



EURÓPAI  
BIZOTTSÁG

Brüsszel, 2017.10.4.  
COM(2017) 477 final

2017/0225 (COD)

NOTE

This language version reflects the corrections done to the original EN version transmitted under COM(2017) 477 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 477 final/2 of 4.10.2017

Javaslat

**AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE**

**az ENISA-ról, az „Európai Unió Kiberbiztonsági Ügynökségéről”,  
az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és  
kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági  
jogszabály”)**

(EGT-vonatkozású szöveg)

{SWD(2017) 500 final}

{SWD(2017) 501 final}

{SWD(2017) 502 final}

## INDOKOLÁS

### **1. A JAVASLAT HÁTTERE**

#### **• A javaslat indokai és céljai**

Az Európai Unió több lépést tett az ellenálló képesség növelése és kiberbiztonsági felkészültségének fokozása érdekében. A 2013-ban elfogadott első uniós kiberbiztonsági stratégia<sup>1</sup> stratégiai célokat és konkrét intézkedéseket fogalmazott meg az ellenálló képesség elérése, a kiberbűnözés csökkentése, a kibervédelmi politika és kapacitások, valamint az ipari és technológiai erőforrások fejlesztése és egy koherens uniós nemzetközi kibertér-politika kialakítása érdekében. Ebben az összefüggésben azóta fontos fejlemények történtek, köztük különösen az Európai Unió Hálózat- és Információbiztonsági Ügynökség (ENISA) második megbízatása<sup>2</sup> és a hálózati és információs rendszerek biztonságáról szóló irányelv<sup>3</sup> (a továbbiakban: kiberbiztonsági irányelv) elfogadása, amelyek e javaslat alapját képezik.

Ezen túlmenően 2016-ban az Európai Bizottság közleményt fogadott el „Európa kibertámadásokkal szembeni ellenálló képességének erősítése, valamint a versenyképes és innovatív kiberbiztonsági ágazat támogatása”<sup>4</sup> címmel, amelyben további intézkedéseket jelentettek be az együttműködés, az információ- és tudásmegosztás fokozására, valamint az Unió ellenálló képességének és felkészültségének növelésére, figyelembe véve továbbá a nagyszabású incidensek előfordulásának lehetőségeit és egy lehetséges páneurópai kiberbiztonsági válságot. Ezzel összefüggően a Bizottság bejelentette, hogy elő fogja terjesztetni az Európai Unió Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről szóló 526/2013/EU európai parlamenti és tanácsi rendelet (a továbbiakban: ENISA-rendelet) értékelését és felülvizsgálatát. Az értékelési folyamat az Ügynökség lehetséges reformjához, valamint kapacitásainak és képességeinek fokozásához vezethet, hogy fenntartható módon tudja támogatni a tagállamokat. E folyamat eredményeként tehát operatívabb és központi szerepet fog betölteni a kibertámadásokkal szembeni ellenálló képességének elérésében, és új megbízatása részeként megkapja a kiberbiztonsági irányelvben meghatározott új feladatköröket.

A kiberbiztonsági irányelv az első alapvető lépés a kockázatkezelés kultúrája népszerűsítésének irányában azáltal, hogy biztonsági követelményeket vezet be jogi kötelezettségként a főbb gazdasági szereplők, nevezetesen az alapvető szolgáltatást nyújtó szereplők (alapvető szolgáltatásokat nyújtó szereplők – OES) és egyes főbb digitális szolgáltatók (digitális szolgáltatók – DSP-k) számára. Mivel a biztonsági követelmények alapvető fontosságúnak tekinthetők a társadalom digitalizálódásával járó előnyök megőrzése szempontjából – és a csatlakoztatott eszközök (a dolgok internete) gyors elterjedése miatt – a 2016. évi közlemény az IKT-termékek és -szolgáltatások biztonsági tanúsítására szