetőségük nyílt kérdéseik feltevésére és főbb aggályaik megfogalmazására, a Bizottság pedig részletes magyarázattal szolgált a felülvizsgált irányelvet érintő módosításokról.
10. A portugál elnökség alatt a HWPCI 17 ülést szentelt a javaslat ismertetésének és átolvasásának. Az átolvasás nyomán 2021. június 4-én az elért eredményekről szóló jelentést nyújtottak be a TTE Tanácsnak.
11. A munka a szlovén elnökség alatt folytatódott és intenzívebbé vált annak érdekében, hogy a Tanács (Közlekedés, Távközlés és Energia) 2021. december 3-i ülésén általános megközelítést lehessen elérni. A szlovén elnökség 15 ülést szentelt a NIS 2 irányelvről szóló javaslat felülvizsgálatának, és valamennyi szinten számos kétoldalú megbeszélést szervezett.
12. A HWPCI munkájának középpontjában a javaslat újraszövegezése állt, először is a NIS 2 irányelv és az ágazati jogszabályok közötti kölcsönhatás és a hatály tekintetében, különösen ami a közigazgatást, a DNS gyökérszervereket és a kizáró rendelkezést illeti, később pedig többek között a szakértői értékelések, a joghatóság és a kölcsönös segítségnyújtás, az összehangolt sebezhetőség-feltárás, a doménnevek és nyilvántartási adatok adatbázisai, valamint a nemzetközi együttműködés tekintetében.
13. 2021. szeptember 21-én előterjesztették az irányelvjavaslat szövegére vonatkozó első kompromisszumos javaslatot⁷, amely a tagállamok által benyújtott írásbeli észrevételeken és informális dokumentumokon, valamint a NIS 2 irányelv és az ágazati jogszabályok közötti kölcsönhatásra és a NIS 2 irányelv hatályára vonatkozó, előző kompromisszumos javaslatokon alapul.

⁷ 12019/21.

14. Az elnökségi kompromisszumos javaslat legutóbb felülvizsgált szövegéről⁸ munkacsoporti szinten 2021. november 22-én zajlott megbeszélés. A delegációk általánosságban üdvözltek a kompromisszumos szöveget, néhány delegáció azonban továbbra is vizsgálati fenntartással élt, illetve észrevételeket tett a kompromisszumos javaslat egyes részeivel kapcsolatban. A szöveg egyes részeit illetően továbbra is javasoltak némi technikai jellegű újraszövegezést.

III. TARTALMI KÉRDÉSEK

15. A munkacsoporti szintű megbeszélések alapján a főbb politikai kérdések a következők:

a) Hatály (2. cikk)

A tagállamok már a NIS 2 irányelvről szóló javaslattal kapcsolatos megbeszélések kezdete óta azt tartották a leginkább aggályosnak, hogy az irányelv hatálya a korábbinál sokkal több szervezetre terjed ki, valamint különösen azt, hogy az irányelv olyan méretkorlát-szabályt vezet be, amelynek értelmében minden olyan közép- és nagyvállalkozás, amely a NIS 2 irányelv hatálya alá tartozó ágazatokban működik vagy a NIS 2 irányelv hatálya alá tartozó szolgáltatásokat nyújt, az irányelv hatálya alá tartozik. Noha ez az általános szabály a kompromisszumos javaslatból sem került ki, a javaslat kiegészült olyan rendelkezésekkel, amelyek célja a szükséges arányosság és a nagyobb mértékű kockázatkezelés biztosítása, valamint a kritikus szintre vonatkozó egyértelmű kritériumok meghatározása annak megállapítása tekintetében, hogy mely szervezetek tartoznak az irányelv hatálya alá. A kompromisszumos javaslat ezenkívül egyedi rendelkezéseket tartalmaz a felügyeleti intézkedések alkalmazásának kockázatalapú rangsorolására vonatkozóan.

⁸ 12019/5/21 REV 5.

b) Közigazgatási szervek (a 2. cikk (2a) bekezdése)

A közigazgatási szerveknek a NIS 2 irányelv hatálya alá vonásáról élénk vita folyt, tekintettel arra, hogy a közigazgatási ágazat határozottan elkülönül a NIS 2 irányelv hatálya alá tartozó többi ágazattól. Az elnökség olyan kiegyensúlyozott megközelítés kialakítására törekedett, amely figyelembe veszi a nemzeti közigazgatási keretek sajátosságait és bizonyos fokú rugalmasságot biztosít a tagállamok számára annak meghatározása terén, hogy mely közigazgatási szervek tartoznak a NIS 2 irányelv hatálya alá. A kompromisszumos szöveg értelmében ezért a NIS 2 irányelv a központi kormányzatok közigazgatási szerveire alkalmazandó, a tagállamok pedig dönthetnek úgy, hogy az irányelv a regionális és helyi szintű közigazgatási szervekre is alkalmazandó legyen.

c) A kizáró rendelkezés (a 2. cikk (3a) és (3aa) bekezdése)

A tagállamok pontosabbá kívánták tenni azt a rendelkezést, amely kizárja az irányelv hatálya alól egyrészt azokat a szervezeteket, amelyek főként a védelem, a nemzetbiztonság, a közbiztonság vagy a bűnüldözés területén végeznek tevékenységet, másrészt pedig a nemzetbiztonsággal vagy a védelemmel kapcsolatos tevékenységeket. Az irányelv az igazságszolgáltatásra, a parlamentekre és a központi bankokra sem alkalmazandó.

d) Az ágazati jogszabályokkal való kölcsönhatás

A tagállamok hangsúlyozták, hogy a NIS 2 irányelvet össze kell hangolni az ágazati jogszabályokkal, különösen a pénzügyi ágazat digitális működési rezilienciájáról szóló rendelettel (DORA-rendelet), valamint a kritikus fontosságú szervezetek rezilienciájáról szóló irányelvvel (CER-irányelv). A NIS 2 irányelvben, amelynek a kiberbiztonságra vonatkozó minimumharmonizáció alapjául kell szolgálnia, külön cikk foglalkozik az ágazatspecifikus uniós jogi aktusokkal (2b. cikk). A CER-irányelvvel való kölcsönhatás tekintetében a kompromisszumos javaslat egyértelműbbé teszi a „minden veszélyre kiterjedő” megközelítést. A szöveg a vonatkozó jogszabályok szerinti illetékes hatóságok közötti együttműködési megállapodások tekintetében is fontos rendelkezésekkel egészült ki.

e) Szakértői tanulás (16. cikk)

Néhány kivételtől eltekintve a tagállamok ellenezték, hogy a Bizottság kötelező szakértői értékeléseket vezessen be. A javasolt kompromisszum biztosítja, hogy a szakértői tanulásra vonatkozó új mechanizmus a kölcsönös bizalmon alapuljon és a tagállamok által irányított önkéntes folyamat keretében valósuljon meg.

f) Joghatóság és területi elv (24. cikk), valamint kölcsönös segítségnyújtás (34. cikk)

A tagállamok aggodalmuknak adtak hangot az IKT-ágazatban működő szervezetek esetében a Bizottság által javasolt differenciált joghatóság következményeivel kapcsolatban. A kompromisszumos szövegben egyértelműbbé vált a szervezettípusok szerinti joghatóság kérdése, a kölcsönös segítségnyújtásra vonatkozó rendelkezések megfogalmazása pedig erősebb lett.

g) Bejelentési kötelezettségek (20. cikk)

A tagállamok azzal kapcsolatos aggályai nyomán, hogy a jelentős kiberbiztonsági fenyegetések bejelentésére vonatkozó kötelezettség miatt a NIS 2 irányelv hatálya alá tartozó szervezetekre túlzott terhek hárulnának, valamint hogy a kötelezettség túlzott mértékű bejelentésekhez vezethet, ez a kötelezettség kikerült a kompromisszumos szövegből.

IV. ÖSSZEGZÉS

16. Az Állandó Képviselők Bizottsága 2021. november 24-én megállapodásra jutott a mellékletben foglalt kompromisszumos szövegről, és úgy határozott, hogy általános megközelítés elfogadása céljából benyújtja azt a Tanácsnak (Közlekedés, Távközlés és Energia).
17. Felkérjük ezért a Tanácsot, hogy a 2021. december 3-i ülésén hagyja jóvá az elnökség által előterjesztett, a mellékletben foglalt kompromisszumos szöveget és fogadjon el általános megközelítést.

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE

**az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről,
valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU)
2016/1148 irányelv hatályon kívül helyezéséről**

(EGT-vonatkozású szöveg)

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

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

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére⁹,

tekintettel a Régiók Bizottságának véleményére¹⁰,

rendes jogalkotási eljárás keretében,

⁹ HL C , , . o.

¹⁰ HL C , , . o.

mivel:

- (1) Az Európai Parlament és a Tanács (EU) 2016/1148 irányelvének¹¹ 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. Az említett irányelv **a hálózati és információs rendszerek biztonságára** vonatkozó nemzeti [...] stratégiák meghatározásával, a nemzeti képességek kialakításával és az egyes tagállamok által azonosított alapvető infrastruktúrákra és szereplőkre vonatkozó szabályozási intézkedések végrehajtásával biztosította a nemzeti keretek kiteljesítését. Az együttműködési csoport¹², valamint **a [...] nemzeti számítógép-biztonsági eseményekre reagáló csoportok hálózata** („a CSIRT-ek hálózata”)¹³ létrehozásával hozzájárult az uniós szintű együttműködéshez is. Ezen eredmények ellenére az (EU) 2016/1148 irányelv felülvizsgálata olyan hiányosságokat tárt fel, amelyek megakadályozzák, hogy eredményesen kezelje az aktuális és felmerülő kiberbiztonsági kihívásokat.

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., 2016.7.19., 1. o.).

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

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

- (3) A hálózati és információs rendszerek a mindennapi élet központi jellemzőjévé fejlődtek a társadalom gyors digitális transzformációjával és összekapcsoltságával, beleértve a határokon átnyúló cseréket is. Ez a fejlődés a kiberbiztonsági fenyegetettség bővüléséhez vezetett, új kihívásokat támasztva, amelyek minden tagállamban kiigazított, koordinált és innovatív reagálást igényelnek. A kiberbiztonsági események száma, nagysága, kifinomultsága, gyakorisága és hatása növekszik, ami komoly veszélyt jelent a hálózati és információs rendszerek működésére. Ennek következtében a kiberbiztonsági események akadályozhatják a belső piacon a gazdasági tevékenységek folytatását, pénzügyi veszteségeket okozhatnak, alááshatják a felhasználók bizalmát, és jelentős károkat okozhatnak az Unió gazdaságában és a társadalmában. A kiberbiztonsági felkészültség és hatékonyság ezért most minden eddiginél elengedhetetlenebb a belső piac megfelelő működéséhez.
- (4) Az (EU) 2016/1148 irányelv jogalapja az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikke, amelynek célja a belső piac megteremtése és működésének biztosítása 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, részletességi 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 ha egy tagállamban a kiberbiztonsági [...] **intézkedések** kialakítása vagy végrehajtása esetleg elmarad az optimálistól, az valószínűleg visszahat más tagállamok kiberbiztonsági szintjére is, különös tekintettel az intenzív, határokon átnyúló cserékre. Az (EU) 2016/1148 irányelv felülvizsgálata jelentős eltérésekre világított rá a tagállamok általi végrehajtás terén, többek között a hatállyal kapcsolatban is, amelynek behatárolása nagyrészt a tagállamok mérlegelési jogkörében maradt. Az (EU) 2016/1148 irányelv szintén nagyon tág mérlegelési jogkört biztosított a tagállamoknak a biztonsággal és a biztonsági eseményekkel kapcsolatban az irányelvben meghatározott bejelentési kötelezettségek végrehajtása tekintetében. Ezeket a kötelezettségeket tehát az egyes tagállamok 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 érintve a szolgáltatások határokon átnyúló nyújtását és a kiberreziliencia szintjét az eltérő [...] **intézkedések** alkalmazása miatt. Ennek az irányelvnek az a célja, hogy kiküszöbölje a tagállamok közötti ilyen nagy eltéréseket, különösen olyan minimumszabályok megállapításával, amelyek révén összehangolt szabályozási keret működik, 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 a kötelezettségek tényleges érvényesítéséhez. Ezért az (EU) 2016/1148 irányelvet hatályon kívül kell helyezni, és helyébe ezt az irányelvet kell léptetni.

- (6) [...] A tagállamok **számára biztosítani kell** a lehetőséget, hogy meg hozzák az alapvető biztonsági érdekeik védelméhez, a közrend és a közbiztonság megóvásához, valamint a bűncselekmények nyomozásának, felderítésének és a büntetőeljárások lefolytatásának lehetővé tételéhez szükséges intézkedéseket [...]. [...] **Az irányelv nem alkalmazandó az e területeken tevékenységet folytató bizonyos állami vagy magánszervezetekre. Nem alkalmazandó továbbá a szervezetek e területeken végzett tevékenységeire. Ezenkívül egyetlen tagállamot sem lehet kötelezni arra, hogy olyan információkat szolgáltatson, amelyek közlése ellentétes lenne alapvető közbiztonsági érdekeivel. [...] Figyelembe kell venni a minősített adatok védelmére vonatkozó nemzeti [...] vagy uniós szabályokat, a titoktartási megállapodásokat és az informális titoktartási megállapodásokat, például a TLP-protokollt¹⁴.**
- (6a) **A személyes adatok és a magánélet védelmére vonatkozó uniós jogszabályokat alkalmazni kell a személyes adatok ezen irányelv szerinti bármely kezelésére. Ez az irányelv különösen nem érinti az Európai Parlament és a Tanács (EU) 2016/679 rendeletét, valamint 2002/58/EK irányelvét, és ezért különösen nem érintheti a vonatkozó uniós adatvédelmi jogszabályoknak való megfelelés nyomon követésében illetékes független felügyeleti hatóságok feladatait és hatásköreit.**

¹⁴ A TLP-protokoll 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).

- (7) Az (EU) 2016/1148 irányelv hatályon kívül helyezésével az ágazati alkalmazási kört ki kell terjeszteni a gazdaság nagyobb részére, a (4)–(6) preambulumbekkezdésben foglalt megfontolásokra figyelemmel. Az (EU) 2016/1148 irányelv hatálya alá tartozó ágazatok körét ezért ki kell terjeszteni, hogy átfogóan lefedjék azokat az ágazatokat és szolgáltatásokat, amelyek létfontosságúak a belső piacon végzett 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 szereplőkre vonatkozó kritériumoknak („azonosítási eljárás”). A tagállamok között e tekintetben mutatkozó nagy eltérések kiküszöbölése, valamint az összes érintett szervezet vonatkozásában a kockázatkezelési követelmények és a bejelentési 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 magában kell foglalnia 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 tartozik. [...]

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

- (8a) **Annak biztosítása érdekében, hogy világosan áttekinthető legyen, hogy mely szervezetek tartoznak ezen irányelv hatálya alá, a tagállamoknak lehetőséget kell biztosítani arra, hogy nemzeti önbejelentési mechanizmusokat hozzanak létre, amelynek keretében előírják az ezen irányelv hatálya alá tartozó valamennyi szervezet számára, hogy legalább a nevüket, címüket, elérhetőségi adataikat, tevékenységi ágazatukat vagy az általuk nyújtott szolgáltatás típusát, valamint adott esetben az általuk nyújtott szolgáltatások helye szerinti tagállamok jegyzékét nyújtsák be az ezen irányelv szerinti illetékes hatóságoknak vagy a tagállamok által erre a célra kijelölt szerveknek. Amennyiben nemzeti szinten már léteznek nyilvántartások, a tagállamok dönthetnek az ezen irányelv hatálya alá tartozó szervezetek meghatározását lehetővé tevő megfelelő mechanizmusokról.**
- (9) [...] Az irányelv hatálya alá kell tartozniuk azoknak a **mikro- vagy** kisvállalkozásoknak [...] is, amelyek megfelelnek bizonyos kritériumoknak, amelyek alapján kulcsfontosságú szerepet töltenek be a tagállamok gazdasága vagy társadalma, illetve bizonyos ágazatok vagy szolgáltatástípusok szempontjából. A tagállamok számára elő kell írni, hogy [...] benyújtsák [...] a Bizottságnak **legalább az azonosított szervezetek számára, az ágazatukra vagy az általuk nyújtott szolgáltatás típusára vonatkozó releváns információkat, valamint azon konkrét kritériumokat, amelyek alapján e szervezeteket azonosították. A tagállamok dönthetnek úgy, hogy ha a nemzetbiztonsági szabályok megengedik, benyújtják a Bizottságnak az ilyen szervezetek nevét is.**
- (9a) **Azok a közigazgatási szervek, amelyek a nemzetbiztonság, a védelem, a közbiztonság vagy a bűnüldözés területén folytatnak tevékenységet, továbbá az igazságszolgáltatás, a parlamentek és a központi bankok ki vannak zárva ezen irányelv hatálya alól. Ezen irányelv alkalmazásában a szabályozási hatáskörrel rendelkező szervezetek nem tekintendők a bűnüldözés területén tevékenységet folytató szervezetnek, ezért nincsenek ezen az alapon kizárva az irányelv hatálya alól. Ezenkívül nem tartoznak az irányelv hatálya alá a központi kormányzat azon közigazgatási szervei, amelyeket valamely nemzetközi megállapodással összhangban harmadik országgal közösen hoztak létre.**

- (9aa) **A tagállamoknak lehetőséget kell biztosítani arra, hogy megállapítsák, hogy az ezen irányelv hatálybalépése előtt az (EU) 2016/1148 irányelvvel összhangban alapvető szolgáltatásokat nyújtó szereplőként azonosított szervezetek alapvető szervezetnek minősülnek.**
- (9aaa) **Ez az irányelv nem alkalmazandó a tagállamok külföldi diplomáciai és konzuli képviseleteire és az ilyen képviseletek által használt IKT-infrastruktúrákra, amennyiben az ilyen infrastruktúra külföldön található és azt külföldi felhasználók részére működtetik.**
- (10) A Bizottság az együttműködési csoporttal együttműködve iránymutatásokat adhat ki a mikro- és kisvállalkozásokra alkalmazandó kritériumok végrehajtásáról.
- (11) [...] **Az ezen irányelv hatálya alá tartozó szervezetek két kategóriába sorolandók, mégpedig az alapvető és a fontos szervezetek kategóriájába, a besoroláshoz pedig figyelembe kell venni azt, hogy az ágazat vagy a szervezet által nyújtott szolgáltatások mennyire kritikus fontosságúak, valamint a szervezet méretét. E tekintetben kellően figyelembe kell venni a vonatkozó ágazati kockázatértékeléseket vagy adott esetben az illetékes hatóságok által adott iránymutatást is.** Mind az alapvető, mind a fontos szervezetekre alkalmazni kell [...] a kockázatkezelési követelményeket és a bejelentési kötelezettségeket. A szervezetek e két kategóriája között a felügyeleti és szankciórendszer tekintetében különbséget kell tenni, hogy biztosítani lehessen a méltányos egyensúlyt a **kockázatalapú** követelmények és kötelezettségek, valamint a megfelelés felügyeletéből adódó adminisztratív terhek között.

- (12) **Ez az irányelv a kiberbiztonsági kockázatkezelési intézkedések és bejelentési kötelezettségek alapjául szolgál a hatálya alá tartozó valamennyi ágazatban. Annak érdekében, hogy elkerülhető legyen az uniós jogi aktusokban foglalt kiberbiztonsági rendelkezések felaprózódása, azokban az esetekben, amikor a kiberbiztonság magas szintjének biztosítása érdekében a kiberbiztonsági kockázatkezelési intézkedésekre és bejelentési kötelezettségekre vonatkozó kiegészítő ágazatspecifikus rendelkezésekre van szükség, a Bizottságnak értékelnie kell, hogy az ilyen rendelkezéseket meg lehet-e állapítani az ezen irányelvben foglalt felhatalmazás alapján elfogadott végrehajtási jogi aktus keretében. Amennyiben az ilyen jogi aktusok nem alkalmasak erre a célra, az ágazatspecifikus jogszabályok hozzájárulhatnak a kiberbiztonság [...] magas szintjének biztosításához, teljeskörűen figyelembe véve az [...] érintett ágazatok sajátosságait és összetettségét. Az ágazatspecifikus jogszabályban meg kell indokolni, hogy az ezen irányelvben foglalt felhatalmazás alapján elfogadott végrehajtási jogi aktus miért nem alkalmas. Ugyanakkor az uniós jogi aktusokban foglalt ilyen ágazatspecifikus rendelkezéseknek kellően figyelembe kell venniük azt, hogy átfogó és harmonizált kiberbiztonsági keretre van szükség. [...] Ez [...] nem érinti a [...] Bizottságra számos ágazatban – ideértve a közlekedést és az energiaágazatot is – ruházott, meglévő végrehajtási hatásköröket.**

(12a) Amennyiben egy ágazatspecifikus uniós jogi aktus olyan **rendelkezéseket tartalmaz** [...], amelyek **értelmében** az alapvető vagy a fontos szervezeteknek **az ebben az irányelvben** [...] a kiberbiztonsági kockázatkezelés tekintetében **meghatározott kötelezettségekkel**, valamint a **jelentős** biztonsági események vagy jelentős kiberfenyegetések [...] bejelentésére vonatkozó **kötelezettségekkel legalább egyenértékű hatású intézkedéseket** kell elfogadniuk, ezen ágazatspecifikus rendelkezések – **beleértve a felügyeletre és a végrehajtásra vonatkozókat is** – alkalmazandók. Az uniós jogi aktusokban foglalt ágazatspecifikus intézkedésekben megállapított kötelezettségek egyenértékű hatásának a meghatározásakor a következő tényezőket kell figyelembe venni: i. a kiberbiztonsági kockázatkezelési intézkedéseknek megfelelő és arányos technikai és szervezési intézkedéseket kell magukban foglalniuk annak a hálózati és információs rendszernek a biztonságát veszélyeztető kockázatok kezelésére, amelyet az érintett szervezetek a szolgáltatásaik nyújtása során használnak, továbbá tartalmazniuk kell legalább az ezen irányelvben meghatározott valamennyi elemet; ii. a jelentős biztonsági események vagy jelentős kiberfenyegetések bejelentésére vonatkozó kötelezettségnek a tartalmát, formát és a bejelentésre vonatkozó határidőket tekintve legalább egyenértékűnek kell lennie az ezen irányelvben meghatározott kötelezettségekkel; iii. a szervezetek és az ágazatspecifikus uniós jogi aktusok szerinti illetékes hatóságok általi bejelentésre vonatkozó szabályoknak a tartalmát, a formát és a határidőket tekintve legalább egyenértékűnek kell lenniük az ezen irányelvben meghatározott követelményekkel, és figyelembe kell venniük a CSIRT-ek szerepét; iv. az érintett hatóságokra vonatkozó, a határokon átnyúló együttműködéssel kapcsolatos követelményeknek legalább egyenértékűnek kell lenniük az ezen irányelvben foglaltakkal. Amennyiben az ágazatspecifikus uniós jogi aktus rendelkezései nem terjednek ki az ezen irányelv hatálya alá tartozó adott ágazatban működő valamennyi szervezetre, ezen irányelv vonatkozó rendelkezéseit továbbra is alkalmazni kell azokra a szervezetekre, amelyek nem tartoznak az említett ágazatspecifikus rendelkezések hatálya alá.

- (12aa)** A Bizottságnak rendszeresen felül kell vizsgálnia az uniós jogi aktusok ágazatspecifikus rendelkezéseinek egyenértékű hatására vonatkozó követelmények alkalmazását [...]. Az említett időszakos felülvizsgálatok előkészítése során a Bizottságnak konzultálnia kell az együttműködési csoporttal.
- (12aaa)** A jövőbeli ágazatspecifikus uniós jogi aktusokban megfelelően figyelembe kell venni az ezen irányelv 4. cikkében foglalt fogalommeghatározásokat, valamint az ezen irányelv VI. fejezetében foglalt felügyeleti és végrehajtási keretet.
- (12ab)** Amennyiben egy uniós jogi aktus ágazatspecifikus rendelkezései értelmében az alapvető vagy a fontos szervezeteknek az ebben az irányelvben meghatározott bejelentési kötelezettségekkel legalább egyenértékű hatású intézkedéseket kell elfogadniuk, kerülni kell a bejelentési kötelezettségek közötti átfedéseket, valamint a kiberfenyegetésekre vagy a biztonsági eseményekre vonatkozó bejelentések kezelése során biztosítani kell a koherenciát és a hatékonyságot. Ebből a célból az említett ágazatspecifikus rendelkezések lehetővé tehetik a tagállamok számára, hogy közös, automatikus és közvetlen bejelentési mechanizmust hozzanak létre a jelentős biztonsági eseményeknek és kiberfenyegetéseknek mind azon hatóságok részére történő bejelentésére, akiknek feladatait a vonatkozó ágazatspecifikus rendelkezések határozzák meg, mind az ezen irányelv szerinti kiberbiztonsági feladatok ellátásában illetékes hatóságok részére, beleértve adott esetben az egyedüli kapcsolattartó pontot és a CSIRT-et, vagy egy olyan mechanizmus részére, amely az ilyen bejelentések kezelése tekintetében biztosítja az információk szisztematikus és haladéktalan megosztását, valamint az együttműködést az illetékes hatóságok és a CSIRT között. A bejelentések egyszerűsítése és a közös, automatikus és közvetlen bejelentési mechanizmus létrehozása érdekében a tagállamok az ágazatspecifikus jogszabályokkal összhangban igénybe vehetik az ezen irányelv 11. cikkének (5a) bekezdése szerint létrehozott egyedüli kapcsolattartó pontot. A harmonizáció biztosítása érdekében az ágazatspecifikus uniós jogszabályokban foglalt bejelentési kötelezettségeknek összhangban kell lenniük az ebben az irányelvben meghatározottakkal. A tagállamok kiköthetik, hogy az ágazatspecifikus jogszabályokkal összhangban az ezen irányelv szerinti illetékes hatóságok vagy a nemzeti CSIRT-ek a bejelentések címzettjei.

- (13) Az XXXX/XXXX európai parlamenti és tanácsi rendeletet ezen irányelv vonatkozásában ágazatspecifikus uniós jogi aktusnak kell tekinteni a pénzügyi ágazatbeli szervezetek tekintetében. Az ezen irányelvben [...] **meghatározott** rendelkezések helyett az XXXX/XXXX rendeletnek az információs és kommunikációs technológiai (IKT) kockázatkezelési intézkedésekre, az IKT-vel kapcsolatos biztonsági események kezelésére és különösen a biztonsági események bejelentésére, valamint a digitális működési rezilienciára vonatkozó tesztekre, az információmegosztási megállapodásokra és a harmadik féllel kapcsolatos IKT-kockázatokra vonatkozó rendelkezéseit kell alkalmazni. A tagállamok ezért nem alkalmazhatják az ezen irányelvben a kiberbiztonsági kockázatkezelésre és [...] bejelentési kötelezettségekre, valamint a felügyeletre és végrehajtásra vonatkozóan meghatározott rendelkezéseket [...] az 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 az XXXX/XXXX rendelet értelmében [...] a pénzügyi ágazat európai felügyeleti hatóságai és az XXXX/XXXX rendelet szerinti illetékes nemzeti hatóságok [...] részt vehetnek [...] **az együttműködési csoport [...] munkájában**, valamint információt cserélhetnek és együttműködhetnek az ezen irányelv alapján kijelölt egyedüli kapcsolattartó ponttal [...] és a nemzeti CSIRT-ekkel. Az XXXX/XXXX rendelet szerint illetékes hatóságoknak továbbítaniuk kell az IKT-vel kapcsolatos jelentős biztonsági események és **jelentős kiberfenyegetések** részleteit az ezen irányelv alapján kijelölt egyedüli kapcsolattartó pontoknak, **illetékes hatóságoknak vagy nemzeti CSIRT-eknek. Ez megtehető a biztonsági eseményekre vonatkozó bejelentések automatikus és közvetlen továbbítása révén vagy közös bejelentési platformon keresztül.** Ezenkívül a tagállamoknak továbbra is be kell vonniuk a pénzügyi ágazatot kiberbiztonsági stratégiájukba, és a nemzeti CSIRT-ek tevékenységei [...] kiterjedhetnek a pénzügyi ágazatra.

(13a) Az I. melléklet 2. pontjának a) alpontjában említett légiközlekedési ágazatban működő szervezetekre vonatkozó kiberbiztonsági kötelezettségek közötti hiányosságok és átfedések elkerülése érdekében a 300/2008/EK¹⁶, valamint az (EU) 2018/1139¹⁷ európai parlamenti és tanácsi rendelet alapján kijelölt nemzeti hatóságoknak és az ezen irányelv szerinti illetékes hatóságoknak együtt kell működniük egymással a kiberbiztonsági kockázatkezelési intézkedések végrehajtása és az ilyen intézkedések nemzeti szinten történő felügyelete terén. Amennyiben valamely szervezet betartja az ebben az irányelvben foglalt kiberbiztonsági kockázatkezelési intézkedéseket, [...] a 300/2008/EK, valamint az (EU) 2018/1139 rendelet alapján kijelölt nemzeti hatóságok tekinthetik úgy, hogy a szervezet betartja az említett rendeletekben és az azok alapján elfogadott vonatkozó, felhatalmazáson alapuló, illetve végrehajtási jogi aktusokban foglalt követelményeket.

¹⁶ Az Európai Parlament és a Tanács 300/2008/EK rendelete (2008. március 11.) a polgári légi közlekedés védelmének közös szabályairól és a 2320/2002/EK rendelet hatályon kívül helyezéséről (HL L 97., 2008.4.9., 72. o.).

¹⁷ Az Európai Parlament és a Tanács (EU) 2018/1139 rendelete (2018. július 4.) a polgári légi közlekedés területén alkalmazandó közös szabályokról és az Európai Unió Repülésbiztonsági Ügynökségének létrehozásáról és a 2111/2005/EK, az 1008/2008/EK, a 996/2010/EU, a 376/2014/EU európai parlamenti és tanácsi rendelet és a 2014/30/EU és a 2014/53/EU európai parlamenti és tanácsi irányelv módosításáról, valamint az 552/2004/EK és a 216/2008/EK európai parlamenti és tanácsi rendelet és a 3922/91/EGK tanácsi rendelet hatályon kívül helyezéséről (HL L 212., 2018.8.22., 1. o.).

- (14) A kiberbiztonság és a szervezetek fizikai biztonsága közötti összefüggésekre tekintettel koherens megközelítést kell biztosítani az (EU) XXX/XXX európai parlamenti és tanácsi irányelv és ezen irányelv között. Ennek elérése érdekében a tagállamoknak biztosítaniuk kell, hogy az (EU) XXX/XXX irányelv szerinti, kritikus fontosságú szervezeteket [és az azokkal egyenértékű szervezeteket] ezen irányelv keretében alapvető szervezeteknek [...] tekintsék. A tagállamoknak arról is gondoskodniuk kell, hogy kiberbiztonsági stratégiáik rendelkezzenek az ezen irányelv és az (EU) XXX/XXX irányelv szerinti illetékes hatóság közötti fokozott koordinációra vonatkozó politikai keretről a biztonsági eseményekkel és a kiberfenyegetésekkel kapcsolatos információk megosztása és a felügyeleti feladatok összefüggésében. A két irányelv szerinti **illetékes** [...] hatóságoknak együtt kell működniük és információt kell cserélniük egymással, különösen a következőkkel kapcsolatban: a kritikus fontosságú szervezetek azonosítása, a kritikus fontosságú szervezeteket **[vagy a kritikus fontosságú szervezetekkel egyenértékű szervezeteket]** érintő kiberfenyegetések, kiberbiztonsági kockázatok és biztonsági események, **valamint nem kiberjellegű kockázatok, fenyegetések és biztonsági események**, [...] **beleértve** a kritikus fontosságú szervezetek által végrehajtott kiberbiztonsági és **fizikai** intézkedéseket, **valamint az ilyen szervezetek tekintetében végzett felügyeleti tevékenységek eredményeit. Ezenkívül a két irányelv alapján kijelölt illetékes hatóságokat érintő felügyeleti feladatok észszerűsítése, valamint az érintett hatóságok adminisztratív terheinek minimálisra csökkentése érdekében az illetékes hatóságoknak törekedniük kell a biztonsági események bejelentésére szolgáló sablonok és a felügyeleti eljárások összehangolására.** [...] Az (EU) XXX/XXX irányelv szerinti illetékes hatóságok **adott esetben** [...] **felkérhetik** az ezen irányelv szerinti illetékes hatóságokat arra, hogy [...] gyakorolják felügyeleti és végrehajtási jogkörüket [...] egy kritikus fontosságúként azonosított szervezet tekintetében. [...]

- (14a) A digitálisinfrastruktúra-ágazathoz tartozó szervezetek lényegében a hálózati és információs rendszereken alapulnak, ezért az ezen irányelvben az ilyen szervezetekre vonatkozóan meghatározott kötelezettségeknek átfogó módon ki kell terjedniük az ilyen rendszerek fizikai biztonságára a kiberbiztonsági kockázatkezelési és bejelentési kötelezettségek keretében. Mivel az említett területek ezen irányelv hatálya alá tartoznak, az (EU) XXX/XXX irányelv [CER-irányelv] III–VI. fejezetében meghatározott kötelezettségek nem vonatkoznak ezekre a szervezetekre.
- (15) A megbízható, reziliens 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 alkalmazni kell a DNS-ellátási és -feloldási lánc mentén **a belső piac szempontjából fontos** DNS-szolgáltatókra, ideértve [...] a legfelső szintű doménnév-nyilvántartókat [...], **a doménnév-regisztrációs szolgáltatásokat nyújtó szervezeteket**, a doménnevek autoritatív névszervereinek **működtetőit**, valamint a rekurzív feloldás **működtetőit**. A „DNS-szolgáltató” fogalma nem alkalmazandó az érintett szervezet és kapcsolódó szervezetei saját céljára működtetett DNS-szolgáltatásokra. A szolgáltatók ezen kategóriájára vonatkozó, az ezen irányelvből eredő kiberbiztonsági kötelezettségek szigorúan a kiberbiztonsági kockázatkezelési intézkedésekre és bejelentésre korlátozódnak, ezért nem érintik a globális DNS-nek a több érdekelt felet tömörítő közösség általi irányítását.

- (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 pooljához. 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 szolgáltatási modelljei magukban foglalják többek között az infrastruktúra-szolgáltatást (IaaS), a platformszolgáltatást (PaaS), a szoftverszolgáltatást (SaaS), valamint a hálózatszolgáltatást (NaaS).** A felhőalapú számítástechnika telepítési modelljeinek ki kell terjedniük a magán-, a közösségi, a nyilvános és a hibrid felhőre. A 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 módon számítástechnikai kapacitásokat, például kiszolgálói időt vagy hálózati tárhelyet vegyen igénybe, a felhőszolgáltató emberi beavatkozása nélkül, igény szerinti adminisztrációként jellemezhető. A „kiterjedt távoli hozzáférés” kifejezést annak leírására használják, hogy a felhőképességeket a hálózaton keresztül biztosítják, a hozzáférés pedig heterogén vékony- vagy vastagkliensek (beleértve a mobiltelefonokat, táblagépeket, laptopokat, munkaaállomásokat) használatát elősegítő mechanizmusok révén történik.

A „méretezhető” kifejezés olyan számítástechnikai erőforrásokra utal, amelyeket a felhőszolgáltató rugalmasan allokal, függetlenül az erőforrások földrajzi elhelyezkedésétől, a kereslet ingadozásainak kezelése érdekében. A „rugalmas pool” kifejezés azokat a számítástechnikai erőforrásokat foglalja magában, amelyeket az igényeknek megfelelően hoznak létre és bocsátanak ki a rendelkezésre álló erőforrások gyors növelése és csökkentése érdekében, a munkaterheléstől függően. A „megosztható” kifejezés alatt azok a számítástechnikai erőforrások értendők, 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 alatt azok a számítástechnikai erőforrások értendők, 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, a felhőalapú számítástechnikában várhatóan új 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, -kezelési és -továbbítási szolgáltatásokat nyújtó információs technológiai 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 irányelv¹⁸ értelmében vett postai szolgáltatóknak, [...] **köztük** a [...] futárszolgálatot nyújtó [...] 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.

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.).

- (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 zavarnak – akkor is, ha eredetileg csak egy szervezetre vagy egy ágazatra korlátozódik – szélesebb körben lépcsőzetes hatásai lehetnek, ami messzemenő és hosszú távú negatív hatásokat eredményezhet a szolgáltatások belső piacon történő nyújtásában. A Covid19-járvány megmutatta az egyre inkább egymásra utalt társadalmaink sérülékenységet az alacsony valószínűségű kockázatokkal szemben.
- (20a) **A magas szintű kiberbiztonság megteremtése és fenntartása érdekében az ezen irányelv által előírt nemzeti kiberbiztonsági stratégiáknak olyan koherens kereteknek kell lenniük, amelyek meghatározzák a kiberbiztonság területének irányítását. Ezek a stratégiák állhatnak egy vagy több, jogalkotási vagy nem jogalkotási jellegű dokumentumból.**
- (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 az ezen irányelv szerinti alapvető és fontos szervezetek hálózati és információs rendszerei biztonságával kapcsolatos feladatok ellátásáért felelnek. A tagállamok számára lehetővé kell tenni, hogy ezt a szerepkört egy meglévő hatóságra bízzák.

- (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 a biztonsági eseményekre vonatkozó bejelentéseket, **adott esetben többek között annak elősegítése érdekében is, hogy a biztonsági eseményekre időben lehessen reagálni és választ lehessen adni a bejelentő szervezetnek.** Az egyedüli kapcsolattartó pontokat azzal kell megbízni, hogy továbbítsák a biztonsági eseményekre vonatkozó bejelentéseket a többi érintett tagállam egyedüli kapcsolattartó pontjának. [...]

- (23a) Az olyan ágazatspecifikus uniós jogi aktusokban, amelyek az ebben az irányelvben meghatározottakkal legalább egyenértékű kiberbiztonsági kockázatkezelési intézkedéseket vagy bejelentési kötelezettségeket írnak elő, lehet rendelkezni arról, hogy a szóban forgó jogi aktus alapján kijelölt illetékes hatóságok az ezen irányelvvel összhangban kijelölt illetékes hatóságok segítségével gyakorolják felügyeleti és végrehajtási jogkörüket az ilyen intézkedések vagy kötelezettségek tekintetében. Az érintett illetékes hatóságok e célból együttműködési megállapodásokat hozhatnak létre. Az ilyen együttműködési megállapodásokban meg lehet határozni többek között a felügyeleti tevékenységek koordinálásával kapcsolatos eljárásokat, beleértve a nemzeti joggal összhangban végzett vizsgálatokra és helyszíni ellenőrzésekre vonatkozó eljárásokat, valamint a felügyelettel és a végrehajtással kapcsolatos releváns információk illetékes hatóságok közötti cseréjét, beleértve az ezen irányelvvel összhangban kijelölt illetékes hatóságok által a kiberjellegű információkhoz való hozzáférés iránti kérelmeket.
- (24) A tagállamoknak mind technikai, mind szervezeti képességek tekintetében megfelelő felszereléssel kell rendelkezniük a hálózati és információs rendszerekkel kapcsolatos biztonsági 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 a biztonsági események és kockázatok kezelésének hatékony és kompatibilis képességeit, valamint hogy uniós szinten biztosítsák a hatékony együttműködést. A szervezetek és a CSIRT-ek közötti bizalmi kapcsolat fokozása céljából azokban az esetekben, amikor a CSIRT az illetékes hatóság része, a tagállamok [...] fontolóra vehetik a CSIRT-ek által biztosított operatív feladatok funkcionális elkülönítését, különösen az információmegosztással, valamint a szervezetek és az illetékes hatóságok felügyeleti tevékenységei támogatásával kapcsolatban.

- (25) A személyes adatok tekintetében a CSIRT-eknek képeseknek kell lenniük arra, hogy az (EU) 2016/679 európai parlamenti és tanácsi rendeletnek¹⁹ megfelelően a személyes adatok tekintetében ezen irányelv alapján – valamely szervezet nevében és kérésére – proaktívan átvizsgálják a szolgáltatásaik nyújtásához használt hálózati és információs rendszereket. A tagállamoknak **adott esetben** 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.
- (26) Tekintettel a kiberbiztonság terén folytatott nemzetközi együttműködés fontosságára, a CSIRT-ek részt vehetnek a CSIRT-eknek az ezen irányelv által létrehozott hálózata mellett nemzetközi együttműködési hálózatokban is. **Ezért a CSIRT-ek és az illetékes hatóságok a feladataiknak az (EU) 2016/679 rendelettel összhangban történő végrehajtása céljából információkat – többek között személyes adatokat – cserélhetnek harmadik országbeli CSIRT-ekkel vagy harmadik országbeli hatóságokkal. Az (EU) 2016/679 rendelet 45. cikkének megfelelően elfogadott megfelelőségi határozat vagy az említett rendelet 46. cikke szerinti megfelelő garanciák hiányában a személyes adatoknak a jelentős kiberfenyegetések mérséklése és a folyamatban lévő jelentős biztonsági eseményekre való reagálás céljából szükségesnek ítélt cseréje az (EU) 2016/679 rendelet 49. cikke (1) bekezdésének d) pontja értelmében vett fontos közérdeknek tekinthető.**

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 ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

- (27) A nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló (EU) 2017/1548 bizottsági ajánlás („Tervezet”)²⁰ mellékletével összhangban, nagyszabású biztonsági eseménynek azt a biztonsági 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 biztonsági események eszkalálódhatnak, és olyan teljes körű válsággá válhatnak, amely nem teszi lehetővé a belső piac megfelelő működését. Tekintettel az említett biztonsági 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 sebezhetőségeinek kihasználása jelentős zavarokat és kárt okozhat, a sebezhetőségek gyors azonosítása és elhárítása fontos tényező a kiberbiztonsági kockázat csökkentésében. Az említett rendszereket fejlesztő **vagy kezelő** szervezeteknek ezért megfelelő eljárásokat kell kidolgozniuk a sebezhetőségek felfedezéskor történő kezelésére. Mivel a sebezhetőségeket gyakran harmadik felek (adatszolgáltatásra kötelezett szervezetek) fedezik fel és jelentik be (tárják fel), az IKT-termékek vagy -szolgáltatások gyártójának vagy szolgáltatójának szintén be kell vezetnie a sebezhetőségre vonatkozó információk harmadik felektől történő fogadásához szükséges eljárásokat. Ebben a tekintetben az ISO/IEC 30111 és az ISO/IEC [...] **29147** nemzetközi szabvány útmutatást nyújt a sebezhetőségek kezelése, illetve a sebezhetőségek feltárása tekintetében. A sebezhetőségek feltárását illetően különösen fontos az adatszolgáltatásra kötelezett szervezetek és az IKT-termékek vagy -szolgáltatások gyártói vagy szolgáltatói közötti koordináció. Az összehangolt sebezhetőség-feltárás strukturált folyamatot határoz meg, amelyen keresztül a szervezetek a sebezhetőségeket oly módon jelentik be, hogy az lehetővé tegye a szervezet számára a sebezhetőség azt megelőzően történő diagnosztizálását és orvosolását, hogy a sebezhetőségre vonatkozó részletes információkat harmadik felek vagy a nyilvánosság előtt feltárná. Az összehangolt sebezhetőség-feltárásnak magában kell foglalnia az adatszolgáltatásra kötelezett szervezet és a szervezet közötti koordinációt is a sebezhetőségek orvosolásának és közzétételének időzítése tekintetében.

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.).

- (29) A tagállamoknak ezért intézkedéseket kell hozniuk az összehangolt sebezhetőség-feltárásnak egy megfelelő nemzeti politika kialakításával történő megkönnyítésére. **A tagállamoknak nemzeti politikájuk részeként törekedniük kell arra, hogy – a nemzeti jogrendjükkel összhangban – a lehető legnagyobb mértékben kezeljék a sebezhetőségeket kutatókkal szembeni kihívásokat, beleértve az esetleges büntetőjogi felelősségre vonásnak való kitettségüket is.** [...] 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 sebezhetőségek kezelése (több felet érintő **összehangolt** sebezhetőség-feltárás). Ha **a bejelentett** sebezhetőség [...] több tagállamban [...] **is jelentős hatást gyakorolhat szervezetekre,** [...] a kijelölt CSIRT-eknek **adott esetben** együtt kell működniük a CSIRT-ek hálózatán belül.
- (30) Az IKT-termékeket és -szolgáltatásokat érintő sebezhetőségekkel kapcsolatos helyes és időszerű információkhoz való hozzáférés hozzájárul a jobb kiberbiztonsági kockázatkezeléshez. E tekintetben a sebezhetőségekről 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 sebezhetőség-nyilvántartást kell létrehoznia, amelyben az alapvető és a fontos szervezetek és beszállítók, valamint az ezen irányelv alkalmazásának hatálya alá nem tartozó szervezetek **vagy a kijelölt CSIRT-ek** önkéntes alapon feltárhatják a sebezhetőségeket és megadhatják a sebezhetőségre vonatkozó azon információkat, amelyek lehetővé teszi a felhasználók számára a megfelelő mérséklési intézkedések megtételét.

- (31) Noha léteznek hasonló sebezhetőség-nyilvántartások vagy adatbázisok, ezeket nem az Unióban letelepedett szervezetek üzemeltetik és tartják fenn. Az ENISA által fenntartott európai sebezhetőség-nyilvántartás javulást hoz a sebezhetőségek hivatalos feltárása 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. **Az ENISA-nak különösen meg kell vizsgálnia a közös sebezhetőségi és kitettségi nyilvántartás üzemeltetőivel való szoros együttműködés lehetőségét, beleértve annak lehetőségét is, hogy a közös sebezhetőségi és kitettségi nyilvántartás gyökérszintű számozási hatóságává váljon.**
- (32) **Az együttműködési csoportnak továbbra is támogatnia kell és elő kell segítenie a stratégiai együttműködést és az információcserét, valamint erősítenie kell a tagállamok közötti bizalmat.** Az együttműködési csoportnak kétévente munkaprogramot kell kidolgoznia, 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 szakpolitikai 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 politikában részt vevő uniós szervek és ügynökségek – például a Kiberbűnözés Elleni Európai Központ (EC3), az Európai Unió Repülésbiztonsági Ügynöksége (EASA) és az Európai Unió Űrprogramügynöksége (EUSPA) meghívását a munkájában történő részvételre.
- (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.
- (35a) A CSIRT-ek hálózatának továbbra is hozzá kell járulnia a bizalom erősítéséhez és továbbra is elő kell mozdítania a tagállamok közötti gyors és hatékony operatív együttműködést. Az uniós szintű operatív együttműködés intenzívebbé tétele érdekében a CSIRT-ek hálózatának fontolóra kell vennie, hogy felkérje a kiberbiztonsági politikában részt vevő uniós szerveket és ügynökségeket – például az Europol – arra, hogy vegyenek részt a hálózat munkájában.**
- (36) [...]

- (36a) Ezen irányelv rendelkezései – például a sebezhetőségek kezelése, a kiberbiztonsági kockázatkezelés, a jelentéstételi intézkedések és az információmegosztási megállapodások – hatékony végrehajtásának elősegítése érdekében a tagállamok együttműködhetnek harmadik országokkal, és folytathatnak e célból megfelelőnek ítélt tevékenységeket, ideértve a fenyegetésekre, biztonsági eseményekre, sebezhetőségekre, eszközökre és módszerekre, taktikákra, technikákra és eljárásokra, a kiberválságok kezelésére való felkészültségre és az erre irányuló gyakorlatokra, képzésre, bizalomépítésre és strukturált információmegosztási rendszerekre vonatkozó információcserét. Az ilyen együttműködési megállapodásoknak összhangban kell lenniük az adatvédelemre vonatkozó uniós jogszabályokkal.
- (37) A tagállamoknak hozzá kell járulniuk az (EU) 2017/1584 ajánlásban meghatározott uniós kiberbiztonsági válságreakálási keret létrehozásához a meglévő együttműködési hálózatokon, nevezetesen az **Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatán (EU-CyCLONe)**, a CSIRT-ek hálózatán és az együttműködési csoporton keresztül. Az EU-CyCLONe-nak és a CSIRT-ek hálózatának az említett együttműködés módozatait meghatározó eljárási megállapodások alapján kell együttműködniük **és el kell kerülniük a párhuzamos munkavégzést**. 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 **politikai** szintű válságkezelés során az érintett feleknek a politikai szintű integrált válságelhárítási (IPCR) mechanizmusokra kell támaszkodniuk. A Bizottságnak erre a célra az ARGUS magas szintű, ágazatok közötti válságkoordinációs folyamatát kell alkalmaznia. Ha a válságnak fontos külső vagy közös biztonság- és védelempolitikai (KBVP) dimenziója van, aktiválni kell az Európai Külügyi Szolgálat (EKSZ) válságelhárítási mechanizmusát (VEM).

- (37a) Az EU-CyCLONe-nak a nagyszabású kiberbiztonsági események és válságok idején közvetítő hálózatként kell működnie a technikai és a politikai szint között. Intenzívebbé kell tennie az operatív szintű együttműködést, ennek során pedig építenie kell a CSIRT-ek hálózatának megállapításaira, alkalmaznia kell a saját képességeit a nagyszabású biztonsági események és válságok hatásvizsgálatának kidolgozása érdekében, és támogatnia kell a politikai szintű döntéshozatalt. Az uniós intézményeknek, szervezeteknek és ügynökségeknek ki kell jelölniük egy, a nagyszabású biztonsági események és válságok kezeléséért felelős illetékes hatóságot, hogy az az EU-CyCLONe tagjává váljon.
- (38) [...]
- (39) [...]
- (39a) A hálózati és információs rendszer biztonságának biztosítása nagymértékben az alapvető és a fontos szervezetek felelőssége. Ösztönözni és fejleszteni kell a – kockázatértékelésre és a felmerülő kockázatok súlyosságának megfelelő biztonsági intézkedések végrehajtására egyaránt kiterjedő – kockázatkezelési kultúrát.
- (40) A kockázatkezelési intézkedéseknek **figyelembe kell venniük, hogy a szervezet milyen mértékben függ a hálózati és információs rendszerektől**, és intézkedéseket kell tartalmazniuk a biztonsági események kockázatainak azonosítására, továbbá a biztonsági események megelőzésére, felderítésére és kezelésére, valamint azok hatásainak mérséklésére. A hálózati és információs rendszerek biztonságának magában kell foglalnia a tárolt, továbbított és kezelt adatok biztonságát.

- (40a) Mivel a hálózati és információs rendszerek biztonságát fenyegető veszélyek különböző eredetűek lehetnek, ez az irányelv egy „minden veszélyre kiterjedő” megközelítést alkalmaz, amely magában foglalja a hálózati és információs rendszereknek és azok fizikai környezetének a védelmét minden olyan eseménytől, mint például a lopás, a tűz, az árvíz, a távközlési és áramellátási zavarok, vagy a szervezet információs és információfeldolgozó létesítményeihez való jogosulatlan fizikai hozzáférés, az azokban keletkezett kár és az azokon végrehajtott beavatkozás, amely veszélyeztetheti a tárolt, továbbított vagy kezelt adatok vagy a hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, integritását vagy bizalmas jellegét. A kockázatkezelési intézkedéseknek ezért a fizikai és a környezetbiztonsággal is foglalkozniuk kell azáltal, hogy magukban foglalnak olyan intézkedéseket, amelyek – az európai vagy nemzetközileg elismert szabványokkal, például az ISO 27000 szabványsorozatban foglalt szabványokkal összhangban – védik a szervezet hálózati és információs rendszereit a rendszerhibákkal, az emberi hibával, a rosszindulatú tevékenységekkel vagy a természeti jelenségekkel szemben. E tekintetben a szervezeteknek kockázatkezelési intézkedéseik részeként foglalkozniuk kell az emberi erőforrások biztonságával is, és megfelelő hozzáférés-ellenőrzési politikákkal kell rendelkezniük. Az említett intézkedéseknek összhangban kell lenniük a(z) XXXX irányelvvel [CER-irányelv].**
- (40b) Az (EU) 2019/881 rendelettel összhangban elfogadott megfelelő európai kiberbiztonsági tanúsítási rendszerek hiányában a tagállamok megkövetelhetik a szervezetektől, hogy tanúsított IKT-termékeket, -szolgáltatásokat és -folyamatokat használjanak, vagy a rendelkezésre álló nemzeti kiberbiztonsági rendszerek keretében tanúsítványt szerezzenek be az ezen irányelvben foglalt kiberbiztonsági kockázatkezelési követelményeknek való megfelelés céljából.**

- (41) Az alapvető és a fontos szervezetekre aránytalan pénzügyi és adminisztratív terhek előírásának elkerülése érdekében a kiberbiztonsági kockázatkezelési követelményeknek arányosaknak kell lenniük az érintett hálózati és információs rendszerre [...] jelentett kockázattal, figyelembe véve az említett intézkedések korszerűségét és **a végrehajtásuk költségeit. Kellően figyelembe kell venni továbbá a szervezet méretét, valamint a biztonsági események előfordulásának valószínűségét és a súlyosságukat.**
- (41a) **A szabályozásból eredő terhek enyhítése érdekében a közepes, a kis és a mikro méretű szervezetekre vonatkozó kiberbiztonsági kockázatkezelési intézkedések végrehajtására vonatkozó követelményeknek elvben enyhébbeknek kell lenniük, kivéve abban az esetben, ha a kritikussági kritériumok vagy a nemzeti kockázatértékelések szigorúbb követelményeket tennének indokolttá, különösen azon szervezetek tekintetében, amelyek teljesítik az ezen irányelvben meghatározott, a kritikus szintre vonatkozó kritériumokat.**
- (42) Az alapvető és a fontos szervezeteknek biztosítaniuk kell a tevékenységük során használt hálózati és információs rendszerek biztonságát. Ezek elsősorban magánkézben lévő hálózatok és információs rendszerek, amelyeket belső informatikai személyzetük kezel, vagy amelyek biztonságát kiszervezték. Az ezen irányelv szerinti kiberbiztonsági kockázatkezelési és bejelentési követelményeket alkalmazni kell az érintett alapvető és fontos szervezetekre, függetlenül attól, hogy hálózati és információs rendszereik karbantartását házon belül végzik-e vagy kiszervezik.
- (42aa) **A határokon átnyúló jellegükre tekintettel uniós szinten magasabb fokú harmonizációt kell alkalmazni a következőkre: DNS-szolgáltatók, legfelső szintű doménnév-nyilvántartók és a TLD-hez kapcsolódó doménnév-regisztrációs szolgáltatásokat nyújtó szervezetek, felhőszolgáltatók, adatközpont-szolgáltatók, tartalomszolgáltató hálózati szolgáltatók, felügyelt szolgáltatók és felügyelt biztonsági szolgáltatók. A kiberbiztonsági intézkedések végrehajtását ezért végrehajtási jogi aktussal kell elősegíteni.**

- (43) A szervezet ellátási láncából és a beszállítóival való kapcsolatából eredő kiberbiztonsági kockázatok kezelése különösen fontos, tekintettel arra a számos biztonsági eseményre, amikor szervezetek kibertámadások áldozatává váltak, és amikor rosszindulatú szereplők azzal tudták veszélyeztetni valamely szervezet hálózati és információs rendszereinek biztonságát, hogy harmadik fél termékeit és szolgáltatásait érintő sebezhetőségeket használtak ki. 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 a felügyelt biztonsági szolgáltatók olyan területeken, mint a biztonsági események elhárítása, behatolási tesztek, biztonsági auditok és tanácsadás, különösen fontos szerepet töltenek be abban, hogy segítsék a szervezeteket a biztonsági események felderítésében és azok elhárításában. Azonban maguk a felügyelt biztonsági szolgáltatók is kibertámadások célpontjai, és az üzemeltetők működésébe való szoros integrációjuk révén különös kiberbiztonsági kockázatot jelentenek. A szervezeteknek ezért fokozott gondossággal kell eljárniuk a felügyelt biztonsági szolgáltató kiválasztása során.
- (44a) Az illetékes nemzeti hatóságok a felügyeleti feladataikkal összefüggésben olyan kiberbiztonsági szolgáltatásokat is igénybe vehetnek, mint például a biztonsági ellenőrzések, a behatolásvizsgálatok vagy a biztonsági eseményekre való reagálás. Annak érdekében, hogy segítse a szervezeteket és az illetékes nemzeti hatóságokat a képzett és megbízható kiberbiztonsági szolgáltatók kiválasztásában, a Bizottságnak az együttműködési csoport és az ENISA segítségével mérlegelnie kell annak lehetőségét, hogy az (EU) 2019/881 rendelet 48. cikkével összhangban európai kiberbiztonsági tanúsítási rendszereket írjon elő.**

- (45) A szervezeteknek foglalkozniuk kell azon kiberbiztonsági kockázatokkal is, amelyek egy szélesebb ökoszisztémán belüli más érdekeltekkel 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 ajánlást²¹ követően az 5G hálózatok esetében már megtettek szerint, annak meghatározása céljából, hogy melyek a kritikus IKT-szolgáltatások, -rendszerek vagy -termékek, a releváns fenyegetések és a sebezhetőségek.

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

- (47) Az ellátáslánc-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 a fontos szervezetek mennyiben használnak bizonyos kritikus IKT-szolgáltatásokat, -rendszereket vagy -termékeket, és mennyiben támaszkodnak azokra; ii. a konkrét kritikus IKT-szolgáltatások, -rendszerek vagy -termékek relevanciája a kritikus vagy érzékeny funkciók ellátása tekintetében, ideértve a személyes adatok kezelését is; iii. alternatív IKT-szolgáltatások, -rendszerek vagy -termékek elérhetősége; iv. az IKT-szolgáltatások, -rendszerek vagy -termékek teljes ellátási láncának rezilienciája 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 hálózatokat üzemeltető és a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatókra, 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 hatóságaik kiaknázhassák az ezen irányelv által létrehozott jogi keret előnyeit (ideértve a kockázatok és a biztonsági események kezeléséért felelős CSIRT kijelölését, az illetékes hatóságok és szervek részvételét az együttműködési csoportnak és a CSIRT-ek hálózatának a munkájában), ezeket be kell vonni ezen irányelv hatálya alá. A 910/2014/EU európai parlamenti és tanácsi rendelet²² és az (EU) 2018/1972 európai parlamenti és tanácsi irányelv²³ megfelelő, az említett típusú szervezetekre vonatkozó biztonsági követelmények és bejelentési kötelezettségek előírásával kapcsolatos rendelkezéseit ezért hatályon kívül kell helyezni.

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) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról (HL L 321., 2018.12.17., 36. o.).

- (48a) Az ezen irányelvben meghatározott biztonsági kötelezettségeket a 910/2014/EU rendelet (eIDAS-rendelet) értelmében a bizalmi szolgáltatók számára előírt követelményeket kiegészítő jellegűnek kell tekinteni. A bizalmi szolgáltatók számára elő kell írni, hogy tegyenek meg minden megfelelő és arányos intézkedést a szolgáltatásaikat fenyegető – többek között a fogyasztókkal és a szolgáltatást igénybe vevő harmadik felekkel kapcsolatos – kockázatok kezelésére, valamint hogy bejelentsék az ezen irányelv szerinti biztonsági eseményeket. Ezeknek a biztonsági és bejelentési kötelezettségeknek ki kell terjedniük a nyújtott szolgáltatás fizikai védelmére is. A 910/2014/EU rendelet 24. cikkét továbbra is alkalmazni kell.
- (48aa) A tagállamok a bizalmi szolgáltatásokért felelős illetékes hatóságok szerepét az eIDAS-rendelet szerinti felügyeleti szervekre bízhatják annak érdekében, hogy biztosítsák a jelenlegi gyakorlatok folytatását és biztosítsák az eIDAS-rendelet alkalmazása során szerzett ismeretek és tapasztalatok hasznosítását. Amennyiben ezt a szerepet egy másik szervre bízják, az ezen irányelv szerinti illetékes nemzeti hatóságoknak szorosan és kellő időben együtt kell működniük egymással azáltal, hogy megosztják egymással a releváns információkat annak érdekében, hogy biztosítsák a bizalmi szolgáltatók hatékony felügyeletét és az ezen irányelvben, valamint a(z) [XXXX/XXXX] rendeletben meghatározott követelményeknek való megfelelésüket.

Adott esetben az ezen irányelv szerinti illetékes nemzeti hatóságnak haladéktalanul tájékoztatnia kell az eIDAS-rendelet szerinti felügyeleti szervet minden olyan bejelentett jelentős kiberfenyegetésről vagy kiberbiztonsági eseményről, amely hatással van a bizalmi szolgáltatásokra, valamint minden olyan esetről, amikor valamely bizalmi szolgáltató nem felel meg az ezen irányelv szerinti követelményeknek. A bejelentés céljára a tagállamok adott esetben alkalmazhatják az annak céljából létrehozott egyedüli kapcsolattartó pontot, hogy a biztonsági eseményekről közös és automatikus bejelentés történjen mind az eIDAS-rendelet szerinti felügyeleti szerv, mind pedig az ezen irányelv szerinti illetékes hatóság felé. A bejelentési kötelezettségekre vonatkozó szabályok nem érinthetik az (EU) 2016/679 rendeletet és a 2002/58/EK európai parlamenti és tanácsi irányelvet²⁴.

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.).

- (49) Adott esetben és a sürgősségi zavarok elkerülése érdekében az (EU) 2018/1725 irányelv 40. [...] és 41. cikkében meghatározott biztonsági intézkedésekre vonatkozó szabályok átültetésére elfogadott meglévő nemzeti iránymutatásokat [...] **figyelembe kell venni a tagállamok által az ezen irányelvvel kapcsolatban végrehajtott átültetési intézkedések során, építve ezáltal az (EU) 2018/1725 irányelv alkalmazása során a biztonsági kockázatkezelési intézkedésekkel és a biztonsági események bejelentésével kapcsolatban már megszerzett ismeretekre és készségekre. Az ENISA emellett a harmonizáció és az átmenet megkönnyítése, valamint a fennakadások minimálisra csökkentése érdekében iránymutatásokat dolgozhat ki a nyilvános elektronikus hírközlő hálózatokat üzemeltető és a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatókra vonatkozó biztonsági és bejelentési követelményekre vonatkozóan. A tagállamok az elektronikus hírközlésért felelős illetékes hatóságok szerepét a nemzeti szabályozó hatóságokra bízhatják annak érdekében, hogy biztosítsák a jelenlegi gyakorlatok folytatását és biztosítsák az (EU) 2018/1725 irányelv alkalmazása során szerzett ismeretek és tapasztalatok hasznosítását.**
- (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 valamennyi alapvető és fontos szervezet szolgáltatásai az interneten keresztül nyújtott szolgáltatásoktól függenek. Az alapvető és a fontos szervezetek által nyújtott szolgáltatások zavartalanságának biztosítása érdekében fontos, hogy a nyilvános elektronikus hírközlő hálózatok – például az internetes gerinchálózat vagy a tenger alatti hírközlésre szolgáló kábelek – megfelelő kiberbiztonsági intézkedéseket vezessenek be, és bejelentsék az ezekkel kapcsolatos biztonsági eseményeket.
- (52) Adott esetben a szervezeteknek tájékoztatniuk kell a szolgáltatásaikat igénybe vevőket [...] azokról a konkrét intézkedésekről, **amelyeket megtehetnek annak érdekében, hogy csökkentsék a jelentős kiberfenyegetésekből eredő, őket érintő [...] kockázatot [...]. A szervezeteknek adott esetben – és különösen azokban az esetekben, amikor a jelentős kiberfenyegetés bekövetkezhet – az illetékes hatóságokkal vagy a CSIRT-ekkel párhuzamosan a szolgáltatásaikat igénybe vevőket is értesíteniük kell a fenyegetésről.** A szolgáltatás említett igénybe vevői ilyen fenyegetésekről történő tájékoztatásának követelménye nem mentesítheti a szervezeteket azon kötelezettség alól, hogy saját költségükre megfelelő és azonnali intézkedéseket hozzanak a kiberfenyegetések megelőzésére vagy elhárítására, valamint a szolgáltatás normál biztonsági szintjének helyreállítására. A **kiberbiztonsági** fenyegetésekkel kapcsolatos említett információkat a szolgáltatást igénybe vevőknek ingyenesen kell megkapniuk.
- (53) A nyilvános elektronikus hírközlő hálózatokat üzemeltető vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatóknak 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 a biztonsági események bejelentésével kapcsolatban annak érdekében, hogy megtalálja a megfelelő egyensúlyt egyrészt a gyors bejelentések között, amelyek segítenek mérsékelni a biztonsági 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 biztonsági eseményekből, és idővel javítja az egyes vállalatok és teljes ágazatok kiberfenyegetésekkel szembeni rezilienciáját. Ha a szervezetek tudomást szereznek egy biztonsági 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 a biztonsági eseményről, és lehetővé tegyék a szervezet számára, hogy szükség esetén segítséget kérjen. Az említett bejelentésnek adott esetben fel kell tüntetnie, hogy a biztonsági 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 a biztonsági események kezelésével kapcsolatos tevékenységektől, amelyeket prioritásként kell kezelni. Annak elkerülése érdekében, hogy a biztonsági események bejelentési kötelezettségei elvonják az erőforrásokat a biztonsági 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.

- (55a) **A kiberfenyegetések proaktív megközelítése a kiberbiztonsági kockázatkezelés alapvető eleme, amely várhatóan lehetővé fogja tenni az illetékes hatóságok számára, hogy hatékonyan megakadályozzák, hogy a kiberfenyegetések esetlegesen jelentős vagyoni vagy nem vagyoni veszteséget okozó tényleges biztonsági eseményekké váljanak. E célból kulcsfontosságú a jelentős kiberbiztonsági fenyegetések bejelentése.**
- (56) Az alapvető és a fontos szervezetek gyakran vannak olyan helyzetben, amikor egy adott biztonsági 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 tagállamok[...] **létrehozhatnak** 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 biztonsági 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 a fontos szervezeteket a vélhetően súlyos bűncselekménynek minősülő biztonsági 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) A biztonsági 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 az adatkezelés személyes adatokra is kiterjed, az említett adatkezelésnek meg kell felelnie az uniós adatvédelmi jogszabályoknak.
- (60) Ezen adatok rendelkezésre állása és időben történő hozzáférhetősége a hatóságok – ideértve a bűncselekmények megelőzése, nyomozása vagy a vádeljárás lefolytatása 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 kapcsolódó doménnév-regisztrációs szolgáltatásokat nyújtó szervezeteknek (úgynevezett regisztrátoroknak) össze kell gyűjteniük a doménnevek nyilvántartási adatait és garantálniuk kell azok integritását és elérhetőségét. **A nyilvántartási adatok tekintetében a szervezeteknek ellenőrizniük kell különösen a doménnév bejegyzését igénylők nevét és e-mail-címét.** [...] A legfelső szintű doménnév-nyilvántartóknak és a TLD-hez kapcsolódó doménnév-regisztrációs 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-regisztrációs 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 kapcsolódó doménnév-regisztrációs 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-regisztrációs szolgáltatásokat nyújtó szervezetek **a jogosult hozzáférés-igénylők – például az uniós vagy nemzeti jog szerint a nemzetbiztonság és a büntető igazságszolgáltatás területén illetékes hatóságok vagy a CSIRT-ek – azon kérésére** indokolatlan késedelem nélkül reagáljanak [...], hogy a doménnév-nyilvántartási adatokat nyilvánosságra hozzák. A legfelső szintű doménnév-nyilvántartóknak és a számukra doménnév-regisztrációs 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 tagállamoknak biztosítaniuk kell, hogy a domén-nyilvántartási adatokhoz (a személyes és nem személyes adatokhoz egyaránt) való bármilyen típusú hozzáférés ingyenes legyen.** A Bizottság a belső piacon a harmonizált gyakorlatok előmozdítása érdekében – az Európai Adatvédelmi Testület hatáskörének sérelme nélkül – iránymutatásokat fogadhat el az említett eljárásokról, **összhangban a több érdekelt felet tömörítő közösség által kidolgozott nemzetközi szabványokkal, és kiegészítve azokat.**

²⁵ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (14) preambulumbekzdésének 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”.

- (63) Az ezen irányelv szerinti alapvető és fontos [...] szervezeteknek annak a tagállamnak a joghatósága alá kell tartozniuk, ahol a szolgáltatásaikat nyújtják. **Az ezen irányelv I. mellékletének 1–7. és 10. pontjában említett szervezeteknek, valamint az I. mellékletének 8. pontjában és a II. mellékletének 1–5. pontjában említett bizalmi szolgáltatóknak és internetes exchange pont szolgáltatóknak a letelepedésük helye szerinti tagállam joghatósága alá kell tartozniuk.** Ha a szervezet több tagállamban nyújt szolgáltatásokat **vagy több tagállamban is letelepedési hellyel rendelkezik**, 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. **Amennyiben a tagállamok úgy döntenek, hogy gyakorolják a joghatóságukat, el kell kerülniük, hogy ugyanazt a magatartást többször szankcionálják az ezen irányelvben meghatározott kötelezettségek megsértése miatt.**
- (64) A DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, **a TLD-hez kapcsolódó doménnév-regisztrációs szolgáltatásokat nyújtó szervezetek**, a tartalomszolgáltató hálózati szolgáltatók, a felhőszolgáltatók, az adatközpont-szolgáltatók és a digitális szolgáltatók szolgáltatásai és műveletei határokon átnyúló jellegének figyelembevétele érdekében e szervezetek felett csak egy tagállamnak lehet joghatósága. A joghatóságot annak a tagállamnak kell tulajdonítani, amelyben az adott szervezetnek az Unióban a üzleti tevékenységének fő helye található. A letelepedési kritérium ezen irányelv alkalmazásában a tevékenység állandó megállapodások útján történő tényleges gyakorlását jelenti. Ebben a tekintetben nem meghatározó tényező az említett megállapodások jogi formája, függetlenül attól, hogy fióktelepen vagy jogi személyiséggel rendelkező leányvállalaton keresztül kötötték-e azokat.

E kritérium teljesülése nem függhet attól, hogy a hálózati és információs rendszerek fizikailag egy adott helyen találhatók-e; az említett rendszerek jelenléte és használata önmagukban nem képezi az üzleti tevékenység említett fő helyét, ezért nem meghatározó kritériumok az üzleti tevékenység fő helyének meghatározásához. Az üzleti tevékenység fő helyének annak a helynek kell lennie, ahol az Unióban **túlnyomórészt** meghozzák a kiberbiztonsági kockázatkezelési intézkedésekkel kapcsolatos döntéseket. Ez általában megfelel a vállalatok uniós központi ügyvezetése helyének. Ha **nem lehet meghatározni azt a helyet, ahol túlnyomórészt meghozzák az ilyen döntéseket, vagy ha** nem hoznak az Unióban ilyen döntéseket, 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.

(64a) Amennyiben egy nyilvános elektronikus hírközlő hálózatokat üzemeltető vagy nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltató kizárólag az internet-hozzáférési szolgáltatás részeként nyújt rekurzív DNS-szolgáltatást, úgy kell tekinteni, hogy a szervezet valamennyi olyan tagállamnak a joghatósága alá tartozik, amelyben a szolgáltatásait nyújtja.

(64aa) Az ezen irányelv értelmében az Unióban szolgáltatásokat nyújtó DNS-szolgáltatók, legfelső szintű doménnév-nyilvántartók, TLD-hez kapcsolódó doménnév-regisztrációs szolgáltatásokat nyújtó szervezetek, tartalomszolgáltató hálózati szolgáltatók, felhőszolgáltatók, adatközpont-szolgáltatók és digitális szolgáltatók világos áttekinthetőségének biztosítása érdekében az ENISA-nak létre kell hoznia és fenn kell tartania e szervezetek nyilvántartását, amely a tagállamok által – adott esetben a nemzeti önbejelentési mechanizmusaiokon keresztül – kapott bejelentéseken alapul. Az e nyilvántartásban feltüntetendő információk pontosságának és teljességének biztosítása céljából a tagállamoknak be kell nyújtaniuk az ENISA számára a nemzeti nyilvántartásaikban e szervezetekre vonatkozóan rendelkezésre álló információkat. Az ENISA-nak és a tagállamoknak intézkedéseket kell hozniuk az ilyen nyilvántartások interoperabilitásának elősegítésére, biztosítva ugyanakkor a bizalmas vagy minősített adatok védelmét.

- (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 szolgáltatásokat tervez nyújtani személyek számára egy vagy több tagállamban. A szervezet vagy a közvetítő webhelyének, az e-mail-címnek és más elérhetőségeknek az Unióban való pusztán elérhetősége, vagy a szervezet letelepedési helye 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 megemlítése 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 a biztonsági események bejelentését 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 sebezhetőségekre vonatkozó információk rendszeres megosztásától. Az információmegosztás hozzájárul a kiberfenyegetésekkel kapcsolatos tudatosság erősítéséhez, ami viszont fokozza a szervezetek azon képességét, hogy megakadályozzák a fenyegetések valós biztonsági eseménnyé válását, és lehetővé teszi a szervezetek számára, hogy jobban visszaszorítsák a biztonsági események hatásait és a hatékonyabb helyreállítást. Uniós szintű iránymutatás 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 hálózat- és információbiztonság biztosítása céljából feltétlenül szükséges és arányos mértékben **a személyes adatok alapvető és fontos** szervezetek, [...] valamint biztonsági technológiákat és szolgáltatásokat nyújtó szolgáltatók által történő **kezelését úgy lehet tekinteni, hogy az szükséges a jogi kötelezettség teljesítéséhez vagy az [...]** az érintett adatkezelő jogos érdekét [...] képezi, az (EU) 2016/679 rendeletben említettek szerint. [...] **Ez kiterjedhet** a biztonsági események megelőzésével, felderítésével, elemzésével és az azok elhárításával kapcsolatos intézkedésekre, a konkrét kiberfenyegetésekkel kapcsolatos tudatosság növelésére, a sebezhetőség elhárításával és az összehangolt feltárással kapcsolatos információmegosztásra, valamint az ezekre a biztonsági eseményekre, valamint a kiberfenyegetésekre és sebezhetőségekre, a kompromisszummutatókra, taktikákra, technikákra és eljárásokra, kiberbiztonsági figyelmeztetésekre és konfigurációs eszközökre vonatkozó önkéntes információmegosztásra. Az említett intézkedések megkövetelhetik [...] **olyan különböző** típusú személyes adatok kezelését, **mint például a következők:** IP-címek, egységes forrásazonosítók (URL-ek), doménnevek és e-mail-címek. **A személyes adatoknak az illetékes hatóságok, az egyedüli kapcsolattartó pontok és a CSIRT-ek általi kezelését a nemzeti jogban kell meghatározni, és úgy kell tekinteni, hogy az az (EU) 2016/679 rendelet 6. cikke (1) bekezdésének c) vagy e) pontjában foglaltak szerint szükséges valamely jogi kötelezettség teljesítéséhez, illetve közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához.**
- (69a) A tagállamok jogszabályai olyan szabályokat állapíthatnak meg, amelyek lehetővé teszik az illetékes hatóságok, az egyedüli kapcsolattartó pontok és a CSIRT-ek számára, hogy az alapvető és a fontos szervezetek hálózati és információs rendszerei biztonságának biztosításához feltétlenül szükséges és arányos mértékben – az (EU) 2016/679 rendelet 9. cikkének [...] megfelelően – kezeljék a személyes adatok különleges kategóriáit, különösen azáltal, hogy megfelelő és konkrét intézkedéseket írnak elő a természetes személyek alapvető jogainak és érdekeinek védelme érdekében, ideértve az ilyen adatok további felhasználásának technikai korlátozását, a legkorszerűbb biztonsági és magánéltvédelmi intézkedések alkalmazását – így például az álnevesítést –, valamint a titkosítást, ha az anonimizálás jelentős mértékben befolyásolhatja a kitűzött célt.

- (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 a fontos szervezeteket. Ezen túlmenően ennek az irányelvnek eltérő felügyeleti rendszert kell meghatároznia az alapvető és a fontos szervezetek vonatkozásában annak érdekében, hogy biztosítsa a kötelezettségek méltányos egyensúlyát 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 rendszert. Ez utóbbi esetében ez azt jelenti, hogy a fontos szervezeteknek nem kell szisztematikusan dokumentálniuk a kibebiztonsági 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. **A fontos szervezetek esetében az utólagos felügyeletet bizonyíték vagy az illetékes hatóságok tudomására hozott olyan jelzés vagy információ alapján lehet elindítani, amelyről a hatóságok úgy vélik, hogy az az ezen irányelvben meghatározott kötelezettségeknek való lehetséges meg nem felelésre utal. Ilyen bizonyíték, jelzés vagy információ lehet például a más hatóságok, szervezetek, állampolgárok, a média vagy más források által az illetékes hatóságok rendelkezésére bocsátott információ, továbbá a nyilvánosan hozzáférhető információk, illetve az származhat az illetékes hatóságok által a feladataik ellátása során végzett egyéb tevékenységekből is.**

- (70a) Az előzetes felügyelet végrehajtása során az illetékes hatóságoknak képeseknek kell lenniük arra, hogy arányos módon döntsenek a rendelkezésükre álló felügyeleti intézkedések és eszközök alkalmazásának rangsorolásáról. Ez azt jelenti, hogy az illetékes hatóságok e rangsorolásról olyan felügyeleti módszerek alapján dönthetnek, amelyeknek kockázatalapú megközelítést kell követniük. Konkrétabban, ezek a módszerek tartalmazhatnak kritériumokat vagy referenciaértékeket az alapvető szervezetek kockázati kategóriákba sorolására és a megfelelő felügyeleti intézkedésekre, valamint kockázati kategóriánként ajánlott eszközökre, például a helyszíni ellenőrzések vagy célzott biztonsági ellenőrzések vagy biztonsági vizsgálatok használatára, gyakoriságára vagy típusára, a bekérendő információk típusára és ezen információk részletességének szintjére. Ezeket a felügyeleti módszereket munkaprogramok is kísérhetik, továbbá rendszeresen értékelni kell és felül kell vizsgálni azokat, többek között olyan szempontok alapján, mint az erőforrások elosztása és a szükségletek.**
- (70aa) A közigazgatási szervek tekintetében a felügyeleti hatásköröket a nemzeti keretekkel és jogrenddel összhangban kell gyakorolni. A tagállamok számára lehetővé kell tenni, hogy e szervezetekkel kapcsolatban megfelelő, arányos és hatékony felügyeleti és végrehajtási intézkedések előírásáról döntsenek.**
- (70aaa) Bizonyos kiberbiztonsági kockázatkezelési intézkedéseknek való megfelelés igazolása érdekében a tagállamok megkövetelhetik az alapvető és a fontos szervezetektől, hogy a 910/2014/EU rendelet szerinti minősített bizalmi szolgáltatásokat vagy bejelentett elektronikus azonosítási rendszereket alkalmazzanak.**

- (71) A hatékony végrehajtás érdekében meg kell határozni az ezen irányelvben a kiberbiztonsági kockázatkezelési és bejelentési kötelezettségek megszegése esetére előírt közigazgatási 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. A közigazgatási 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 jogszerű eljárást.
- (71a) **A valamely szervezeten belül bizonyos felelősségi körökkel rendelkező természetes személyek azon kötelezettségének megsértésével kapcsolatos felelősségére vonatkozó rendelkezések, mely szerint biztosítaniuk kell az ezen irányelvben meghatározott kötelezettségek teljesítését, nem írják elő a tagállamok számára, hogy gondoskodjanak arról, hogy az ilyen jogsértések által harmadik felek számára okozott károk miatt sor kerüljön büntetőeljárás lefolytatására vagy a polgári jogi felelősség megállapítására.**
- (72) Az ezen irányelvben megállapított kötelezettségek hatékony végrehajtásának biztosítása érdekében minden illetékes hatóságnak rendelkeznie kell hatáskörrel közigazgatási bírság kiszabására vagy annak indítványozására.

- (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 közigazgatási 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. A büntetőjogi szankcióknak az említett nemzeti szabályok és a kapcsolódó közigazgatási szankciók megsértése esetén történő kiszabása azonban nem ütközhet a *ne bis in idem* elvével, ahogyan azt a Bíróság értelmezi.
- (75) Ha ez az irányelv nem harmonizálja a közigazgatási 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 fogyasztókra 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 azon hiányosságok orvoslására vagy az illetékes hatóság által támasztott azon követelmények teljesítésére, amelyek miatt a szankciók kiszabásra kerültek. 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 jogszerű eljárást, az ártatlanság vélelmét és a védelemhez való jogot.
- (76a) A hatékony felügyelet és végrehajtás biztosítása érdekében – különösen a határokon átnyúló dimenzióval rendelkező esetekben – azon tagállamoknak, amelyek kölcsönös segítségnyújtás iránti megkeresést kaptak, a megkeresés alapján szükséges mértékben megfelelő felügyeleti és végrehajtási intézkedéseket kell hozniuk azon érintett szervezettel kapcsolatban, amely a területükön szolgáltatást nyújt vagy amelynek a hálózati és információs rendszere a területükön található.**

- (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 bejelentési 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) **A kölcsönös bizalom javításának és a bevált gyakorlatokból és a tapasztalatokból való tanulás elősegítése céljából** be kell vezetni egy szakértői [...] **tanulásra szolgáló rendszert**, amely lehetővé teszi a tagállamok által kijelölt szakértők **részvételével történő szakértői csereprogramokat** [...] a kiberbiztonsági politikák végrehajtásának értékeléséről [...]. **A szakértői tanulásra szolgáló rendszer megvalósítása során különös figyelmet kell fordítani annak biztosítására, hogy az ne rójon szükségtelen vagy aránytalan terhet az érintett tagállamok hatóságaira. A Bizottságnak fel kell tárnia minden olyan lehetőséget, amely hozzájárulhat a szakértői tanulásra irányuló kiküldetések szervezéséből esetlegesen felmerülő költségek pénzügyi fedezetének biztosításához. Ezen túlmenően a szakértői tanulásra szolgáló rendszernek figyelembe kell vennie a hasonló mechanizmusok – például a CSIRT-ek hálózatának szakértői értékelési rendszere – eredményeit, hozzáadott értéket kell teremtenie, és el kell kerülnie a párhuzamos munkavégzést. A szakértői tanulásra szolgáló rendszer megvalósítása nem sértheti a bizalmas és minősített adatok védelmére vonatkozó nemzeti vagy uniós jogszabályokat. A szakértői tanulás fordulójának megkezdése előtt a tagállamok önértékelést végezhetnek a releváns szempontok alapján. Az együttműködési csoport kérésére az ENISA szükség esetén iránymutatást nyújthat az önértékelésről és a vonatkozó mintadokumentumokról. A tagállamok dönthetnek úgy, hogy a jelentéseiket nyilvánosan hozzáférhetővé teszik.**

- (80) [...]
- (81) Ezen irányelv vonatkozó rendelkezései végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni az együttműködési csoport működéséhez szükséges eljárási szabályokra, a kockázatkezelési intézkedésekhez kapcsolódó technikai elemekre, a biztonsági események bejelentésében feltüntetendő információ típusára, a bejelentés formátumára és a bejelentési eljárásra, **valamint a szervezetek azon kategóriáira vonatkozóan, amelyeknek bizonyos tanúsított IKT-termékeket, -szolgáltatásokat és -folyamatokat kell használniuk.** Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek megfelelően kell gyakorolni.²⁶
- (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.

²⁶ Az Európai Parlament és a Tanács 182/2011/EU rendelete (2011. február 16.) a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról (HL L 55., 2011.2.28., 13. o.).

- (83) Mivel ezen irányelv célját, nevezetesen a kiberbiztonság Unión belüli egységesen magas szintjének megvalósítását a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban az intézkedés hatásai miatt e cél jobban megvalósítható, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritás elvének megfelelően. Az említett cikkben foglalt arányosság elvének megfelelően ezen irányelv nem lépi túl az e cél 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,

ELFOGADTA EZT AZ IRÁNYELVET:

I. FEJEZET

Általános rendelkezések

1. cikk

Tárgy

- (1) Ez az irányelv **a belső piac működésének javítása érdekében** intézkedéseket határoz meg a hálózati és információs rendszerek egységesen magas szintű biztonságának az Unión belüli megvalósítása céljából.
- (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 bejelentési kötelezettségeket állapít meg az **I. és a II.** mellékletben említett [...] típusú szervezetek számára;
 - c) **szabályokat és** kötelezettségeket állapít meg a kiberbiztonsági információk megosztására vonatkozóan.

2. cikk

Hatály

- (1) Ezt az irányelvet az **I. és a II. mellékletben [...]** felsorolt típusú olyan állami és magánszervezetekre kell alkalmazni, **amelyek elérik vagy meghaladják [...]** a 2003/361/EK bizottsági ajánlás²⁷ értelmében **a középvállalkozásokra vonatkozó határértékeket. Az említett ajánlás melléklete 3. cikkének (4) bekezdése és 6. cikke (2) bekezdésének második és harmadik albekezdése ezen irányelv alkalmazásában nem alkalmazandó.**
- (2) **Az (1) bekezdésben említett szervezetek méretétől függetlenül [...]** ez az irányelv **[...] a következő esetekben is alkalmazandó: [...]**
- a) a szolgáltatásokat a következő szervezetek valamelyike nyújtja:
- i. az I. melléklet 8. pontjában említett nyilvános elektronikus hírközlő hálózatokat **üzemeltető** vagy nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat **nyújtó szolgáltatók;**
 - ii. **az I. melléklet XX. pontjában említett minősített bizalmi szolgáltatók;**
 - iii. **az I. melléklet XX. pontjában említett nem minősített bizalmi szolgáltatók;**
 - iv. az I. melléklet 8. pontjában említett legfelső szintű doménnév-nyilvántartók [...];
- b) [...]

²⁷ A Bizottság 2003/361/EK ajánlása (2003. május 6.) a mikro-, kis- és középvállalkozások meghatározásáról (HL L 124., 2003.5.20., 36. o.).

- c) a szervezet egy tagállamban az egyetlen szolgáltató **egy olyan szolgáltatás tekintetében, amely elengedhetetlen a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához**;
- d) a szervezet által nyújtott szolgáltatás esetleges zavara **jelentős** hatással lehet a közvédelemre, a közbiztonságra vagy a közegészségre;
- e) a szervezet által nyújtott szolgáltatás esetleges zavara **jelentős** rendszerszintű kockázatokat idézhet elő, különösen azokban az ágazatokban, ahol az említett zavarnak határokon átnyúló hatása lehet;
- f) [...];
- g) a szervezetet az (EU) XXXX/XXXX európai parlamenti és tanácsi irányelv²⁸ [A kritikus fontosságú szervezetek rezilienciájáról szóló irányelv] alapján kritikus fontosságú szervezetként, [vagy az említett irányelv 7. cikke alapján a kritikus fontosságú szervezetekkel egyenértékű szervezetként] azonosítják.

(2a) Méretüktől függetlenül ez az irányelv a központi kormányzatoknak a nemzeti joggal összhangban valamely tagállamban elismert és az I. melléklet 9. pontjában említett közigazgatási szerveire is alkalmazandó. A tagállamok dönthetnek úgy, hogy ez az irányelv a regionális és a helyi szintű közigazgatási szervekre is alkalmazandó.

²⁸ [illessze be a teljes címet és a HL-kiadvány hivatkozását, amikor ismertté válik].

(3) [...]

Ez az irányelv nem érinti a tagállamoknak a nemzetbiztonság védelmével kapcsolatos feladatait vagy az egyéb alapvető állami funkciók védelmére vonatkozó hatáskörüket, beleértve az állam területi integritásának biztosítását és a közrend fenntartását.

(3a) 1. Ez az irányelv nem alkalmazandó a következőkre:

- a) az uniós jog hatályán kívül eső szervezetek és minden olyan szervezet, amely főként a védelem, a nemzetbiztonság, a közbiztonság vagy a bűnüldözés területén végez tevékenységet, függetlenül attól, hogy mely szervezet végzi ezeket a tevékenységeket, valamint attól, hogy az közjogi szervezet vagy magánjogi szervezet, a 2. pont sérelme nélkül;**

- b) olyan szervezetek, amelyek az igazságszolgáltatás, a parlamentek és a központi bankok terén folytatnak tevékenységet. [...]

2. Amennyiben a közigazgatási szervek ezeken a területeken csak az általános tevékenységük részeként folytatnak tevékenységeket, teljes egészében ki kell zárni őket ezen irányelv hatálya alól.

(3aa) Ez az irányelv nem alkalmazandó a következőkre:

- i. a szervezetek olyan tevékenységei, amelyek nem tartoznak az uniós jog hatálya alá, valamint a nemzetbiztonsággal vagy a védelemmel kapcsolatos valamennyi tevékenység, függetlenül attól, hogy mely szervezet végzi ezeket a tevékenységeket, valamint attól, hogy az közjogi szervezet vagy magánjogi szervezet;
- ii. az igazságszolgáltatás, a parlamentek, a központi bankok és a közbiztonság területén működő szervezetek tevékenységei, beleértve a bűncselekmények megelőzése, nyomozása, felderítése és büntetőeljárás alá vonása, illetve büntetőjogi szankciók végrehajtása céljából bűnüldözési tevékenységet végző közigazgatási szerveket is.

(3aaa) Az ezen irányelvben meghatározott kötelezettségek nem foglalják magukban olyan információk közlését, amelyek közlése ellentétes a tagállamok alapvető nemzetbiztonsági, közbiztonsági vagy védelmi érdekeivel.

(3aaaa) Ez az irányelv nem érinti a személyes adatok védelmére vonatkozó uniós jogot és különösen az (EU) 2016/679 rendeletet és a 2002/58/EK irányelvet.

(3b) Ez az irányelv nem alkalmazandó azokra a szervezetekre, amelyek az (EU) XXXX/XXXX európai parlamenti és tanácsi rendelet [a DORA-rendelet] 2. cikkének (4) bekezdésének megfelelően mentesülnek a DORA-rendelet alkalmazása alól.

(4) Ezt az irányelvet [...] ²⁹ a 2011/93/EU ³⁰ és a 2013/40/EU ³¹ európai parlamenti és tanácsi irányelv sérelme nélkül kell alkalmazni.

(5) Az EUMSZ 346. cikkének sérelme nélkül, az uniós és nemzeti szabályok értelmében bizalmas információkat – például az üzleti titoktartási szabályokat – csak akkor lehet megosztani a Bizottsággal és **az ezen irányelv szerinti** más érintett hatóságokkal, ha az említett információcsere ezen irányelv alkalmazásához szükséges. A kicserélt információknak az említett információcsere célja szempontjából lényeges és azzal arányos információkra kell korlátozódniuk. Az információcsere során meg kell őrizni a rendelkezésre bocsátott információk bizalmas jellegét, és óvni kell az alapvető és a fontos szervezetek biztonsági és kereskedelmi érdekeit.

²⁹ [...]

³⁰ 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.).

³¹ 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.).

2a. cikk

Alapvető és fontos szervezetek

- (1) Azon szervezetek közül, amelyekre ezt az irányelvet alkalmazni kell, a következők tekintendők alapvetőnek:**
- i. az ezen irányelv I. mellékletének 1–8a. és 10. pontjában említett típusú olyan szervezetek, amelyek meghaladják a közép vállalkozások tekintetében a 2003/361/EK bizottsági ajánlásban meghatározott határértékeket;**
 - ii. a 2. cikk (2) bekezdése a) pontjának i. alpontjában említett közép vállalkozások;**
 - iii. az ezen irányelv 2. cikke (2) bekezdése a) pontjának ii. és iv. alpontjában említett szervezetek, a méretüktől függetlenül;**
 - iv. az ezen irányelv 2. cikke (2) bekezdése g) pontjában és a 2. cikke (2a) bekezdésében említett szervezetek, a méretüktől függetlenül;**
 - v. amennyiben a tagállamok hozták létre, olyan szervezetek, amelyeket a tagállamok ezen irányelv hatálybalépése előtt az (EU) 2016/1148 irányelvvel vagy a nemzeti joggal összhangban alapvető szolgáltatásokat nyújtó szereplőként azonosítottak;**
 - vi. azok a II. mellékletben említett típusú szervezetek, amelyek meghaladják a 2003/361/EK bizottsági ajánlásban a közép vállalkozásokra meghatározott határértékeket, és amelyeket a tagállamok a 2. cikk (2) bekezdésének c)–e) pontjában említett kritériumok alapján alapvető fontosságúnak tartanak;**

- vii. a 2003/361/EK bizottsági ajánlás értelmében vett középvállalkozások, amelyeket a tagállamok a 2. cikk (2) bekezdésének c)–e) pontjában említett kritériumok alapján alapvető fontosságúként határoznak meg;
 - viii. az e cikk (2) bekezdése a) pontjának i. alpontjában meghatározott, vagy a (2) bekezdés c)–e) pontja alapján azonosított, a 2003/361/EK bizottsági ajánlás értelmében vett mikro- vagy kisvállalkozások, amelyeket a tagállamok nemzeti kockázatértékelések alapján alapvető fontosságúként határoznak meg.
- (2) Azon szervezetek közül, amelyekre ezt az irányelvet alkalmazni kell, a következők tekintendők fontos szervezetnek:
- i. az ezen irányelv I. mellékletében meghatározott típusú, a 2003/361/EK bizottsági ajánlás értelmében középvállalkozásoknak minősülő szervezetek, valamint a II. mellékletben meghatározott típusú olyan szervezetek, amelyek elérik vagy meghaladják a 2003/361/EK bizottsági ajánlás³² értelmében a középvállalkozásokra vonatkozó határértékeket;
 - ii. az ezen irányelv 2. cikke (2) bekezdése iii. alpontjában említett szervezetek, a méretüktől függetlenül;
 - iii. a 2. cikk (2) bekezdése a) pontjának i. alpontjában említett kis- és mikrovállalkozások;
 - iv. azon kis- és mikrovállalkozások, amelyeket a tagállamok a 2. cikk (2) bekezdésének c)–e) pontja alapján fontos szervezatként határoznak meg.

³² A Bizottság 2003/361/EK ajánlása (2003. május 6.) a mikro-, kis- és középvállalkozások meghatározásáról (HL L 124., 2003.5.20., 36. o.).

2a. cikk

Bejelentési mechanizmusok

- (1) **A tagállamok nemzeti önbejelentési mechanizmust hozhatnak létre, amelynek keretében előírják az ezen irányelv hatálya alá tartozó valamennyi szervezet számára, hogy legalább a nevüket, címüket, elérhetőségi adataikat, tevékenységi ágazatukat vagy az általuk nyújtott szolgáltatás típusát, valamint adott esetben az ezen irányelv hatálya alá tartozó, általuk nyújtott szolgáltatások helye szerinti tagállamok jegyzékét nyújtsák be az ezen irányelv szerinti illetékes hatóságoknak vagy a tagállamok által erre a célra kijelölt szervezeteknek.**
- (2) **A tagállamok [...] a 2. cikk (2) bekezdésének b)–e) pontja alapján általuk azonosított szervezetekkel kapcsolatban [12 hónappal ezen irányelv átültetési határidejét követően]–ig benyújtják a Bizottságnak legalább az azonosított szervezetek számára, az ágazatukra vagy a mellékletek szerinti, általuk nyújtott szolgáltatás típusára vonatkozó releváns információkat, valamint jelzik a 2. cikk (2) bekezdésének azon konkrét rendelkezését/rendelkezéseit, amely/amelyek alapján e szervezeteket azonosították. A tagállamok [...] ezeket az információkat[...] rendszeresen, de az említett időpontot követően legalább két évente felülvizsgálják, és adott esetben frissítik.**

2b. cikk

Ágazatspecifikus uniós jogi aktusok

- (1) Ha [...] az ágazatspecifikus **uniós jogi** aktusok [...] megkövetelik, hogy az alapvető vagy fontos szervezetek [...] kiberbiztonsági kockázatkezelési intézkedéseket fogadjanak el, vagy bejelentsék a **jelentős** biztonsági eseményeket vagy [...] kiberfenyegetéseket, és ha ezek a követelmények hatásukban legalább egyenértékűek az ezen irányelvben meghatározott kötelezettségekkel, akkor ezen irányelv vonatkozó rendelkezései – **beleértve a VI. fejezetben meghatározott, a felügyeletre és a végrehajtásra vonatkozó rendelkezéseket** – nem alkalmazandók az **említett szervezetekre**. Amennyiben az ágazatspecifikus uniós jogi aktusok **nem terjednek ki az ezen irányelv hatálya alá tartozó adott ágazatban működő valamennyi szervezetre, ezen irányelv vonatkozó rendelkezései továbbra is alkalmazandók azokra a szervezetekre, amelyek nem tartoznak az említett ágazatspecifikus rendelkezések hatálya alá.**
- (2) Az e cikk (1) bekezdésében említett követelmények az ezen irányelvben meghatározott kötelezettségekkel hatásukban egyenértékűnek tekintendők, ha az adott ágazatspecifikus uniós jogi aktus előírja az illetékes hatóságok ezen irányelv szerinti biztonságiesemény-bejelentéseihez vagy a kijelölt CSIRT-ekhez való azonnali – adott esetben automatikus és közvetlen – hozzáférést, és ha:
- a) a kiberbiztonsági kockázatkezelési intézkedések hatásukban legalább egyenértékűek az ezen irányelv 18. cikkének (1) és (2) bekezdésében meghatározottakkal; vagy
 - b) a jelentős biztonsági események bejelentésére vonatkozó követelmények hatásukban legalább egyenértékűek a 20. cikk (1)–(6) bekezdésében meghatározottakkal.

- (3) A Bizottság az uniós jogi aktusok ágazatspecifikus rendelkezéseivel összefüggésben rendszeresen felülvizsgálja az e cikk (1) és (2) bekezdésében előírt, egyenértékű hatásra vonatkozó követelmények alkalmazását. Az említett időszakos felülvizsgálatok előkészítése során a Bizottság konzultál az együttműködési csoporttal és az ENISA-val.

3. cikk

Minimális harmonizáció

A tagállamok az uniós jog szerinti egyéb kötelezettségeik sérelme nélkül [...] magasabb szintű kiberbiztonságot biztosító rendelkezéseket fogadhatnak el vagy tarthatnak fenn **az ezen irányelv hatálya alá tartozó területeken.**

4. cikk

Fogalommeghatározások

Ezen irányelv alkalmazásában:

1. „hálózati és információs rendszer”:

- a) az (EU) 2018/1972 irányelv 2. cikkének 1. pontja értelmében vett elektronikus hírközlő hálózat;
- b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi;
- c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

2. „hálózati és információs rendszerek biztonsága”: a hálózati és információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan **eseménynek**, amely veszélyeztetheti [...] a tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát;
- 2a. „elektronikus hírközlési szolgáltatások”: az (EU) 2018/1972 irányelv 2. cikkének 4. pontja értelmében vett elektronikus [...] hírközlési szolgáltatások;**
3. „kiberbiztonság”: az (EU) 2019/881 európai parlamenti és tanácsi rendelet³³ 2. cikkének 1. pontja értelmében vett kiberbiztonság;
4. „nemzeti **kiberbiztonsági** stratégia”: [...] olyan koherens tagállami keret, amely [...] iránymutatást határoz meg az adott tagállam [...] **kiberbiztonsága területén** elérendő stratégiai célok és prioritások megvalósításához;
5. „biztonsági esemény”: minden olyan esemény, amely veszélyezteti a tárolt, továbbított vagy kezelt adatok vagy a hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető [...] szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát;
- 5a. „nagy szabású kiberbiztonsági esemény”: olyan biztonsági esemény, amely legalább két tagállamra jelentős hatást gyakorol, vagy az általa keltett zavar meghaladja az adott tagállam reagálási kapacitását;**

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.).

6. „biztonsági esemény kezelése”: minden olyan intézkedés és eljárás, amely a biztonsági események észlelését, elemzését és elszigetelését, valamint a rájuk való reagálást célozza;
- 6a. **„kockázat”: egy biztonsági esemény által potenciálisan okozható veszteség vagy zavar mértéke, amelyet az említett veszteség vagy zavar nagyságrendjének és az említett biztonsági esemény bekövetkezési valószínűségének kombinációjaként kell kifejezni;**
7. „kiberfenyegetés”: az (EU) 2019/881 rendelet 2. cikkének 8. pontja értelmében vett kiberfenyegetés;
- 7a. **„jelentős kiberfenyegetés”: olyan kiberfenyegetés, amelyről – technikai jellemzői alapján – feltételezhető, hogy jelentős vagyoni vagy nem vagyoni veszteséget okozva súlyos hatást gyakorolhat egy szervezet hálózati és információs rendszereire vagy azok felhasználóira;**
8. „sebezhetőség”: valamely IKT-eszköz vagy rendszer [...] olyan gyengesége, érzékenysége vagy hiányossága, amely egy kiberfenyegetés során kihasználható;
- 8a. **„majdnem bekövetkezett (near miss) esemény”: olyan esemény, amely kárt okozhatott volna valamely szervezet hálózati és információs rendszereinek vagy azok felhasználóinak, de teljes kibontakozását sikeresen megakadályozták;**
9. „képviselő”: az Unióban letelepedett minden olyan természetes vagy jogi személy, akit vagy amelyet kifejezetten kijelöltek arra, hogy az Unióban nem letelepedett, i. az I. melléklet 8. pontjában említett DNS-szolgáltatók, legfelső szintű doménnév-nyilvántartók, felhőszolgáltatók, adatközpont-szolgáltatók, tartalomszolgáltató hálózati szolgáltatók, vagy ii. a II. melléklet [...] 6. pontjában említett szervezetek nevében eljárjon, és akihez vagy amelyhez az illetékes nemzeti hatóság vagy a CSIRT a szervezet ezen irányelv szerinti kötelezettségeit illetően az adott szervezet helyett fordulhat;

10. „szabvány”: az 1025/2012/EU európai parlamenti és tanácsi rendelet³⁴ 2. cikkének 1. pontja értelmében vett szabvány;
11. „műszaki előírás”: az 1025/2012/EU rendelet 2. cikkének 4. pontja értelmében vett műszaki előírás;
12. „internetes exchange pont (IXP)”: olyan hálózati létesítmény, amely elsősorban az internetes forgalomcsere megkönnyítése érdekében lehetővé teszi kettőnél több, egymástól független hálózat (autonóm rendszer) összekapcsolását; az IXP kizárólag autonóm rendszerek részére biztosít összekapcsolást; az IXP nem kívánja meg, hogy a részt vevő bármely két autonóm rendszer között zajló internetes forgalom egy bármely harmadik autonóm rendszeren is áthaladjon, továbbá nem változtatja meg az említett forgalmat és egyéb módon sem avatkozik be abba;
13. „doménnévrendszer (DNS)”: olyan 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 autoritatív doménnév-feloldási szolgáltatásokat nyújt [...] **harmadik felek általi felhasználásra, a gyökérnévszerverek kivételével** [...];

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.).

15. „legfelső szintű doménnév-nyilvántartó”: olyan szervezet, amelyre egy konkrét legfelső szintű domént (TLD) bízta, és amely felelős egyrészt a TLD kezeléséért – ideértve a TLD alatti doménnevek nyilvántartásba vételét –, másrészt a TLD technikai üzemeltetéséért, amely magában foglalja a névszerverek üzemeltetését, adatbázisainak karbantartását és a TLD zónafájlok elosztását a névszerverek között, **kivéve azon eseteket, amikor a legfelső szintű doménnéveket a nyilvántartó kizárólag saját használatra veszi igénybe;**
- 15a. „a TLD-hez kapcsolódó doménnév-regisztrációs szolgáltatásokat nyújtó szervezetek”: a TLD név-nyilvántartók, a TLD-k regisztrátorai és a regisztrátorok ügynökei, például viszonteladók és proxy szolgáltatók;**
16. „digitális szolgáltatás”: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv³⁵ 1. cikke (1) bekezdésének b) pontja értelmében vett szolgáltatás;
- 16a. „bizalmi szolgáltatások”: a 910/2014/EU rendelet 3. cikkének 16. pontja értelmében vett bizalmi szolgáltatások;**

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.).

- 16b. „minősített bizalmi szolgáltató”: a 910/2014/EU rendelet 3. cikkének 20. pontja értelmében vett minősített bizalmi szolgáltató;**
17. „online piactér”: a 2005/29/EK európai parlamenti és tanácsi irányelv³⁶ 2. cikkének n) pontja értelmében vett digitális szolgáltatás;
18. „online keresőprogram”: az (EU) 2019/1150 európai parlamenti és tanácsi rendelet³⁷ 2. cikkének 5. pontja értelmében vett digitális szolgáltatás;
19. „felhőszolgáltatás”: olyan digitális szolgáltatás, amely igény szerinti adminisztrációt és kiterjedt távoli hozzáférést tesz lehetővé a megosztható [...] számítástechnikai erőforrások méretezhető és rugalmas pooljához, **beleértve azt is, amikor azokat több helyszínen osztják el;**
20. „adatközpont-szolgáltatás”: olyan szolgáltatás, amelynek részét képezik olyan struktúrák vagy struktúracsoportok, amelyek az adattárolási, -kezelési és -továbbítási szolgáltatásokat nyújtó információs technológiai és hálózati berendezések központosított elhelyezésére, összekapcsolására és működtetésére szolgálnak a villamosenergia-elosztás és a környezetvédelmi ellenőrzés összes létesítményével és infrastruktúrájával együtt;

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.).

21. „tartalomszolgáltató hálózat”: földrajzilag elosztott szerverek hálózata, amelynek célja a tartalomszolgáltatók és a szolgáltatásokat nyújtók nevében biztosítani, hogy a digitális tartalmak és szolgáltatások széleskörűen, zökkenőmentesen 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”: olyan szerv, **amelyet az adott tagállam a nemzeti joggal összhangban ilyenként elismer, [...]** és amely megfelel a következő kritériumoknak:
- a) az általános érdekű szükségletek kielégítése céljából jött létre, és nincs ipari vagy kereskedelmi jellege;
 - b) jogi személyiséggel rendelkezik, **vagy jogszabály alapján jogosult egy másik jogi személyiséggel rendelkező szervezet nevében eljárni;**
 - c) finanszírozását többnyire állam, regionális hatóság vagy más, közjog által szabályozott szervek végzik; irányítása az említett hatóságok vagy szervek felügyelete alatt áll; vagy van olyan igazgatási, irányító vagy felügyelő testülete, amely tagjainak több mint felét az állam, a regionális hatóságok vagy más közjogi szerv nevezi ki;
 - d) hatásköre van arra, hogy természetes vagy jogi személyekhez a személyek, áruk, szolgáltatások vagy tőke határokon átnyúló mozgásával kapcsolatos jogaikat érintő közigazgatási vagy szabályozási határozatokat intézzon;
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;

25. „alapvető szervezet”: [...] az I. mellékletben meghatározott típusú szervezet, amely a 2a. cikk (1) bekezdése szerint „alapvetőnek” minősül;
26. „fontos szervezet”: [...] az I. és II. mellékletben meghatározott típusú szervezet, amely a 2a. cikk (2) bekezdése szerint „fontosnak” minősül;
- 26a. „IKT-termék”: az (EU) 2019/881 rendelet 2. cikkének 12. pontja értelmében vett IKT-termék;
- 26aa. „IKT-szolgáltatás”: az (EU) 2019/881 rendelet 2. cikkének 13. pontja értelmében vett IKT-szolgáltatás;
- 26ab. „IKT-folyamat”: az (EU) 2019/881 rendelet 2. cikkének 14. pontja értelmében vett IKT-folyamat;
- 26ac. „felügyelt szolgáltató”: minden olyan szervezet, amely folyamatos és rendszeres irányítás, támogatás és aktív adminisztráció révén szolgáltatásokat – például hálózatot, alkalmazást, infrastruktúrát és biztonságot – nyújt az ügyfelek helyiségeiben, a felügyelt szolgáltató (MSP) adatközpontjában (tárhelyszolgáltatás) vagy harmadik fél adatközpontjában;
- 26ad. „felügyelt biztonsági szolgáltató”: minden olyan szervezet, amely a biztonsági eszközök és rendszerek kiszervezett nyomon követését és kezelését végzi. A közös szolgáltatások közé tartozik a felügyelt tűzfal, a behatolásérzékelés, a virtuális magánhálózat, a sebezhetőségi vizsgálat és a vírusirtó szolgáltatások.

Magukban foglalják továbbá a magas rendelkezésre állású biztonsági műveleti központok igénybevételét (akár saját létesítményeikben, akár más adatközpont-szolgáltatóknál) a hét minden napján 24 órában olyan szolgáltatások nyújtásához, amelyek célja, hogy csökkenteni lehessen azon biztonsági műveleti személyzet létszámát, amelyet a vállalatnak fel kell vennie, képeznie kell és meg kell tartania az elfogadható kiberbiztonsági helyzetének fenntartásához.

II. FEJEZET

Összehangolt kiberbiztonsági szabályozási keretek

5. cikk

Nemzeti kiberbiztonsági stratégia

- (1) A magas szintű kiberbiztonság elérése és fenntartása céljából minden tagállam nemzeti kiberbiztonsági stratégiát fogad el, amelyben meghatározza a stratégiai célokat, valamint a megfelelő szakpolitikai és szabályozási intézkedéseket. A nemzeti kiberbiztonsági stratégiának különösen a következőket kell tartalmaznia:
- a) a kiberbiztonságra vonatkozó tagállami stratégia céljai és prioritásai [...];
 - b) irányítási keretrendszer az említett célok és prioritások elérése érdekében, ideértve a (2) bekezdésben említett politikákat, valamint a stratégia végrehajtásában részt vevő különféle hatóságok és szereplők [...] szerepét és felelősségi körét;
 - c) [...] **iránymutatás** a releváns eszközök azonosítására és az adott tagállamban fennálló kiberbiztonsági kockázatok **felmérésére** vonatkozóan [...];
 - d) a kiberbiztonsági eseményekre való felkészültséget, reagálást és a helyreállítást biztosító intézkedések azonosítása, ideértve a köz- és a magánszféra közötti együttműködést is;
 - e) [...]

f) az ezen irányelv és az (EU) XXXX/XXXX európai parlamenti és tanácsi irányelv³⁸ [a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv] szerinti illetékes hatóságok közötti, a [...] **kiberbiztonsági kockázatokkal**, a kiberfenyegetésekkel és a **biztonsági eseményekkel, továbbá a nem kiberbiztonsági jellegű kockázatokkal, fenyegetésekkel és eseményekkel** kapcsolatos információk megosztását és **adott esetben** a felügyeleti feladatok ellátását célzó fokozott koordináció politikai kerete.

fa) az ezen irányelv szerinti illetékes hatóságok és az ágazatspecifikus jogszabályok alapján kijelölt illetékes hatóságok közötti koordinációra és együttműködésre vonatkozó szakpolitikai keret.

(2) A nemzeti kiberbiztonsági stratégia részeként a tagállamok különösen a következő politikákat fogadják el:

- a) a [...] szervezetek által szolgáltatásaik nyújtásához használt IKT-termékek és -szolgáltatások ellátási láncának kiberbiztonságával foglalkozó politika;
- b) [...] az IKT-termékek és -szolgáltatások kiberbiztonsággal kapcsolatos követelményeinek, **többek között a kiberbiztonsági tanúsításnak** a közbeszerzésekbe történő felvételére és meghatározására vonatkozó **politika**;
- c) **a sebezhetőségek kezelésére vonatkozó politika, amely magában foglalja a 6. cikk (1) bekezdése szerinti [...] önkéntes összehangolt sebezhetőség-feltárás előmozdítását és megkönnyítését**;
- d) a nyílt internet nyilvános alkotóelemei általános rendelkezésre állásának, [...] sértetlenségének és **bizalmasságának** fenntartásával kapcsolatos politika;
- e) a kiberbiztonsági **oktatás és képzés**, készségek és figyelemfelkeltés előmozdítására és fejlesztésére, valamint a kutatási és fejlesztési kezdeményezésekre vonatkozó politika;

³⁸ [illesse be a teljes címet és a HL-kiadvány hivatkozását, amikor ismertté válik].

- 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, amely szükségletek a kiber[...]fenyegetésekkel szembeni rezilienciájuk javítása terén nyújtott iránymutatással és támogatással kapcsolatosak.
- (3) A tagállamok az elfogadástól számított három hónapon belül értesítik a Bizottságot nemzeti kiberbiztonsági stratégiájukról. **E tájékoztatásból** a tagállamok kihagyhatják **a stratégia** [...] nemzetbiztonsággal **kapcsolatos elemeit**.
- (4) A tagállamok a legfontosabb teljesítménymutatók alapján rendszeresen, de legalább [...] **ötévente** értékeli nemzeti kiberbiztonsági stratégiájukat, és szükség esetén módosítják azt. Az Európai Unió Kiberbiztonsági Ügynökség (ENISA) kérésre segítséget nyújt a tagállamoknak a nemzeti stratégia és a stratégia értékeléséhez szükséges fő teljesítménymutatók kidolgozásához.

Összehangolt sebezhetőség-feltárás és európai sebezhetőség-nyilvántartás

- (1) Minden tagállam kijelöli a 9. cikkben említett egyik CSIRT-jét koordinátorként az összehangolt sebezhetőség-feltárás céljából. A kijelölt CSIRT-nek megbízható közvetítőként kell eljárnia, szükség esetén megkönnyítve a bejelentő szervezet, **a potenciális sebezhetőség-tulajdonos** és az IKT-termékek vagy IKT-szolgáltatások gyártója vagy szolgáltatója közötti kapcsolattartást. **Bármely természetes vagy jogi személy – akár névtelenül – bejelentheti a kijelölt CSIRT-nek a 4. cikk 8. pontjában említett sebezhetőséget. A kijelölt CSIRT-nek biztosítania kell a bejelentés gondos nyomon követését és a sebezhetőséget bejelentő személy személyazonosságának bizalmas kezelését.** Ha a bejelentett sebezhetőség [...] **több tagállamban is jelentős hatást gyakorolhat szervezetekre**, az érintett tagállamok kijelölt CSIRT-jének **adott esetben** együtt kell működnie **a többi kijelölt CSIRT-tel** a CSIRT-ek hálózatán **belül**.
- (2) Az ENISA **az együttműködési csoporttal konzultálva** kifejleszti és fenntartja az európai sebezhetőség-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 a hálózati és információs rendszereket biztosító szolgáltatóik számára lehetővé tegye az IKT-termékekben vagy az IKT-szolgáltatásokban található, **nyilvánosan ismert sebezhetőségek önkéntes alapon történő** feltárását és nyilvántartását, és hogy az összes érdekelt fél számára hozzáférést biztosítson a nyilvántartásba vett sebezhetőségekre vonatkozó információkhoz. A nyilvántartásnak információkat kell tartalmaznia különösen a sebezhetőségről, az érintett IKT-termékről vagy IKT-szolgáltatásokról, valamint a sebezhetőség súlyosságáról a kihasználható körülmények, a kapcsolódó javítások rendelkezésre állása és a javítás hiánya fényében, és elérhető javítás hiányában **az illetékes nemzeti hatóságok vagy a CSIRT-ek által kiadott** iránymutatással kell szolgálnia a sebezhetőséggel érintett termékek és szolgáltatások felhasználóinak arról, hogy miként csökkenthetők a feltárt sebezhetőségekből fakadó kockázatok. **Az ENISA biztosítja, hogy az európai sebezhetőség-nyilvántartás biztonságos és reziliens kommunikációs és információs infrastruktúrát használjon.**

Nemzeti kiberbiztonsági válságkezelési keretek

- (1) Minden tagállam kijelöl egy vagy több illetékes hatóságot, amely felelős a nagyszabású **kiberbiztonsági** események és válságok kezeléséért. A tagállamok biztosítják, hogy az illetékes hatóságok megfelelő erőforrásokkal rendelkezzenek a rájuk bízott feladatok hatékony és eredményes ellátásához. **A tagállamok biztosítják a koherenciát a meglévő általános válságkezelési keretekkel.**
- (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) kiberbiztonsági válságkezelési eljárások, **beleértve azok integrálását az általános nemzeti válságkezelési keretbe** és az információcserére szolgáló csatornába;
 - d) felkészültségi intézkedések, beleértve a rendszeres gyakorlatokat és képzési tevékenységeket;
 - e) az érintett állami és magán[...]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 [...] **tájékoztatják** a Bizottságot az (1) bekezdésben említett illetékes hatóságaik kijelöléséről, a nemzeti kiberbiztonsági esemény- és válságelhárítási terveikre **vonatkozó, az e cikk (3) bekezdésében említett követelményekkel kapcsolatos releváns információkat pedig** [...] a kijelöléstől és a tervek elfogadásától számított három hónapon belül benyújtják. A tagállamok kihagyhatnak bizonyos információkat [...], annyiban és amennyiben ez nemzetbiztonságuk, **közbiztonságuk vagy védelmük** szempontjából [...] 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 (a továbbiakban: 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 a biztonsági eseményeknek egy jól meghatározott eljárással összhangban történő 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. **E feladatok ellátása során a CSIRT-ek kockázatalapú megközelítés alapján előnyben részesíthetik meghatározott szolgáltatások szervezetek számára történő nyújtását.**
- (3) A tagállamok biztosítják, hogy minden CSIRT rendelkezzen megfelelő, biztonságos és reziliens 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 releváns információkat cserélnek az alapvető és fontos szervezetek megbízható ágazati vagy ágazatközi közösségeivel.
- (5) A CSIRT-ek részt vesznek a 16. cikkel összhangban szervezett szakértői [...] **tanulásban**.
- (6) A tagállamok biztosítják, hogy a CSIRT-jeik hatékonyan, eredményesen és biztonságosan működnek együtt a 13. cikkben említett CSIRT-ek hálózatában.
- (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 kialakításához.

10. cikk

A CSIRT-ekre vonatkozó követelmények és feladataik

- (1) A CSIRT-eknek meg kell felelniük a következő követelményeknek:
 - a) a CSIRT-eknek a kritikus hibapontok kiküszöbölése révén biztosítaniuk kell a kommunikációs [...] **csatornáik** magas szintű elérhetőségét, továbbá elérhetőségük és másokkal való kapcsolattartásuk céljára folyamatosan több eszközt kell fenntartaniuk. A CSIRT-eknek a kommunikációs csatornákat egyértelműen meg kell határozniuk, és azokat a felhasználóik és az együttműködési partnereik tudomására kell hozniuk;
 - b) a CSIRT-ek hivatali helyiségeit és a támogató információs rendszereket biztonságos helyszíneken kell elhelyezni;

- c) a CSIRT-eknek megfelelő rendszerrel kell rendelkezniük a megkeresések kezelésére és továbbítására, különösen a hatékony és eredményes átadás megkönnyítése céljából;
- d) a CSIRT-eket elegendő személyzettel kell ellátni ahhoz, hogy mindig készenlétben legyenek;
- e) a CSIRT-eket redundáns rendszerekkel és tartalék munkaterülettel kell ellátni a szolgáltatásuk folyamatosságának biztosítása érdekében;
- f) a CSIRT-ek számára lehetővé kell tenni, hogy részt vehessenek nemzetközi együttműködési hálózatokban.

(2) A CSIRT-eknek a következő feladatokat kell ellátniuk:

- a) a kiberfenyegetések, a sebezhetőségek és a biztonsági események nemzeti szintű monitoringja;
- b) a kiberfenyegetésekkel, a sebezhetőségekkel és a biztonsági eseményekkel kapcsolatos korai előrejelzés, riasztás, bejelentéstétel és információterjesztés az alapvető és fontos szervezetek, valamint **az illetékes hatóságok és az egyéb releváns érdekelték számára;**
- c) reagálás a biztonsági eseményekre;
- d) forenzikus adatok gyűjtése és elemzése, továbbá dinamikus kockázat- és eseményelemzés, valamint a kiberbiztonsággal kapcsolatos helyzetismeret biztosítása;
- e) [...] a [...] hálózati és információs rendszerek proaktív vizsgálatának biztosítása **az olyan sebezhetőségek észlelése céljából, amelyek jelentős hatást gyakorolhatnak, feltéve, hogy az adott szervezet hozzájárulása nélkül nem hatolnak be a hálózati és információs rendszerekbe, illetve nem gyakorolnak negatív hatást azok működésére;**

- f) részvétel a CSIRT-ek hálózatában, valamint **kapacitásainak és hatásköreiknek megfelelően** kölcsönös segítségnyújtás a hálózat többi tagjának azok kérésére;
 - fa) **adott esetben a 6. cikk (1) bekezdése szerinti összehangolt sebezhetőség-feltárás céljából koordinátori szerep betöltése, amelynek magában kell foglalnia különösen a bejelentő szervezetek, a potenciális sebezhetőség-tulajdonos és az IKT-termékek vagy IKT-szolgáltatások gyártója vagy szolgáltatója közötti kapcsolattartás megkönnyítését, szükség esetén az érintett szervezetek azonosítását és a velük való kapcsolatfelvételt, a bejelentő szervezetek támogatását, a feltárás ütemtervének megtárgyalását és a több szervezetet érintő sebezhetőségek kezelését (több felet érintő összehangolt sebezhetőség-feltárás).**
- (3) A CSIRT-eknek az irányelv céljainak jobb megvalósítása érdekében együttműködési kapcsolatokat kell kialakítaniuk a magánszektor érintett szereplőivel.
- (3a) A CSIRT-ek együttműködési kapcsolatokat alakíthatnak ki a harmadik országok nemzeti CSIRT-jeivel. Ezen együttműködés részeként az adatvédelemre vonatkozó uniós joggal összhangban releváns információkat, többek között személyes adatokat cserélhetnek egymással.**
- (4) Az együttműködés megkönnyítése érdekében a CSIRT-eknek közös vagy szabványosított gyakorlatok, osztályozási rendszerek és taxonómiák elfogadását és alkalmazását kell szorgalmazniuk az alábbiakra vonatkozóan:
- a) a biztonsági események kezelésére vonatkozó eljárások;
 - b) kiberbiztonsági válságkezelés;
 - c) összehangolt sebezhetőség-feltárás.

11. cikk

Nemzeti szintű együttműködés

- (1) Ugyanazon tagállam 8. cikkben említett illetékes hatóságai, egyedüli kapcsolattartó pontja, valamint CSIRT-je(i), amennyiben különállóak, kötelesek egymással együttműködni az ezen irányelvben meghatározott kötelezettségek végrehajtása tekintetében.
- (2) A tagállamok biztosítják, hogy vagy az illetékes hatóságaik vagy a CSIRT-jeik megkapják az ezen irányelv alapján tett bejelentéseket a biztonsági eseményekről, jelentős kiberfenyegetésekről és majdnem bekövetkezett (near miss) eseményekről. Ha egy tagállam úgy dönt, hogy a 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 biztonsági eseményekre vonatkozó adatokhoz.
- (3) Minden tagállam biztosítja, hogy illetékes hatóságai vagy CSIRT-jei tájékoztassák az egyedüli kapcsolattartó pontját az ezen irányelv alapján bejelentett biztonsági eseményekről, jelentős kiberfenyegetésekről és majdnem bekövetkezett (near miss) eseményekről.

- (4) Az ebben az irányelvben meghatározott feladatok és kötelezettségek eredményes végrehajtásához szükséges mértékben a tagállamok az adott tagállamon belül biztosítják a megfelelő együttműködést az illetékes hatóságok, **a CSIRT-ek, az egyedüli kapcsolattartó pontok és a bűnüldöző hatóságok, az adatvédelmi hatóságok és az (EU) XXXX/XXXX irányelv [a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv [...]] szerint kijelölt [...] illetékes hatóságok, az (EU) 2019/1583 bizottsági végrehajtási rendelet szerinti illetékes hatóságok, az (EU) 2018/1972 irányelvvel összhangban kijelölt nemzeti szabályozó hatóságok, a 910/2014/EU rendelet 17. cikkével összhangban kijelölt nemzeti hatóságok, [...] az (EU) XXXX/XXXX európai parlamenti és tanácsi rendelettel [a DORA-rendelet] összhangban kijelölt nemzeti pénzügyi hatóságok, továbbá az egyéb ágazatspecifikus uniós jogi aktusokkal kijelölt illetékes hatóságok között.**
- (5) A tagállamok biztosítják, hogy **az ezen irányelv szerinti illetékes hatóságaik és az (EU) XXXX/XXXX irányelv [a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv] szerint kijelölt illetékes hatóságok rendszeresen [...] információt cseréljenek [...] a kritikus fontosságú szervezetek, a kiberbiztonsági kockázatok, a kiberfenyegetések és a biztonsági események azonosításáról, továbbá az (EU) XXXX/XXXX irányelv [a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv] szerint kritikus fontosságúként [vagy a kritikus fontosságú szervezetekkel egyenértékű szervezetként] azonosított alapvető szervezeteket érintő nem kiberbiztonsági jellegű kockázatokról, fenyegetésekről és eseményekről, valamint az [...] említett kockázatokra és biztonsági eseményekre való reagálásként hozott intézkedésekről. A tagállamok biztosítják továbbá, hogy az ezen irányelv szerinti illetékes hatóságok [...] és az (EU) XXXX/XXXX rendelet [DORA-rendelet], az (EU) 2018/1972 irányelv és a 910/2014/EU rendelet szerint kijelölt illetékes hatóságok egymással rendszeresen releváns információkat cseréljenek.**

A bizalmi szolgáltatókat illetően, és [...] különösen [...] abban az esetben, ha az ezen irányelv szerinti említett felügyeleti szerepet a 910/2014/EU rendelet szerint kijelölt felügyeleti szervektől eltérő szervre bízják, az ezen irányelv szerinti illetékes nemzeti hatóságoknak szorosan és kellő időben együtt kell működniük egymással azáltal, hogy megosztják egymással a releváns információkat annak érdekében, hogy biztosítsák a bizalmi szolgáltatók hatékony felügyeletét és az ezen irányelvben, valamint az (EU) [XXXX/XXXX] rendeletben meghatározott követelményeknek való megfelelésüket, **továbbá adott esetben az ezen irányelv szerinti illetékes nemzeti hatóságnak indokolatlan késedelem nélkül tájékoztatnia kell az eIDAS-rendelet szerinti felügyeleti szervet minden olyan bejelentett jelentős kiberfenyegetésről vagy biztonsági eseményről, amely hatással van a bizalmi szolgáltatásokra.**

- (5a) A [...] biztonsági események bejelentésének egyszerűsítése céljából a tagállamok egyedüli kapcsolattartó pontot hozhatnak létre az ezen irányelv, az (EU) 2016/679 rendelet és a 2002/58/EK irányelv által előírt összes bejelentés tekintetében. A tagállamok az egyedüli kapcsolattartó pontot alkalmazhatják az egyéb ágazatspecifikus uniós jogi aktusokban előírt bejelentésekhez is. Az egyedüli kapcsolattartó pont nem érinti az (EU) 2016/679 rendelet és a 2002/58/EK irányelv rendelkezéseinek alkalmazását, különös tekintettel a független felügyeleti hatóságokra vonatkozó rendelkezésekre.**

III. FEJEZET

Unió együttműködés

12. cikk

Együttműködési csoport

- (1) Egy együttműködési csoport kerül létrehozásra a tagállamok közötti stratégiai együttműködés és információcsere támogatása és megkönnyítése, **valamint [...] a bizalom erősítése [...]** érdekében.
- (2) Az együttműködési csoport a (6) bekezdésben említett kétéves munkaprogramok keretében végzi feladatait.
- (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 (EFH-k) és az **(EU) XXXX/XXXX rendelet [a DORA-rendelet] szerint kijelölt illetékes hatóságok [...] az (EU) XXXX/XXXX rendelet [a DORA-rendelet] 42. cikkének (1) bekezdésével összhangban** részt vehetnek az együttműködési csoport tevékenységeiben.

Az együttműködési csoport adott esetben az érdekelt felek képviselőit is felkérheti, hogy vegyenek részt a munkájában.

A titkárságot a Bizottság biztosítja.

- (4) Az együttműködési csoport a következő feladatokat látja el:
 - a) iránymutatás nyújtása az illetékes hatóságok számára ezen irányelv átültetésével és végrehajtásával kapcsolatban;
 - aa) **iránymutatás nyújtása az 5. cikk (2) bekezdésének c) pontjában és a 6. cikk (1) bekezdésében említett összehangolt sebezhetőség-feltáráshoz vonatkozó politikák kidolgozásához és végrehajtásához;**

- b) az ezen irányelv végrehajtásával kapcsolatos bevált gyakorlatok és információk cseréje, többek között a kiberfenyegetések, a biztonsági események, a sebezhetőségek, a majdnem bekövetkezett (near miss) események, a figyelemfelkeltő kezdeményezések, a képzések, gyakorlatok és készségek, a kapacitásépítés, valamint a szabványok és a műszaki előírások tekintetében;
- c) tanácsadás és együttműködés a Bizottsággal a kialakulóban lévő kiberbiztonsági politikai kezdeményezésekkel kapcsolatban;
- d) tanácsadás és együttműködés a Bizottsággal az ezen irányelv alapján elfogadott bizottsági végrehajtási [...] jogi aktusok tervezetével kapcsolatban;
- e) bevált gyakorlatok és információk cseréje az érintett uniós intézményekkel, szervezetekkel, hivatalokkal és ügynökségekkel;
- ea) véleménycsere a kiberbiztonsági szempontokat tartalmazó ágazati jogszabályok végrehajtásáról;**
- f) a 16. cikk (7) bekezdésében említett szakértői [...] **tanulásról** szóló jelentések megvitatása;
- g) a 34. cikkben említett, határokon átnyúló esetekben végzett közös felügyeleti tevékenységek során szerzett **tapasztalatok** [...] megvitatása;
- h) stratégiai iránymutatás nyújtása a CSIRT-ek hálózata és az EU–CyCLONe számára konkrét felmerülő kérdésekben;

ha) véleménycsere a nagyszabású kiberbiztonsági események szakpolitikai nyomon követéséről a CSIRT-ek hálózata és az EU–CyCLONe által levont tanulságok alapján;

i) hozzájárulás Unió-szerte a kiberbiztonsági képességekhez a nemzeti tisztviselők cseréjének a tagállami illetékes hatóságok vagy a CSIRT-ek munkatársait bevonó kapacitásépítő program révén történő elősegítésével;

j) rendszeres közös találkozók szervezése az Unió egész területéről részt vevő érintett magánérdekeltekkel, hogy megvitassák a csoport által végzett tevékenységeket, és információkat gyűjtsenek a felmerülő szakpolitikai kihívásokkal kapcsolatban;

k) a kiberbiztonsági gyakorlatokkal kapcsolatos munka megvitatása, ideértve az ENISA által végzett munkát is;

ka) a szakértői tanulásra szolgáló mechanizmus létrehozása ezen irányelv 16. cikkével összhangban.

(5) Az együttműködési csoport kiválasztott témákról műszaki jelentést kérhet a CSIRT-ek hálózatától.

(6) Az együttműködési csoport ...-ig[24 hónappal ezen irányelv hatálybalépését követően], majd azt követően két évente munkaprogramot állít össze a céljai és feladatai végrehajtása érdekében megvalósítandó intézkedésekről. 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, amelyekben meghatározza az együttműködési csoport működéséhez szükséges eljárási szabályokat. Ezeket a végrehajtási jogi aktusokat a 37. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.
- (8) Az együttműködési csoport rendszeresen és évente legalább egy alkalommal ülésezik az (EU) XXXX/XXXX irányelv [a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv] alapján létrehozott, a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoporttal a stratégiai együttműködés előmozdítása és az információcsere **elősegítése** érdekében.

13. cikk

A CSIRT-ek hálózata

- (1) A tagállamok közötti bizalom erősítése, valamint a gyors és hatékony operatív együttműködésük előmozdítása érdekében létrejön a nemzeti CSIRT-ek hálózata.
- (2) A CSIRT-ek hálózata **a 9. cikkkel összhangban kijelölt** tagállami CSIRT-ek és a CERT–EU képviselőiből áll. A Bizottság megfigyelőként vesz részt a CSIRT-ek hálózatában. Az ENISA biztosítja a titkárságot, és aktívan támogatja a CSIRT-ek közötti együttműködést.
- (3) A CSIRT-ek hálózata a következő feladatokat látja el:
- a) a CSIRT-ek képességeivel kapcsolatos információk megosztása;
 - b) a biztonsági eseményekkel, a majdnem bekövetkezett (near miss) eseményekkel, a kiberfenyegetésekkel, a kockázatokkal és a sebezhetőségekkel kapcsolatos releváns információk megosztása;

- ba) a kiberbiztonsági kiadványokkal és ajánlásokkal kapcsolatos információk megosztása;
- bb) a biztonsági események műszaki kezelését megkönnyítő műszaki megoldások megosztása;
- bc) a CSIRT-ek feladataival kapcsolatos bevált gyakorlatok, eszközök és folyamatok cseréje;
- c) a CSIRT-ek hálózatának egy biztonsági esemény által potenciálisan érintett [...] **tagja** kérésére az adott biztonsági eseménnyel és a kapcsolódó kiberfenyegetésekkel, kockázatokkal és sebezhetőségekkel kapcsolatos információk megosztása és megvitatása;
- d) a CSIRT-ek hálózatának [...] **tagja** kérésére az adott tagállam joghatósága alá tartozó területen azonosított biztonsági esemény megvitatása és lehetőség szerint koordinált válaszadás a problémára;
- e) támogatás nyújtása a tagállamoknak a határokon átnyúló biztonsági események ezen irányelv szerinti kezeléséhez;
- f) együttműködés, **a bevált gyakorlatok cseréje** és segítségnyújtás a 6. cikkben említett kijelölt CSIRT-ek számára az [...] összehangolt sebezhetőség-feltárás kezeléséhez, ha a sebezhetőségek az IKT-termékek, IKT-szolgáltatások és IKT-folyamatok különböző tagállamokban letelepedett több gyártóját, illetve szolgáltatóját érintik;
- g) az operatív együttműködés további formáinak megvitatása és meghatározása, amelyek többek között az alábbiakkal kapcsolatosak:
 - i. a kiberfenyegetések és a biztonsági események kategóriái;
 - ii. korai előrejelzés;
 - iii. kölcsönös segítségnyújtás;

- iv. a koordináció elvei és módjai olyan esetekben, amikor határokon átnyúló kockázatokra és biztonsági eseményekre kell reagálni;
- v. **tagállami kérésre** hozzájárulás a 7. cikk (3) bekezdésében említett nemzeti kiberbiztonsági esemény- és válságelhárítási tervhez;
- h) az együttműködési csoport tájékoztatása a tevékenységeiről és az operatív együttműködésnek a g) pont szerint megvitatott további formáiról, és adott esetben iránymutatás kérése az operatív együttműködésre nézve;
- 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-ok) annak érdekében, hogy az egész Unióban javuljon a biztonsági eseményekkel és fenyegetésekkel kapcsolatos közös helyzetismeret;
- l) a szakértői [...] **tanulásról** készült, a 16. cikk (7) bekezdésében említett jelentések megvitatása;
- m) iránymutatások kibocsátása annak érdekében, hogy az e cikk operatív együttműködésre vonatkozó rendelkezéseinek alkalmazása tekintetében elősegítse az operatív gyakorlatok közelítését.

- (4) A CSIRT-ek hálózata a 35. cikkben említett felülvizsgálat céljából és ...-ig[□24 hónappal ezen irányelv hatálybalépését követően□], majd azt követően kétévente értékeli az operatív együttműködés terén elért előrehaladást, és jelentést készít. A jelentésben különösen a 16. cikkben említett, a nemzeti CSIRT-ekkel kapcsolatban végzett szakértői **tanulás** [...] eredményeire vonatkozóan kell következtetéseket levonni, beleértve az e cikknek megfelelően megfogalmazott következtetéseket és ajánlásokat is. Ezt a jelentést az együttműködési csoportnak is be kell nyújtani.
- (5) A CSIRT-ek hálózata elfogadja saját eljárási szabályzatát.
- (6) **A CSIRT-ek hálózata egyeztetett eljárási szabályok alapján együttműködik az EU-CyCLONE hálózattal.**

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 létrejön az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (EU-CyCLONE).
- (2) Az EU-CyCLONE a tagállamok **kiberválságok** kezelésével foglalkozó hatóságainak a 7. cikkel összhangban kijelölt képviselőiből [...] áll. **A Bizottság megfigyelőként vesz részt a hálózat tevékenységeiben.** Az ENISA biztosítja a hálózat titkárságát, támogatja a biztonságos információcserét, **valamint szolgáltatja a tagállamok közötti együttműködés támogatásához szükséges eszközöket, ezáltal biztosítva a biztonságos információcserét.**

Az EU-CyCLONE adott esetben az érdekelt felek képviselőit is felkérheti, hogy vegyenek részt a munkájában.

- (3) Az EU-CyCLONe a következő feladatokat látja el:
- a) a nagyszabású **kiberbiztonsági** [...] események és válságok kezelésére való felkészültség szintjének növelése;
 - b) a [...] nagyszabású **kiberbiztonsági** eseményekkel és válságokkal kapcsolatos [...] közös helyzetismeret kifejlesztése;
 - ba) a releváns nagyszabású kiberbiztonsági események következményeinek és hatásának értékelése, valamint javaslattétel lehetséges mérséklési intézkedésekre;**
 - c) a nagyszabású kiberbiztonsági események és válságok **kezelésének** koordinálása [...], valamint az említett eseményekkel és válságokkal kapcsolatos szakpolitikai szintű döntéshozatal támogatása;
 - d) **tagállami kérésre** a 7. cikk (3[...]) bekezdésében említett nemzeti kiberbiztonsági esemény- és **válságelhárítási tervének** megvitatása;[...]
- (4) Az EU-CyCLONe elfogadja eljárási szabályzatát.
- (5) Az EU-CyCLONe rendszeresen jelentést tesz az együttműködési csoportnak **a nagyszabású kiberbiztonsági események kezelésével és a válságkezeléssel** [...] kapcsolatban, különös tekintettel az alapvető és fontos szervezetekre gyakorolt hatásukra.
- (6) Az EU-CyCLONe egyeztetett eljárási szabályok alapján együttműködik a CSIRT-ek hálózatával.
- (7) **Az EU-CyCLONe [24 hónappal ezen irányelv hatálybalépését követően]-ig jelentést nyújt be az Európai Parlamentnek és a Tanácsnak, amelyben értékeli a munkáját.**

14a. cikk

Nemzetközi együttműködés

Az Unió az EUMSZ 218. cikkével összhangban adott esetben nemzetközi megállapodásokat köthet harmadik országokkal vagy nemzetközi szervezetekkel, ezáltal lehetővé téve és megszervezve az együttműködési csoport, a CSIRT-ek hálózata és az EU-CyCLONe egyes tevékenységeiben való, az uniós adatvédelmi jogszabályoknak megfelelő részvételüket.

15. cikk

Jelentés az uniós kiberbiztonsági helyzetről

- (1) Az ENISA a Bizottsággal **és az együttműködési csoporttal** együttműködve két évente jelentést ad ki az uniós kiberbiztonsági helyzetről. A jelentésnek **különösen a [...]** következőket [...] kell [...] tartalmaznia:
- aa) uniós szintű kiberbiztonsági kockázatértékelés, amely figyelembe veszi a fenyegetettségi helyzetet;**
 - a) a köz- és a magánszektor**beli** kiberbiztonsági képességek egész Unióban megvalósított fejlesztésének az **értékelése** [...];
 - b) [...]
 - c) kiberbiztonsági [...] **menyiségi és minőségi mutatókon alapuló összesített értékelés,** amely [...] **áttekintést** nyújt a kiberbiztonsági képességek, **köztük az ágazatspecifikus képességek** kiforrottságának szintjéről.

- (2) A jelentésnek magában kell foglalnia a kiberbiztonság szintjének az Unió egész területén történő növelésére vonatkozó konkrét szakpolitikai ajánlásokat, valamint az ENISA által az (EU) 2019/881 rendelet 7. cikkének (6) bekezdésével összhangban kiadott uniós kiberbiztonsági technikai helyzetjelentésekkel kapcsolatos, az Ügynökség adott időszakra vonatkozó megállapításainak összefoglalását.

16. cikk

Szakértői tanulás

- (1) **A kölcsönös bizalom erősítése, a kiberbiztonság egységesen magas szintjének elérése, valamint az ezen irányelv hatékony végrehajtásához szükséges tagállami kiberbiztonsági képességek és politikák megerősítése céljából a[...]-z együttműködési csoport [...] – a Bizottság támogatásával és [...] az ENISA-val, illetve adott esetben a CSIRT-ek hálózatával folytatott konzultációt követően – legkésőbb 24 [...] hónappal ezen irányelv hatálybalépését követően meghatározza az ezen irányelv tagállamok [...] általi végrehajtására vonatkozó, szakértői [...] tanulásra szolgáló objektív, megkülönböztetéstől mentes és méltányos rendszer [...] módszertanát [...]. A szakértői tanulásban való részvétel önkéntes. A rendszer a [...] tagállamokból érkező kiberbiztonsági [...] szakértők által [...] vezetett értékelési fordulókból áll, és a következő szempontok közül egyet vagy többet [...] vizsgál:**
- i. a 18. cikkben említett kiberbiztonsági kockázatkezelési követelmények és a 20. cikkben említett bejelentési kötelezettségek végrehajtása [...];
 - ii. a képességek [...], beleértve a rendelkezésre álló [...] erőforrásokat, valamint a 8. cikkben említett illetékes nemzeti hatóságok és a 9. cikkben említett CSIRT-ek feladatainak ellátását [...];

[...]

iii.[...] a 34. cikkben említett kölcsönös segítségnyújtás [...] **végrehajtása**;

iv. a [...] 26. cikkben említett információmegosztási keret [...] **végrehajtása**.

- (2) **A kritériumoknak, amelyek alapján a tagállamok kijelölik a szakértői tanulás fordulóiban való részvételre jogosult szakértőket, [...] objektívnek, megkülönböztetéstől mentesnek, méltányosnak és átláthatónak kell lenniük [...], és az (1) bekezdésben említett módszertan részét kell képezniük. Az ENISA és a Bizottság szakértőket jelölhet [...] ki, hogy megfigyelőként vegyenek részt a [...] szakértői tanulás fordulóiban. [...]**
- (3) [...] .

- (3a) **A szakértői tanulás fordulójának megkezdése előtt a tagállamok önértékelést végezhetnek a szakértői tanulás adott fordulójában vizsgált szempontok alapján, és az önértékelés eredményét eljuttathatják a (2) bekezdésben említett kijelölt szakértőkhöz.**
- (4) A szakértői [...] **tanulás személyes** [...] vagy virtuális helyszíni látogatásokkal és helyszínen kívüli találkozókkal is [...] együttjárhat. A jó együttműködés elvére tekintettel a **szakértői tanulásban részt vevő** [...] tagállamok – **a bizalmas vagy minősített adatok védelmét szolgáló nemzeti vagy uniós jogszabályok sérelme nélkül, illetve az alapvető állami funkciók, például a nemzetbiztonság védelmének sérelme nélkül** – a kijelölt szakértőknek megadják az értékeléshez [...] szükséges [...] információkat. A szakértői [...] **tanulás** során kapott információkat kizárólag erre a célra szabad felhasználni. A szakértői [...] **tanulásban** részt vevő szakértők semmilyen, [...] **azzal összefüggésben** kapott érzékeny vagy bizalmas információt nem közölhetnek harmadik személyekkel. **A szakértői tanulásban részt vevő tagállam az együttműködési csoporttal közölt, kellően alátámasztott indokok alapján kifogást emelhet egyes szakértők kijelölésével szemben.**

- (5) A [...] **részt vevő tagállamok esetében** [...] a szakértői [...] **tanulás adott fordulójának** [...] lezárását követő [...] **négy** éven belül ugyanazokat a szempontokat nem lehet a szakértői [...] **tanulás további fordulójának** alávetni [...], **kivéve, ha az érintett tagállam kéri ezt, vagy ha az együttműködési csoport [...] javaslatára hozzájárul ehhez.**
- (6) [...]
- (7) A szakértői [...] **tanulás fordulóiban** részt vevő szakértők jelentéstervezeteket készítenek az [...] **értékelések** keretében megfogalmazott megállapításokról és következtetésekről. **A tagállamok számára lehetővé kell tenni, hogy a rájuk vonatkozó jelentéstervezetekkel kapcsolatban észrevételeket tegyenek, amelyeket csatolni kell az adott jelentéshez. A zárójelentéseket be kell nyújtani az [...] együttműködési csoportnak. [...] A tagállamok dönthetnek úgy, hogy a rájuk vonatkozó jelentéseket nyilvánosan hozzáférhetővé teszik.**

IV. FEJEZET

Kiberbiztonsági kockázatkezelési és bejelentési kötelezettségek

I. SZAKASZ

Kiberbiztonsági kockázatkezelés és bejelentés

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, [...] **felügyeljék** annak végrehajtását és [...] **elszámoltathatók** legyenek az e cikk szerinti kötelezettségeknek a szervezetek általi be nem tartásáért.

E bekezdés alkalmazása nem érinti a tagállamok azon nemzeti jogszabályait, amelyek a közintézményekben alkalmazandó, valamint a köztisztviselők és a megválasztott és kinevezett tisztviselők jogi felelősségét szabályozzák.

- (2) A tagállamok biztosítják, hogy **a vezető testület tagjainak** rendszeresen [...] képzéseken **kelljen részt venniük** a kiberbiztonsági kockázatok és irányítási gyakorlatok, valamint azoknak a szervezet működésére gyakorolt hatása megismeréséhez és értékeléséhez elegendő ismeretek és készségek elsajátítása érdekében.

Kiberbiztonsági kockázatkezelési intézkedések

- (1a) Ez az irányelv egy „minden veszélyre kiterjedő” megközelítést alkalmaz, amely kiterjed a hálózati és információs rendszereknek és azok fizikai környezetének minden olyan eseménytől való védelmére, amely veszélyeztetheti a tárolt, továbbított vagy kezelt adatok vagy a hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát.
- (1) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek megfelelő és arányos technikai és szervezési intézkedéseket hozzanak annak a hálózat[...]**nak, illetve** információs rendszereknek a biztonságát veszélyeztető kockázatok kezelésére, amelyeket e szervezetek a szolgáltatásaik nyújtása során használnak. Figyelembe véve a technika állását és a **megvalósítás költségét**, ezeknek az intézkedéseknek biztosítaniuk kell a hálózati és információs rendszereknek a fennálló kockázat viszonylatában megfelelő biztonsági szintjét. **Az említett intézkedések arányosságának értékelésekor kellően figyelembe kell venni a szervezet kockázatnak való kitettsége mértékét, a szervezet méretét, a biztonsági események bekövetkezésének valószínűségét és azok súlyosságát. Figyelembe véve az alapvető vagy fontos szervezeteket érintő biztonsági események által a társadalomra jelentett kockázat szintjét és típusát, a fontos szervezetek számára előírt kiberbiztonsági kockázatkezelési intézkedések lehetnek kevésbé szigorúak, mint az alapvető szervezetek számára előírtak.**

- (2) Az (1) bekezdésben említett intézkedéseknek legalább a következőket magukban kell foglalniuk:
- a) kockázatelemzés és az informatikai rendszerek biztonságára vonatkozó politika;
 - b) a biztonsági események kezelése (megelőzés, felderítés [...] elhárítás és a biztonsági eseményt **követő helyreállítás**);
 - c) üzletmenet-folytonosság és válságkezelés;
 - d) az ellátási lánc biztonsága, ideértve az egyes szervezetek és **közvetlen** beszállítóik vagy szolgáltatóik, például az adattárolási és -feldolgozási szolgáltatásokat vagy felügyelt biztonsági szolgáltatásokat nyújtó szolgáltatók közötti kapcsolatok biztonságával kapcsolatos szempontokat;
 - e) biztonság a hálózati és információs rendszerek beszerzésében, fejlesztésében és karbantartásában, beleértve a sebezhetőségek kezelését és feltárását;
 - f) politikák és eljárások [...] a kiberbiztonsági kockázatkezelési intézkedések hatékonyságának értékelésére;
 - g) a kriptográfia és a titkosítás használatára **vonatkozó politika**;
 - ga) humánerőforrás-biztonság, hozzáférés-ellenőrzési politikák és eszközgazdálkodás.**
- (3) A tagállamok biztosítják, hogy a (2) bekezdés d) pontjában említett megfelelő intézkedések mérlegelésekor a szervezetek **kötelesek legyenek** figyelembe [...] **venni** az egyes **közvetlen** beszállítókra és szolgáltatókra jellemző sebezhetőségeket, valamint a beszállítóik és szolgáltatóik termékeinek és kiberbiztonsági gyakorlatainak – többek között biztonságos fejlesztési eljárásaiknak – az általános minőségét. **A tagállamok biztosítják továbbá, hogy a (2) bekezdés d) pontjában említett megfelelő intézkedések mérlegelésekor a szervezetek kötelesek legyenek figyelembe venni a 19. cikk (1) bekezdésének megfelelően elvégzett koordinált kockázatértékelések eredményeit.**

- (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 megfelelésének biztosítása érdekében.
- (5) A Bizottság végrehajtási jogi aktusokat fogadhat el az **e cikk** (2) bekezdésében említett elemek műszaki és módszertani előírásainak, **valamint – amennyiben szükséges – az ágazati sajátosságoknak a meghatározása érdekében. A Bizottság [18 hónappal ezen irányelv hatálybalépését követően]-ig végrehajtási jogi aktusokat fogad el a 24. cikk (1) bekezdésében említett szervezetekre és az I. melléklet 8. pontjában említett bizalmi szolgáltatókra vonatkozó műszaki és módszertani előírások megállapítása érdekében. Ezeket a végrehajtási jogi aktusokat a 37. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni. E végrehajtási jogi aktusok előkészítése során a Bizottság [...] a lehető legnagyobb mértékben követi a nemzetközi és európai szabványokat, valamint a vonatkozó műszaki előírásokat, és a 12. cikk (4) bekezdésének d) pontjában foglaltak szerint tanácsot kér az együttműködési csoporttól és az ENISA-tól a végrehajtási jogi aktus tervezetével kapcsolatban.**
- (6) [...]

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 konkrét kritikus IKT-szolgáltatásokat, -rendszereket vagy -termékeket, amelyekre az (1) bekezdésben említett összehangolt kockázatértékelés vonatkozhat.

20. cikk

Bejelentési 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 biztonsági eseményről, amely jelentős hatással van szolgáltatásaik nyújtására. Adott esetben ezek a szervezetek indokolatlan késedelem nélkül értesítik a szolgáltatásaikat igénybe vevőket **ezen** biztonsági 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 a biztonsági esemény lehetséges határokon átnyúló hatásait. **Pusztán a bejelentés ténye következtében a bejelentő szervezetet többletfelelősség nem terhelheti.**

- (2) [...]

Adott esetben [...] az **alapvető és a fontos** szervezetek indokolatlan késedelem nélkül értesítik a jelentős kiberfenyegetés által potenciálisan érintett szolgáltatásaik igénybe vevőit azokról az intézkedésekről, illetve jogorvoslati lehetőségekről, amelyeket a szolgáltatások igénybe vevői a fenyegetésre válaszul maguk megtehetnek, illetve amelyekkel élhetnek. Adott esetben a szervezetek a szolgáltatások igénybe vevőket magáról a fenyegetésről is értesítik. **Pusztán a bejelentés ténye** következtében a bejelentő szervezetet többletfelelősség nem terhelheti.

- (3) A biztonsági esemény akkor tekintendő jelentősnek, ha:
- a) a biztonsági esemény **a szolgáltatásban súlyos**[...] működési zavart okoz vagy potenciálisan okozhat, vagy az érintett szervezet számára pénzügyi veszteséget okoz vagy potenciálisan okozhat;
 - b) a biztonsági esemény jelentős vagyoni vagy nem vagyoni kár okozása révén más természetes vagy jogi személyeket érint vagy potenciálisan érinthet.
- (4) A tagállamok biztosítják, hogy az (1) bekezdés szerinti bejelentés céljából az érintett szervezetek benyújtásuk az illetékes hatóságoknak vagy a CSIRT-nek a következőket:
- a) indokolatlan késedelem nélkül, de legkésőbb az attól számított 24 órán belül, hogy a biztonsági esemény a tudomásukra jutott, egy első bejelentést **mint korai előrejelzést**, amelyben adott esetben fel kell tüntetni, hogy a biztonsági eseményt vélhetően jogellenes vagy rossz szándékú cselekmény okozta-e;
 - b) valamely illetékes hatóság vagy a CSIRT kérésére közbenső jelentést a helyzet aktuális alakulásáról;
 - c) **zárójelentést**, legkésőbb az a) pont szerinti [...] **első bejelentés** benyújtását követő egy hónapon belül, amely tartalmazza legalább a következőket:
 - i. a biztonsági eseménynek, súlyosságának és hatásának részletes leírása;
 - ii. a biztonsági eseményt valószínűleg kiváltó fenyegetés típusa vagy valószínű kiváltó oka;
 - iii. az alkalmazott és folyamatban lévő mérséklési intézkedések.

A tagállamok előírják, hogy kellően indokolt esetekben, az illetékes hatóságokkal vagy a CSIRT-tel egyetértésben az érintett szervezet eltérhet az a) és c) pontban meghatározott határidőktől. **Különösen, a c) pontban említett határidőtől való eltérés indokoltnak tekinthető, ha a biztonsági esemény még folyamatban van.**

- (5) Az illetékes nemzeti hatóságok vagy a CSIRT a (4) bekezdés a) pontjában említett első bejelentés kézhezvételét [...] **követően indokolatlan késedelem nélkül** választ ad a bejelentő szervezetnek, ideértve az eseményre vonatkozó első visszajelzést és – a szervezet kérésére – a lehetséges mérséklési intézkedések végrehajtására vonatkozó útmutatást. 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 a biztonsági eseménnyel kapcsolatban bűncselekmény gyanúja merül fel, az illetékes nemzeti hatóságok vagy a CSIRT útmutatást ad a biztonsági esemény bűnüldöző hatóságoknak történő bejelentésére vonatkozóan is.
- (6) Adott esetben, és különösen, ha az (1) bekezdésben említett biztonsági esemény két vagy több tagállamot érint, az illetékes hatóság, a CSIRT vagy **az egyedüli kapcsolattartó pont** tájékoztatja a biztonsági eseményről a többi érintett tagállamot és az ENISA-t. **E tájékoztatásnak legalább az e cikk (4) bekezdésében előírt elemeket tartalmaznia kell.** Ennek során az illetékes hatóságoknak, a CSIRT-eknek és az egyedüli kapcsolattartó pontoknak az uniós joggal vagy az uniós jognak megfelelő nemzeti jogszabályokkal összhangban óvniuk kell a szervezet biztonsági és kereskedelmi érdekeit, valamint a nyújtott információk bizalmas jellegét.
- (7) Ha egy biztonsági esemény megelőzéséhez vagy egy folyamatban lévő biztonsági esemény kezeléséhez lakossági tudatosítás szükséges, vagy ha a biztonsági esemény nyilvánosságra hozatala egyéb okból közérdek, az illetékes hatóság vagy a CSIRT, és adott esetben a többi érintett tagállam hatóságai vagy CSIRT-jei az érintett szervezettel folytatott konzultációt követően tájékoztathatják a nyilvánosságot a biztonsági eseményről, vagy ezt megkövetelhetik a szervezettől.

- (8) Az illetékes hatóság vagy a CSIRT kérésére az egyedüli kapcsolattartó pont az (1) [...] bekezdés alapján kapott bejelentéseket továbbítja a többi érintett tagállam egyedüli kapcsolattartó pontjának.
- (9) Az egyedüli kapcsolattartó pont [...] **félévente** összefoglaló jelentést nyújt be az ENISA-nak, amely anonimizált és összesített adatokat tartalmaz az (1) [...] bekezdéssel, valamint a 27. cikkel összhangban bejelentett biztonsági 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. **Az ENISA félévente tájékoztatja az együttműködési csoportot és a CSIRT-ek hálózatát a beérkezett bejelentésekről tett megállapításairól.**
- (10) Az illetékes hatóságok információt nyújtanak az (EU) XXXX/XXXX irányelv (a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv) alapján kijelölt illetékes hatóságoknak az (EU) XXXX/XXXX irányelv (a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv) alapján kritikus fontosságú szervezetként [vagy kritikus fontosságú szervezetekkel egyenértékű szervezetként] azonosított alapvető szervezetek által az (1) és (2) bekezdéssel összhangban bejelentett biztonsági eseményekről és kiberfenyegetésekről.
- (11) A Bizottság végrehajtási jogi aktusokat fogadhat el az (1) és (2) bekezdés alapján benyújtott bejelentésben feltüntetendő információ típusának, a bejelentés formátumának és a bejelentési eljárásnak a részletesebb meghatározása érdekében. A Bizottság végrehajtási jogi aktusokat fogadhat el továbbá azzal a céllal is, hogy részletesebben meghatározza azokat az eseteket, amikor egy biztonsági eseményt a (3) bekezdésben említettek szerint jelentősnek kell tekinteni. Ezeket a végrehajtási jogi aktusokat a 37. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

Az európai kiberbiztonsági tanúsítási rendszerek használata

- (1) A 18. cikk egyes követelményeinek való megfelelés igazolása érdekében **a tagállamok megkövetelhetik a szervezetektől, hogy [...] olyan meghatározott IKT-termékeket, [...]-szolgáltatásokat és [...]-folyamatokat használjanak, amelyeket az (EU) 2019/881 rendelet 49. cikke alapján elfogadott európai kiberbiztonsági tanúsítási rendszerek keretében tanúsítottak.** A tanúsítás tárgyát képező IKT-termékeket, -szolgáltatásokat és -folyamatokat fejlesztheti alapvető vagy fontos szervezet, vagy azok beszerezhetőik harmadik felektől.
- (2) A Bizottság [...] **végrehajtási [...]** jogi aktusokat fogadhat el annak meghatározása érdekében, hogy az alapvető **vagy fontos** szervezetek mely kategóriái kötelesek **bizonyos tanúsított IKT-termékeket, - szolgáltatásokat és -folyamatokat használni vagy** tanúsítványt szerezni, **az (EU) 2019/881 rendelet 49. cikke szerint elfogadott [...]** mely [...] európai kiberbiztonsági tanúsítási rendszerek alapján. [...] **Ezeket a végrehajtási jogi aktusokat a 37. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni. E végrehajtási jogi aktusok előkészítése során a Bizottság az (EU) 2019/881 rendelet 56. cikkével összhangban:**
- i. **figyelembe veszi az intézkedéseknek az ilyen IKT-termékek, -szolgáltatások vagy - folyamatok gyártóira, illetve szolgáltatóira és a felhasználókra gyakorolt hatását ezen intézkedések költségei, valamint a megcélzott IKT-termékek, -szolgáltatások vagy -folyamatok várható magasabb biztonsági szintjéből eredő társadalmi vagy gazdasági előnyök tekintetében, továbbá ezek alternatív piaci elérhetőségét;**
 - ii. **nyílt, átlátható és inkluzív konzultációt folytat valamennyi releváns érdekelt féllel és tagállammal;**

iii. **figyelembe veszi a végrehajtási határidőket, az átmeneti intézkedéseket és időszakokat, tekintettel különösen az intézkedéseknek az IKT-termékek, -szolgáltatások vagy -folyamatok gyártóira, illetve szolgáltatóira és mindezek felhasználóira – többek között a kkv-kra – gyakorolt lehetséges hatására;**

iv. **figyelembe veszi a vonatkozó tagállami jogszabályok meglétét és végrehajtását.**

- (3) A Bizottság felkérheti az ENISA-t, hogy készítsen egy javasolt tanúsítási rendszert, **vagy végezze el egy meglévő,** az (EU) 2019/881 rendelet 48. cikkének (2) bekezdése szerinti **kiberbiztonsági tanúsítási rendszer felülvizsgálatát** azokban az esetekben, amikor **e cikk** (2) bekezdése alkalmazásában nem áll rendelkezésre 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 területekre, valamint a már meglévő olyan szabványokra vonatkozóan – beleértve a tagállamok nemzeti szabványait is – amelyek lehetővé tennék e területek lefedését.

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 kapcsolódó doménnév-regisztrációs szolgáltatásokat nyújtó szervezetek a személyes adatnak minősülő adatok tekintetében az uniós adatvédelmi jogszabályoknak **megfelelően** a 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, **többek között legalább az alábbi adatokat:**
 - a) **doménnév;**
 - b) **a nyilvántartásba vétel időpontja;**
 - c) **a bejegyzést igénylő adatai, ezen belül:**
 - i. **egyének esetében: utónév, vezetéknév és e-mail-cím,**
 - ii. **jogi személyek esetében: név és e-mail-cím.**

- (3) A tagállamok biztosítják, hogy a legfelső szintű doménnév-nyilvántartók és a TLD-hez kapcsolódó doménnév-regisztrációs szolgáltatásokat nyújtó szervezetek rendelkezzenek az annak biztosítására szolgáló politikákkal és eljárásokkal, hogy az adatbázisok pontos és teljes információkat tartalmazzanak. A tagállamok biztosítják, hogy az említett politikákat és eljárásokat nyilvánosan hozzáférhetővé tegyék.
- (4) A tagállamok biztosítják, hogy a legfelső szintű doménnév-nyilvántartók és a TLD-hez kapcsolódó doménnév-regisztrációs 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 kapcsolódó doménnév-regisztrációs szolgáltatásokat nyújtó szervezetek – jogszerű és kellően indokolt kérésre – 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 kapcsolódó doménnév-regisztrációs szolgáltatásokat nyújtó szervezetek indokolatlan késedelem nélkül, **de legkésőbb 72 órán belül** megválaszoljanak minden hozzáférési kérelmet. A tagállamok biztosítják, hogy az említett adatok közzétételére vonatkozó politikákat és eljárásokat nyilvánosan hozzáférhetővé tegyék.

II. szakasz

Joghatóság és nyilvántartás

24. cikk

Joghatóság és területi elv

- (1a) Az ezen irányelv hatálya alá tartozó szervezeteket annak a tagállamnak a joghatósága alá tartozónak kell tekinteni, ahol a szolgáltatásaikat nyújtják. Az ezen irányelv I. mellékletének 1–7. és 10. pontjában említett szervezeteket, valamint I. mellékletének 8. pontjában és II. mellékletének 1–5. pontjában említett bizalmi szolgáltatókat és internetes exchange pont szolgáltatókat a letelepedésük helye szerinti tagállam joghatósága alá tartozónak kell tekinteni.
- (1) A DNS-szolgáltatókat, a legfelső szintű doménnév-nyilvántartókat [...] és a TLD-hez kapcsolódó doménnév-regisztrációs szolgáltatásokat nyújtó szervezeteket, a felhőszolgáltatókat, az adatközpont-szolgáltatókat [...], az I. melléklet 8. és 8a. pontjában említett tartalomszolgáltató hálózati szolgáltatókat, **felügyelt szolgáltatókat és felügyelt biztonsági 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 **túlnyomórészt** meghozzák. Ha **nem lehet meghatározni azt a helyet, ahol túlnyomórészt meghozzák az ilyen döntéseket, vagy ha** az Unióban található egyetlen telephelyen sem hoznak ilyen döntéseket, úgy kell tekinteni, hogy az üzleti tevékenység fő helye abban a tagállamban van, ahol a szervezetnek a legmagasabb munkavállalói létszámú telephelye található az Unióban. **Ha a szolgáltatásokat vállalkozáscsoport nyújtja, a vállalkozáscsoport üzleti tevékenységének fő helyét kell az üzleti tevékenység fő helyének tekinteni.**

- (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.
- (4a) Amennyiben egy tagállamhoz kölcsönös segítségnyújtás iránti megkeresés érkezik az (1) bekezdésben említett szervezetekkel kapcsolatban, a megkeresés keretein belül felügyeleti és végrehajtási intézkedéseket hozhat azon érintett szervezettel kapcsolatban, amely a területén szolgáltatást nyújt vagy amelynek a hálózati és információs rendszere a területén található.**

25. cikk

Bizonyos digitálisinfrastruktúra-szervezetek és digitális szolgáltatók nyilvántartása

- (1) [...] **A tagállamok biztosítják, hogy a 24. cikk (1) bekezdésében említett azon szervezetek, amelyek üzleti tevékenységének fő helye a területükön található, vagy amennyiben nincsenek letelepedve az Unióban, az Unióban a kijelölt képviselőjük a területükön van letelepedve, kötelesek legyenek benyújtani a következő információkat [...] az illetékes hatóságoknak [legkésőbb az irányelv hatálybalépésétől számított 12 hónapon belül]-ig:**

- a) a szervezet neve;
- aa) a szervezet típusa ezen irányelv I. és II. melléklete szerint;**
- 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 és képviselőik e-mail-címét és telefonszámát;
- d) azok a tagállamok, ahol a szervezet a szolgáltatást nyújtja.**

Ezt az információt adott esetben a 2a. cikkben említett nemzeti önbejelentési mechanizmus[...] útján kell benyújtani.

- (2) **A tagállamok biztosítják, hogy az (1) bekezdésben említett szervezetek az (1) bekezdés alapján benyújtott adatokban bekövetkezett minden változást haladéktalanul, de legkésőbb a változás hatálybalépésétől számított három hónapon belül **szintén** bejelentsenek.**
- (3) [...] **A tagállamok egyedüli kapcsolattartó pontjai az (1) és (2) bekezdésben említett információkat [...] továbbítják [...] az ENISA-nak. [...]**

(3a) Az e cikk (3) bekezdésnek megfelelően kapott információk alapján az ENISA nyilvántartást hoz létre és gondoz az (1) bekezdésben említett szervezetekről. A tagállamok kérésére az ENISA lehetővé teszi az érintett illetékes hatóságok számára a nyilvántartáshoz való hozzáférést, biztosítva adott esetben az információk bizalmas jellegének védelméhez szükséges garanciákat.

(4) [...]

V. FEJEZET

Információmegosztás

26. cikk

Kiberbiztonsági információmegosztási megállapodások

- (1) [...] A tagállamok biztosítják, hogy az alapvető és a fontos szervezetek **önkéntes alapon** megoszthassák egymással a releváns kiberbiztonsági információkat, ideértve a kiberfenyegetésekre, **a majdnem bekövetkezett (near miss) eseményekre,** a sebezhetőségekre, a kompromisszummutatókra, a taktikákra, a technikákra és az eljárásokra, a kiberbiztonsági figyelmeztetésekre és a konfigurációs eszközökre vonatkozó információkat, amennyiben az említett információmegosztás:
- a) célja a biztonsági 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 sebezhetőség elhárítását és feltárását, a fenyegetésészlelési technikákat, a mérséklési stratégiákat vagy az elhárítási és helyreállítást szakaszt.
- (2) A tagállamok biztosítják, hogy az információmegosztás az alapvető és a fontos szervezetek [...] közösségein belül történjen. Az említett megosztást – a megosztott információk potenciálisan érzékeny jellegére figyelemmel – információmegosztási megállapodások útján kell végrehajtani.
- (3) A tagállamok meghatároz**hatnak olyan** [...] szabályokat, amelyek megállapítják a (2) bekezdésben említett információmegosztási megállapodások eljárását, működési elemeit (ideértve az e célra kijelölt IKT-platformok használatát), tartalmát és feltételeit. Az említett szabályok kiterjed**hetnek** [...] a hatóságok említett megállapodásokban való részvételének részleteire, valamint az operatív elemekre is, ideértve az e célra kijelölt 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 a 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 [...] ENISA bevált gyakorlatok megosztásával és útmutatás nyújtásával támogatja a (2) bekezdésben említett kiberbiztonsági információmegosztási megállapodások létrehozását.

A releváns információk önkéntes bejelentése

- (1) **A 20. cikk sérelme nélkül, a tagállamok biztosítják, hogy az alapvető és a fontos szervezetek önkéntes alapon bejelentést tehessenek az illetékes hatóságok vagy a CSIRT-ek számára minden releváns biztonsági eseményről, kiberfenyegetésről vagy majdnem bekövetkezett (near miss) eseményről.**
- (2) A tagállamok biztosítják, hogy a 3. cikk sérelme nélkül az ezen irányelv hatályán kívül eső szervezetek önkéntes alapon bejelentést nyújthassanak be jelentős biztonsági eseményekről, kiberfenyegetésekről vagy majdnem bekövetkezett (near miss) eseményekről. A bejelentések feldolgozása során a tagállamok a 20. cikkben megállapított eljárásnak megfelelően járnak el. A tagállamok előre sorolhatják a kötelező bejelentések feldolgozását az önkéntes bejelentésekkel szemben. **A bűncselekmények nyomozásának, felderítésének és a vádeljárás lefolytatásának sérelme nélkül, a[...]**z önkéntes adatszolgáltatás nem eredményezhet az adatszolgáltatóra nézve olyan további kötelezettségeket, amelyek nem vonatkoztak volna rá, ha nem nyújtja be a bejelentést.
- (3) **Az önkéntes bejelentéseket csak akkor kell feldolgozni, ha az nem jelent aránytalan vagy indokolatlan terhet az érintett tagállam számára.**

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., a 20. és a 23. cikkben meghatározott kötelezettségeknek való megfelelés biztosításához szükséges intézkedéseket. **A tagállamok engedélyezhetik az illetékes hatóságok számára, hogy a felügyeletet tekintsék prioritásnak, amelynek kockázatalapú megközelítésen kell nyugodnia.**
- (2) Az illetékes hatóságok szorosan együttműködnek az adatvédelmi hatóságokkal, az (EU) XXXX/XXXX irányelv (a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv) alapján kijelölt illetékes hatóságokkal, a 910/2014/EU rendelet alapján kijelölt felügyeleti szervekkel, valamint az ágazatspecifikus uniós jogszabályok alapján kijelölt egyéb illetékes hatóságokkal a kiberbiztonsági események kezelése során. [...]
- (3) **A nemzeti jogszabályi és intézményi keretek sérelme nélkül, a tagállamok biztosítják, hogy a közigazgatási szervek ezen irányelvnek való megfelelésének felügyelete és a meg nem felelés miatt kirótt potenciális szankciók végrehajtása során az illetékes hatóságok rendelkezzenek az ahhoz szükséges megfelelő hatáskörökkel, hogy a felügyelet hatálya alá vont szervezetekkel szemben működési szempontból függetlenül végezhessek el ezen feladataikat. A tagállamok a nemzeti keretekkel és jogrenddel összhangban határozhatnak megfelelő, arányos és hatékony felügyeleti és végrehajtási intézkedések foganatosításáról e szervezetekkel szemben.**

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 **kockázatalapú megközelítést alkalmazzanak és** hatáskörrel rendelkezzenek arra, hogy ezeknél a szervezeteknél elvégezzék **legalább az** alábbiakat:
 - a) helyszíni ellenőrzések és távoli ellenőrzés, ideértve a véletlenszerű ellenőrzéseket is;
 - b) rendszeres **biztonsági** ellenőrzések;
 - c) célzott biztonsági ellenőrzések, a kockázatértékelések vagy a kockázattal kapcsolatban rendelkezésre álló információk alapján;
 - d) objektív, megkülönböztetéstől mentes, méltányos és átlátható kockázatértékelési kritériumokon alapuló biztonsági vizsgálatok, **amennyiben technikai okokból ez szükséges, az érintett szervezet együttműködésével;**
 - e) a szervezet által elfogadott kiberbiztonsági intézkedések értékeléséhez szükséges tájékoztatás kérése, ideértve a dokumentált kiberbiztonsági politikákat [...];
 - 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.

- (2a) Az e cikk (2) bekezdésében előírt felügyeleti feladataik ellátása keretében az illetékes hatóságok kialakíthatnak olyan felügyeleti módszereket, amelyek lehetővé teszik e feladatok kockázatalapú megközelítés alapján történő rangsorolását.
- (3) A (2) bekezdés e)–g) pontja szerinti hatásköreik gyakorlása során az illetékes hatóságok közlik a megkeresés célját és pontosan meghatározzák a kért információkat.
- (4) A tagállamok biztosítják, hogy az illetékes hatóságok az alapvető szervezetekkel kapcsolatos végrehajtási hatásköreik gyakorlása során hatáskörrel rendelkezzenek **legalább** 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) az említett szervezetek kötelezése arra, hogy szüntessék meg az ebben az irányelvben meghatározott kötelezettségeknek meg nem felelő magatartást, és tartózkodjanak e magatartás ismételt elkövetésétől;
 - d) az említett szervezetek kötelezése arra, hogy kockázatkezelési intézkedéseiket és/vagy bejelentési kötelezettségeiket meghatározott módon és határidőn belül hozzák összhangba a 18. és 20. cikkben meghatározott kötelezettségekkel;
 - e) az említett szervezetek kötelezése arra, hogy azon természetes vagy jogi személy(ek)e)t, akiknek szolgáltatásokat nyújtanak vagy tevékenységeket végeznek, és amelyeket egy jelentős kiberfenyegetés potenciálisan érinthet, tájékoztassák **a fenyegetés jellegéről, valamint** minden lehetséges védelmi vagy helyreállítási intézkedésről, amelyet e természetes vagy jogi személy(ek) megtehetnek a fenyegetés elhárítására;
 - f) az említett szervezetek kötelezése arra, hogy észszerű határidőn belül hajtsák végre a biztonsági ellenőrzés eredményeként adott ajánlásokat;
 - g) [...]

- h) az említett szervezetek kötelezése arra, hogy az ezen irányelvben meghatározott kötelezettségek be nem tartásának szempontjait meghatározott módon hozzák nyilvánosságra, **amennyiben a nyilvánosságra hozatal nem vezet a szóban forgó szervezet szempontjából káros kitettséghez;**
 - i) [...]
 - j) a 31. cikk szerinti közigazgatási bírság kiszabása vagy annak indítványozása 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 kitűzni, amelyen belül kéri az alapvető szervezettől a hiányosságok orvoslásához vagy az említett hatóságok követelményeinek való megfeleléshez szükséges intézkedések megtételét. 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, **vagy a nemzeti jogszabályoknak megfelelően a bíróságok** erre való felkérése;
 - b) a szóban forgó alapvető szervezetben vezérigazgatói vagy jogi képviselői szintű vezetői feladatokat ellátó személyek – és a jogsértésért felelős bármely más természetes személy – ideiglenes eltiltása a vezetői funkció gyakorlásától az adott szervezetenél, vagy ennek indítványozása az illetékes szervektől vagy bíróságoktól a nemzeti jogszabályok szerint.

Ezeket a szankciókat csak addig kell alkalmazni, amíg a szervezet megteszi a szükséges intézkedéseket a hiányosságok orvoslására, vagy eleget tesz az illetékes hatóság azon követelményeinek, amelyek tekintetében az említett szankciókat alkalmazták.

Az e bekezdésben előírt szankciók nem alkalmazandók az ezen irányelv hatálya alá tartozó közigazgatási szervekre.

- (6) A tagállamok biztosítják, hogy minden alapvető szervezetért felelős vagy annak képviselőjében – képviseleti jogkörre, a nevében történő döntéshozatalra vagy az irányítás gyakorlására való jogosultság 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. **A közigazgatási szervek tekintetében ez a rendelkezés nem érinti a tagállamok azon jogszabályait, amelyek a köztisztviselők és a megválasztott és kinevezett tisztviselők jogi felelősségét szabályozzák.**
- (7) A (4) és (5) bekezdés szerinti végrehajtási intézkedések, illetve szankciók bármelyikének alkalmazása esetén az illetékes hatóságoknak tiszteletben kell tartaniuk a védelemhez való jogot, és figyelembe kell venniük a konkrét esetek körülményeit, és kellően figyelembe kell venniük legalább az alábbiakat:
- a) a jogsértés súlyossága és a megsértett rendelkezések fontossága. A jogsértések közül súlyosnak tekintendők az alábbiak: ismételt jogsértések, jelentős zavart okozó biztonsági események bejelentésének vagy elhárításának elmulasztása, a hiányosságok orvoslásának elmulasztása 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 vagy a 18. és 20. cikkben meghatározott követelményekkel vagy bejelentési kötelezettségekkel kapcsolatban.

- b) a jogsértés időtartama, ideértve az ismételt jogsértések elemét;
 - c) a ténylegesen okozott kár vagy felmerült veszteség, 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 határozataikat. Az említett döntések meghozatala előtt az illetékes hatóságok értesítik az érintett szervezeteket előzetes megállapításaikról, és észszerű időt biztosítanak az említett szervezetek számára észrevételeik benyújtására, **kivéve ha azonnali veszély áll fenn.**

- (9) A tagállamok biztosítják, hogy **az ezen irányelv szerinti** illetékes hatóságai tájékoztassák [...] **ugyanazon** tagállamnak az (EU) XXXX/XXXX irányelv [a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv] alapján kijelölt érintett illetékes hatóságait arról, amikor gyakorolják azon felügyeleti és végrehajtási hatásköreiket, amelyek célja az ezen irányelv szerinti kötelezettségek egy kritikus fontosságúként vagy az (EU) XXXX/XXXX irányelv [a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv] alapján [a kritikus szervezetekkel egyenértékű szervezetként] azonosított alapvető szervezet általi betartásának biztosítása. **Adott esetben** [...] az (EU) XXXX/XXXX irányelv [a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv] szerinti illetékes hatóságok [...] **felkérhetik az ezen irányelv szerinti** illetékes hatóságokat arra, hogy [...] gyakorolják felügyeleti és végrehajtási **hatáskörüket** [...] az ezen irányelv hatálya alá tartozó valamely olyan alapvető szervezettel **kapcsolatban**, amelyet **az (EU) XXXX/XXXX irányelv [a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv] szerint** egyúttal kritikus fontosságúként [vagy azzal egyenértékűként] azonosítottak.
- (10) A tagállamok biztosítják, hogy **az ezen irányelv szerinti** illetékes hatóságaik tájékoztassák az (EU) XXXX/XXXX rendelet [DORA] 29. cikkének (1) bekezdése szerinti felvigyázási fórumot arról, amikor gyakorolják azon felügyeleti és végrehajtási hatásköreiket, amelyek célja az ezen irányelv szerinti kötelezettségeknek az (EU) XXXX/XXXX rendelet [DORA] 28. cikke alapján harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóként kijelölt alapvető szervezet általi betartásának biztosítása.
- (10a) A tagállamok biztosítják, hogy **az ezen irányelv szerinti** illetékes hatóságaik tájékoztassák a 910/2014/EU rendelet alapján kijelölt érintett illetékes hatóságokat arról, amikor gyakorolják azon felügyeleti és végrehajtási hatásköreiket, amelyek célja az ezen irányelv szerinti kötelezettségeknek a 910/2014/EU rendelet szerinti bizalmi szolgáltatóként kijelölt szervezet általi betartásának biztosítása.

Felügyelet és végrehajtás fontos szervezetek esetében

- (1) Ha bizonyítékokat vagy jelzést **vagy információt** kapnak arról, hogy egy fontos szervezet **általólag** 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 **kockázatalapú megközelítést alkalmazzanak és** hatáskörrel rendelkezzenek arra, hogy ezeknél a szervezeteknél elvégezzék **legalább** az alábbiakat:
 - a) helyszíni ellenőrzés és utólagos távoli ellenőrzés;
 - b) célzott biztonsági ellenőrzések, a kockázatértékelések vagy a kockázattal kapcsolatban rendelkezésre álló információk alapján;
 - c) objektív, **megkülönböztetéstől mentes**, méltányos és átlátható kockázatértékelési kritériumokon alapuló biztonsági vizsgálatok, **amennyiben technikai okokból ez szükséges, az érintett szervezet együttműködésével;**
 - d) a kiberbiztonsági intézkedések utólagos értékeléséhez szükséges tájékoztatás kérése [...];
 - e) a felügyeleti feladatok ellátásához szükséges adatokhoz, dokumentumokhoz és/vagy információkhoz való hozzáférés iránti kérelmek;
 - ea) **a kiberbiztonsági politikák végrehajtására vonatkozó bizonyítékok, például a minősített ellenőr által végzett biztonsági ellenőrzések eredményei és az azokat alátámasztó vonatkozó bizonyítékok iránti kérelmek.**

- (2a) Az e cikk (2) bekezdésében előírt felügyeleti feladataik ellátása keretében az illetékes hatóságok kialakíthatnak olyan felügyeleti módszereket, amelyek lehetővé teszik e feladatok kockázatalapú megközelítés alapján történő rangsorolását.
- (3) A (2) bekezdés d)–**ea**) pontja szerinti hatásköreik gyakorlása során az illetékes hatóságok közlik a megkeresés célját és pontosan meghatározzák a kért információkat.
- (4) A tagállamok biztosítják, hogy az illetékes hatóságok a fontos szervezetekkel kapcsolatos végrehajtási hatásköreik gyakorlása során hatáskörrel rendelkezzenek **legalább** 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) az említett szervezetek kötelezése arra, hogy szüntessék meg az ebben az irányelvben meghatározott kötelezettségeknek meg nem felelő magatartást, és tartózkodjanak e magatartás ismételt elkövetésétől;
 - d) az említett szervezetek kötelezése arra, hogy kockázatkezelési intézkedéseiket vagy bejelentési kötelezettségeiket meghatározott módon és határidőn belül hozzák összhangba a 18. és 20. cikkben meghatározott kötelezettségekkel;
 - e) az említett szervezetek kötelezése arra, hogy azon természetes vagy jogi személy(ek)e)t, akiknek szolgáltatásokat nyújtanak vagy tevékenységeket végeznek, és amelyeket egy jelentős kiberfenyegetés potenciálisan érinthet, tájékoztassák **a fenyegetés jellegéről, valamint** minden lehetséges védelmi vagy helyreállítási intézkedésről, amelyet e természetes vagy jogi személy(ek) megtehetnek a fenyegetés elhárítására;
 - f) az említett szervezetek kötelezése arra, hogy észszerű határidőn belül hajtsák végre a biztonsági ellenőrzés eredményeként adott ajánlásokat;

- g) az említett szervezetek kötelezése arra, hogy az ezen irányelvben meghatározott kötelezettségek be nem tartásának szempontjait meghatározott módon hozzák nyilvánosságra, **amennyiben a nyilvánosságra hozatal nem vezet a szóban forgó szervezet szempontjából káros kitettséghez;**
 - h) [...]
 - i) a 31. cikk szerinti közigazgatási bírság kiszabása vagy annak indítványozása 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) A 29. cikk (6)–(8) bekezdését alkalmazni kell az e cikkben [...] a 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 a 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 kötelezettségeknek **az alapvető szervezetek általi** megsértését e cikk (2) és (3) bekezdésével összhangban legalább 4[...] 000 000 EUR, vagy **jogi személy esetében**, ha ez magasabb, azon vállalkozás globális éves forgalma teljes összege 2 %-ának megfelelő [...] összegű közigazgatási bírsággal sújtsák, amelyhez az előző pénzügyi évben az alapvető [...] szervezet tartozik.
- (4a) A tagállamok biztosítják, hogy a 18. vagy a 20. cikkben megállapított kötelezettségeknek a fontos szervezetek általi megsértését e cikk (2) és (3) bekezdésével összhangban legalább 2 000 000 EUR vagy, ha ez magasabb, azon vállalkozás globális éves forgalma teljes összege 1 %-ának megfelelő összegű közigazgatási bírsággal sújtsák, amelyhez az előző pénzügyi évben a 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 arra vonatkozó 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.

(6a) Ha a tagállam jogrendszere nem rendelkezik közigazgatási bíróságokról, a tagállamok biztosítják, hogy ez a cikk oly módon alkalmazható legyen, hogy a bíróságot az illetékes hatóság kezdeményezésére az illetékes nemzeti bíróság rója ki, gondoskodva eközben e jogorvoslatok hatékonyságáról és a hatóságok által kiszabott közigazgatási bíróságokéval megegyező hatásáról. A kiszabott bírágoknak minden esetben hatékonnak, arányosnak és visszatartó erejűnek kell lenniük. E tagállamok az e bekezdésnek megfelelően elfogadott jogszabályokról [...]ig, az ezt követően azokat módosító jogszabályokról, illetve az azokat érintő későbbi módosításokról pedig haladéktalanul értesítik a Bizottságot.

32. cikk

A személyes adatok megsértésével járó jogsértések

- (1) Ha az illetékes hatóságoknak **a felügyelet vagy a végrehajtás során a tudomásukra jut [...]**, hogy **az ezen irányelv 18. és 20. cikkében megállapított kötelezettségeknek egy alapvető vagy fontos szervezet általi megsértése személyes adatok megsértésével járhat** az (EU) 2016/679 rendelet 4. cikkének (12) bekezdésében meghatározottak szerint, amelyet az említett rendelet 33. cikke alapján be kell jelenteni, **indokolatlan késedelem nélkül [...]** tájékoztatniuk kell az említett rendelet 55. 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. cikke **(2) bekezdésének i. pontja** alapján gyakorolják hatásköreiket és közigazgatási bíróságot szabnak ki, az **ezen irányelv 8. cikkében említett** illetékes hatóságok nem szabhatnak ki közigazgatási bíróságot [...] ezen irányelv 31. cikkének [...] **ugyanazon cselekménnyel való** megsértése miatt. 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 meghoznak minden szükséges intézkedést ezek végrehajtására. Az előírt szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek 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 egynél több tagállamban nyújt szolgáltatásokat, vagy ha [...] **egy vagy több** tagállamban **nyújt szolgáltatásokat**, de hálózati és információs rendszerei egy vagy több másik tagállamban találhatóak, [...] **az érintett** tagállamok illetékes hatóságai, [...] szükség szerint együttműködnek és segítik egymást. Ez az együttműködés magában foglalja legalább a következőket:

- a) az egyik tagállamban felügyeleti vagy végrehajtási intézkedéseket alkalmazó illetékes hatóságok az egyedüli kapcsolattartó ponton keresztül tájékoztatják a többi érintett tagállam illetékes hatóságait és konzultálnak velük a megtett felügyeleti és végrehajtási intézkedésekről [...];
 - b) az illetékes hatóság felkérhet egy másik illetékes hatóságot [...]a felügyeleti vagy végrehajtási intézkedések megtételére;
 - c) az illetékes hatóság egy másik illetékes hatóságtól származó indokolt kérelem kézhezvétele után – **a rendelkezésére álló erőforrásokhoz mérten arányos módon** – segítséget nyújt a másik illetékes hatóság számára annak érdekében, hogy a [...] felügyeleti vagy végrehajtási intézkedéseket hatékonyan, eredményesen és következetesen lehessen végrehajtani Ez a kölcsönös segítségnyújtás kiterjedhet tájékoztatás kérésére és felügyeleti intézkedésekre, ideértve a helyszíni ellenőrzések, távoli ellenőrzés 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 [...] folytatott eszmecsere követően megállapítást nyer, hogy a hatóság nem illetékes a kért segítség nyújtására, **vagy nem rendelkezik az ahhoz szükséges erőforrásokkal**, vagy a kért segítségnyújtás nem arányos az illetékes hatóság által [...] végzett felügyeleti feladatokkal, **vagy a kérelem olyan információra irányul vagy olyan tevékenységeket foglal magában, ami ellentétes az adott tagállam nemzetbiztonságával vagy közbiztonságával vagy védelmével.**
- (2) Adott esetben és közös megegyezéssel különböző tagállamok illetékes hatóságai [...] közös felügyeleti intézkedéseket végezhetnek.

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 jelentésben 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 összefüggésben. [...] **A felülvizsgálat** céljából [...] a Bizottság figyelembe veszi [...] a CSIRT-ek hálózatának [...] az operatív szinten szerzett tapasztalatokról szóló jelentéseit. Az első jelentést ...-ig [54 hónappal ezen irányelv hatálybalépését követően] kell benyújtani.

36. cikk

[...]

[...]

[...]

37. cikk

A 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 bizottságnak írásbeli eljárás keretében kell véleményt nyilvánítania, az ilyen eljárást eredmény nélkül lezárják, amennyiben a véleménynyilvánításra megállapított határidőn belül a bizottság elnöke úgy határoz, vagy valamely bizottsági tag ezt kéri.

38. cikk

Átültetés

- (1) A tagállamok ...-ig [24 hónappal ezen irányelv hatálybalépését követően] elfogadják és kihadjatík azokat a törvényi, rendeleti és közigazgatási rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek megfeleljenek. Erről haladéktalanul tájékoztatják a Bizottságot. Ezeket az intézkedéseket ...-tól/-től [egy nappal az első albekezdésben említett időpontot követően] alkalmazzák.
- (2) Amikor a tagállamok elfogadják ezeket az intézkedéseket, azokban hivatkozni kell erre az irányelvre, vagy azokhoz hivatalos kihadjetésük alkalmával ilyen hivatkozást kell fűzni. A hivatkozás módját a tagállamok határozzák meg.

39. cikk

A 910/2014/EU rendelet módosítása

A 910/2014/EU rendeletben a 19. cikket ...-i hatállyal [ezen irányelv átültetési határideje] el kell hagyni.

40. cikk

Az (EU) 2018/1972 irányelv módosítása

Az (EU) 2018/1972 rendeletben a 40. és 41. cikket ...-i hatállyal [ezen irányelv átültetési határideje] el kell hagyni.

41. cikk

Hatályon kívül helyezés

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

Az (EU) 2016/1148 irányelvre történő hivatkozásokat erre az irányelvre való hivatkozásnak kell tekinteni és a II[...] mellékletben szereplő megfelelési táblázattal összhangban kell értelmezni.

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,

az Európai Parlament részéről
az elnök

a Tanács részéről
az elnök

I. MELLÉKLET

ÁGAZATOK, ALÁGAZATOK ÉS SZERVEZETTÍPUSOK

Ágazat	Álágazat	Szervezet típusa
1. Energia	a) Villamos energia	— Az (EU) 2019/944 irányelv 2. cikkének 57. pontjában említett villamosenergia-ipari vállalkozások, amelyek az említett irányelv ⁽³⁹⁾ 2. cikkének 12. pontjában említett „ellátás” funkciót látják el
		— Az (EU) 2019/944 irányelv 2. cikkének 29. pontjában említett elosztórendszer-üzemeltetők
		— Az (EU) 2019/944 irányelv 2. cikkének 35. pontjában említett átvitelirendszer-üzemeltetők
		— Az (EU) 2019/944 irányelv 2. cikkének 38. pontjában említett termelők
		— Az (EU) 2019/943 rendelet 2. cikkének 8. pontjában említett kijelölt villamosenergiapiac-üzemeltetők ⁽⁴⁰⁾
		— Az (EU) 2019/943 rendelet 2. cikkének 25. pontjában említett, az (EU) 2019/944 irányelv 2. cikkének 18., 20. és 59. pontjában említett összesítési, keresletoldali vagy energiatárolási szolgáltatásokat nyújtó villamosenergia-piaci

³⁹ Az Európai Parlament és a Tanács (EU) 2019/944 irányelve (2019. június 5.) a villamos energia belső piacára vonatkozó közös szabályokról és a 2012/27/EU irányelv módosításáról (HL L 158., 2019.6.14., 125. o.).

⁴⁰ Az Európai Parlament és a Tanács (EU) 2019/943 rendelete a villamos energia belső piacról (HL L 158., 2019.6.14., 54. o.).

		szereplők
	b) Távfűtés és -hűtés	— A megújuló energiaforrásokból előállított energia használatának előmozdításáról szóló (EU) 2018/2001 irányelv ⁽⁴¹⁾ 2. cikkének 19. pontjában említett távfűtés vagy távhűtés
	c) Olaj	— Az olajszállító csővezetékek üzemeltetői — Olajtermelő, finomító és kezelő létesítmények, tárolók üzemeltetői és szállításirendszer-üzemeltetők — A 2009/119/EK tanácsi irányelv ⁽⁴²⁾ 2. cikkének f) pontjában említett központi készletezőszervek
	d) Gáz	— A 2009/73/EK irányelv ⁽⁴³⁾ 2. cikkének 8. pontjában említett ellátó vállalkozások — A 2009/73/EK irányelv 2. cikkének 6. pontjában említett elosztórendszer-üzemeltetők — A 2009/73/EK irányelv 2. cikkének 4. pontjában említett szállításirendszer-üzemeltetők — A 2009/73/EK irányelv 2. cikkének 10. pontjában említett

⁴¹ Az Európai Parlament és a Tanács (EU) 2018/2001 irányelve (2018. december 11.) a megújuló energiaforrásokból előállított energia használatának előmozdításáról (HL L 328., 2018.12.21., 82. o.).

⁴² A Tanács 2009/119/EK irányelve (2009. szeptember 14.) a tagállamok minimális kőolaj- és/vagy kőolajtermék-készletezési kötelezettségéről (HL L 265., 2009.10.9., 9. o.).

⁴³ Az Európai Parlament és a Tanács 2009/73/EK irányelve (2009. július 13.) a földgáz belső piacára vonatkozó közös szabályokról és a 2003/55/EK irányelv hatályon kívül helyezéséről (HL L 211., 2009.8.14., 94. o.).

		tárolásrendszer-üzemeltetők
		— A 2009/73/EK irányelv 2. cikkének 12. pontjában említett LNG-létesítmények rendszerüzemeltetői
		— A 2009/73/EK irányelv 2. cikkének 1. pontjában meghatározott földgázipari vállalkozások
		— A földgázfinomító és -kezelő létesítmények üzemeltetői
	e) Hidrogén	A hidrogéntermelés, -tárolás és -szállítás üzemeltetői
2. Közlekedés	a) Légi	— A 300/2008/EK rendelet ⁽⁴⁴⁾ 3. cikkének 4. pontjában említett, kereskedelmi célra igénybe vett légi fuvarozók
		— A 2009/12/EK irányelv ⁽⁴⁵⁾ 2. cikkének 2. pontjában említett repülőtér-irányító szervezetek, az említett irányelv 2. cikkének 1. pontjában említett repülőterek, ideértve az 1315/2013/EU rendelet ⁽⁴⁶⁾ II. mellékletének 2. szakaszában említett törzshálózati repülőterek, valamint a repülőtereken található kiegészítő létesítményeket működtető szervezetek
		— Az 549/2004/EK rendelet ⁽⁴⁷⁾ 2. cikkének 1. pontjában említett légiforgalmi irányító (ATC)

⁴⁴ Az Európai Parlament és a Tanács 300/2008/EK rendelete (2008. március 11.) a polgári légi közlekedés védelmének közös szabályairól és a 2320/2002/EK rendelet hatályon kívül helyezéséről (HL L 97., 2008.4.9., 72. o.).

⁴⁵ Az Európai Parlament és a Tanács 2009/12/EK irányelve (2009. március 11.) a repülőtéri díjakról (HL L 70., 2009.3.14., 11. o.).

⁴⁶ Az Európai Parlament és a Tanács 1315/2013/EU rendelete (2013. december 11.) a transzeurópai közlekedési hálózat fejlesztésére vonatkozó uniós iránymutatásokról és a 661/2010/EU határozat hatályon kívül helyezéséről (HL L 348., 2013.12.20., 1. o.).

⁴⁷ Az Európai Parlament és a Tanács 549/2004/EK rendelete (2004. március 10.) az egységes európai égbolt létrehozására vonatkozó keret megállapításáról (keretrendelet) (HL L 96., 2004.3.31., 1. o.).

		szolgáltatok
	b) Vasúti	— A 2012/34/EU irányelv ⁽⁴⁸⁾ 3. cikkének 2. pontjában említett pályahálózat-működtetők — A 2012/34/EU irányelv 3. cikkének 1. pontjában említett vállalkozó vasúti társaságok, beleértve a 2012/34/EU irányelv 3. cikkének 12. pontjában említett kiszolgáló létesítmények üzemeltetőit
	c) Vízi	— A tengeri szállítás vonatkozásában a 2004/725/EK rendelet ⁽⁴⁹⁾ I. mellékletében említett belvízi, tengeri és part menti személy- és teherszállító vállalkozások, az e társaságok által üzemeltetett egyedi hajók kivételével — A 2005/65/EK irányelv ⁽⁵⁰⁾ 3. cikkének 1. pontjában említett kikötők irányító szervei, ideértve a 2004/725/EK rendelet 2. cikkének 11. pontjában említett kikötői létesítményeket, valamint a kikötőkben található építményeket és berendezéseket működtető szervezeteket

⁴⁸ Az Európai Parlament és a Tanács 2012/34/EU irányelve (2012. november 21.) az egységes európai vasúti térség létrehozásáról (HL L 343., 2012.12.14., 32. o.).

⁴⁹ Az Európai Parlament és a Tanács 2004/725/EK rendelete (2004. március 31.) a hajók és kikötőlétesítmények védelmének fokozásáról (HL L 129., 2004.4.29., 6. o.).

⁵⁰ Az Európai Parlament és a Tanács 2005/65/EK irányelve (2005. október 26.) a kikötővédelem fokozásáról (HL L 310., 2005.11.25., 28. o.).

		— A 2002/59/EK irányelv ⁽⁵¹⁾ 3. cikkének o) pontjában említett hajóforgalmi szolgáltatások
	d) Közúti	— Az (EU) 2015/962 felhatalmazáson alapuló bizottsági rendelet ⁽⁵²⁾ 2. cikkének (12) pontjában említett, a forgalomirányításért felelős közúti hatóságok, azon közigazgatási szervek kivételével, amelyek általános tevékenységének nem alapvető része a forgalomszervezés vagy az intelligens közlekedési rendszerek üzemeltetése. — A 2010/40/EU irányelv ⁽⁵³⁾ 4. cikkének 1. pontjában említett intelligens közlekedési rendszerek üzemeltetői
3. Banki szolgáltatások		— Az 575/2013/EU rendelet ⁽⁵⁴⁾ 4. cikkének 1. pontjában említett hitelintézetek, [kivéve a 2013/36/EU irányelv 2. cikke (5) bekezdésének 8. pontjában említetteket, amelyek az XX rendelet [DORA-rendelet] 2. cikkének (4) bekezdésével összhangban mentességet kapnak]

⁵¹ Az Európai Parlament és a Tanács 2002/59/EK irányelve (2002. június 27.) a közösségi hajóforgalomra vonatkozó megfigyelő és információs rendszer létrehozásáról és a 93/75/EGK irányelv hatályon kívül helyezéséről (HL L 208., 2002.8.5., 10. o.).

⁵² A Bizottság (EU) 2015/962 felhatalmazáson alapuló rendelete (2014. december 18.) a 2010/40/EU európai parlamenti és tanácsi irányelvnek az EU egészére kiterjedő valós idejű forgalmi információs szolgáltatások nyújtása tekintetében történő kiegészítéséről (HL L 157., 2015.6.23., 21. o.).

⁵³ Az Európai Parlament és a Tanács 2010/40/EU irányelve (2010. július 7.) az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről (HL L 207., 2010.8.6., 1. o.).

⁵⁴ Az Európai Parlament és a Tanács 575/2013/EU rendelete (2013. június 26.) a hitelintézetekre és befektetési vállalkozásokra vonatkozó prudenciális követelményekről és a 648/2012/EU rendelet módosításáról (HL L 176., 2013.6.27., 1. o.).

4. Pénzügyi piaci infrastruktúrák		— A 2014/65/EU irányelv ⁽⁵⁵⁾ 4. cikkének 24. pontjában említett kereskedési helyszínek üzemeltetői
		— A 648/2012/EU rendelet ⁽⁵⁶⁾ 2. cikkének 1. pontjában említett központi szerződő felek
5. Egészségügy		— A 2011/24/EU irányelv ⁽⁵⁷⁾ 3. cikkének g) pontjában említett egészségügyi szolgáltatók
		— A határokon át terjedő súlyos egészségügyi veszélyekről szóló XXXX/XXXX rendelet ⁽⁵⁸⁾ 15. cikkében említett uniós referencialaboratóriumok
		— A 2001/83/EK irányelv ⁽⁵⁹⁾ 1. cikkének 2. pontjában említett gyógyszerek kutatásával és fejlesztésével foglalkozó szervezetek — A NACE Rev. 2. C nemzetgazdasági ágának 21. ágazatában említett gyógyszeripari alaptermékeket és gyógyszerkészítményeket gyártó szervezetek — Az XXXX rendelet ⁽⁶⁰⁾ 20. cikkében említett, népegészségügyi szükséghelyzet során kritikus fontosságúnak ítélt orvostechikái

⁵⁵ Az Európai Parlament és a Tanács 2014/65/EU irányelve (2014. május 15.) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról (HL L 173., 2014.6.12., 349. o.).

⁵⁶ Az Európai Parlament és a Tanács 648/2012/EU rendelete (2012. július 4.) a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról (HL L 201., 2012.7.27., 1. o.).

⁵⁷ Az Európai Parlament és a Tanács 2011/24/EU irányelve (2011. március 9.) a határon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről (HL L 88., 2011.4.4., 45. o.).

⁵⁸ [Az Európai Parlament és a Tanács rendelete a határokon át terjedő súlyos egészségügyi veszélyekről és az 1082/2013/EU határozat hatályon kívül helyezéséről, a hivatkozást a COM(2020)727 final javaslat elfogadását követően frissíteni kell.]

⁵⁹ Az Európai Parlament és a Tanács 2001/83/EK irányelve (2001. november 6.) az emberi felhasználásra szánt gyógyszerek közösségi kódexéről (HL L 311., 2001.11.28., 67. o.).

⁶⁰ [Az Európai Parlament és a Tanács rendelete az Európai Gyógyszerügynökség által a gyógyszerek és orvostechikai eszközök tekintetében a válsághelyzetekre való felkészültség és a válságkezelés terén betöltött szerep megerősítéséről, a hivatkozást a COM(2020)725 final javaslat elfogadását követően frissíteni kell.]

		eszközöket előállító szervezetek (a továbbiakban: a népegészségügyi szükséghelyzet kritikus fontosságú eszközeinek jegyzéke)
6. Ivóvíz		A 98/83/EK tanácsi irányelv ⁽⁶¹⁾ 2. cikke 1. pontjának a) alpontjában említett, emberi fogyasztásra szánt víz szállítói és forgalmazói, de azokat a forgalmazókat kivéve, akik számára az emberi fogyasztásra szánt víz elosztása más áruk és javak forgalmazásából álló általános tevékenységüknek nem alapvető része [...]
7. Szennyvíz		A 91/271/EGK tanácsi irányelv ⁽⁶²⁾ 2. cikkének 1–3. pontjában említett települési, háztartási és ipari szennyvíz összegyűjtését, ártalmatlanítását vagy kezelését végző vállalkozások, de azokat a vállalkozásokat kivéve, akik általános tevékenységének nem alapvető része a települési, háztartási és ipari szennyvíz összegyűjtése, ártalmatlanítása és kezelése. [...]
8. Digitális infrastruktúra		— Internetkapcsolódási pont szolgáltatók
		— DNS-szolgáltatók, a gyökérnév-szerverek üzemeltetőit kivéve
		— Legfelső szintű doménnév-nyilvántartók
		— Felhőszolgáltatók

⁶¹ A Tanács 98/83/EK irányelve (1998. november 3.) az emberi fogyasztásra szánt víz minőségéről (HL L 330., 1998.12.5., 32. o.).

⁶² A Tanács 91/271/EGK irányelve (1991. május 21.) a települési szennyvíz kezeléséről (HL L 135., 1991.5.30., 40. o.).

		— Adatközpont-szolgáltatók
		— Tartalomszolgáltató hálózati szolgáltatók
		— A 910/2014/EU rendelet ⁽⁶³⁾ 3. cikkének 19. pontjában említett bizalmi szolgáltatók
		— Az (EU) 2018/1972 irányelv ⁽⁶⁴⁾ 2. cikkének 8. pontjában említett nyilvános elektronikus hírközlő hálózatok szolgáltatói vagy az (EU) 2018/1972 irányelv 2. cikkének 4. pontjában említett elektronikus hírközlési szolgáltatók, amennyiben szolgáltatásaik nyilvánosan elérhetőek
8a. IKT-szolgáltatások felügyelete (B2B)		— Felügyelt szolgáltatók — Felügyelt biztonsági szolgáltatók

⁶³ 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.).

⁶⁴ Az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról (HL L 321., 2018.12.17., 36. o.).

9. Közigazgatási szervek		— A központi kormányzat közigazgatási szervei, a tagállam általi, a nemzeti joggal összhangban lévő meghatározás szerint — [...] ⁶⁵ [...] — [...]
10. Űrpolitika		— A tagállamok vagy magánfelek tulajdonában, kezelésében és üzemeltetésében lévő azon földi infrastruktúra üzemeltetői, amelyek támogatják az űralapú szolgáltatások nyújtását, kivéve az (EU) 2018/1972 irányelv 2. cikkének 8. pontjában említett nyilvános elektronikus hírközlő hálózatok szolgáltatóit

⁶⁵ [...]

II. MELLÉKLET

ÁGAZATOK, ALÁGAZATOK ÉS SZERVEZETTÍPUSOK

Ágazat	Álágazat	Szervezet típusa
1. Postai és futárszolgáltatások		A 97/67/EK irányelv ⁽⁶⁶⁾ 2. cikkének 1[...] pontjában említett postai szolgáltatások, beleértve [...] a futárszolgáltatókat
2. Hulladékgazdálkodás		A 2008/98/EK irányelv ⁽⁶⁷⁾ 3. cikkének 9. pontjában említett hulladékgazdálkodással foglalkozó vállalkozások, de kivéve azokat a vállalkozásokat, amelyek esetében a hulladékgazdálkodás nem gazdasági főtevékenységük

⁶⁶ A 97/67/EK irányelvnek a közösségi postai szolgáltatások belső piacának teljes megvalósítása tekintetében történő módosításáról szóló, 2008. február 20-i 2008/6/EK európai parlamenti és tanácsi irányelvvel (HL L 52., 2008.2.27., 3. o.) módosított, a közösségi postai szolgáltatások belső piacának fejlesztésére és a szolgáltatás minőségének javítására vonatkozó közös szabályokról szóló, 1997. december 15-i 97/67/EK európai parlamenti és tanácsi irányelv (HL L 15., 1998.1.21., 14. o.).

⁶⁷ Az Európai Parlament és a Tanács 2008/98/EK irányelve (2008. november 19.) a hulladékokról és egyes irányelvek hatályon kívül helyezéséről (HL L 312., 2008.11.22., 3. o.).

3. Vegyszerek gyártása, előállítása és forgalmazása		Az 1907/2006/EK rendelet ⁽⁶⁸⁾ 3. cikkének [...], 9. és 14. pontjában említett anyagok és [...] keverékek gyártását [...] és forgalmazását végző vállalkozások, valamint az említett rendelet 3. cikkének 3. pontjában említett árucikkek anyagokból vagy keverékekből történő gyártását végző vállalkozások.
4. Élelmiszer-előállítás, -feldolgozás és -forgalmazás		A 178/2002/EK rendelet ⁽⁶⁹⁾ 3. cikkének 2. pontjában említett azon élelmiszeripari vállalkozások, amelyek nagykereskedelmi forgalmazást, valamint ipari termelést és feldolgozást folytatnak.
5. Gyártás	a) Orvostechnikai eszközök és in vitro diagnosztikai orvostechnikai eszközök gyártása	Az (EU) 2017/745 rendelet ⁽⁷⁰⁾ 2. cikkének 1. pontjában említett orvostechnikai eszközöket, valamint az (EU) 2017/746 rendelet ⁽⁷¹⁾ 2. cikkének 2. pontjában említett in vitro diagnosztikai orvostechnikai eszközöket gyártó szervezetek, kivéve az 1. melléklet 5. pontjában említett orvostechnikai eszközöket gyártó

⁶⁸ Az Európai Parlament és a Tanács 1907/2006/EK rendelete (2006. december 18.) a vegyi anyagok regisztrálásáról, értékeléséről, engedélyezéséről és korlátozásáról (REACH), az Európai Vegyianyag-ügynökség létrehozásáról, az 1999/45/EK irányelv módosításáról, valamint a 793/93/EGK tanácsi rendelet, az 1488/94/EK bizottsági rendelet, a 76/769/EGK tanácsi irányelv, a 91/155/EGK, a 93/67/EGK, a 93/105/EK és a 2000/21/EK bizottsági irányelv hatályon kívül helyezéséről (HL L 396., 2006.12.30., 1. o.).

⁶⁹ Az Európai Parlament és a Tanács 178/2002/EK rendelete (2002. január 28.) az élelmiszerjog általános elveiről és követelményeiről, az Európai Élelmiszerbiztonsági Hatóság létrehozásáról és az élelmiszerbiztonságra vonatkozó eljárások megállapításáról (HL L 31., 2002.2.1., 1. o.).

⁷⁰ Az Európai Parlament és a Tanács (EU) 2017/745 rendelete (2017. április 5.) az orvostechnikai eszközökről, a 2001/83/EK irányelv, a 178/2002/EK rendelet és az 1223/2009/EK rendelet módosításáról, valamint a 90/385/EGK és a 93/42/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 117., 2017.5.5., 1. o.).

⁷¹ Az Európai Parlament és a Tanács (EU) 2017/746 rendelete (2017. április 5.) az in vitro diagnosztikai orvostechnikai eszközökről, valamint a 98/79/EK irányelv és a 2010/227/EU bizottsági határozat hatályon kívül helyezéséről (HL L 117., 2017.5.5., 176. o.).

		szervezeteket
	b) Számítógépek, elektronikai és optikai termékek gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 26. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
	c) Villamos berendezések gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 27. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
	d) Máshova nem sorolt gépek és gépi berendezések gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 28. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
	e) Gépjárművek, pótkocsik és félpótkocsik gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 29. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
	f) Egyéb szállítóeszközök gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 30. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
6. Digitális szolgáltatók		— Online piacterek szolgáltatói
		— Online keresőmotorok szolgáltatói
		— A közösségi hálózati szolgáltató platform szolgáltatói
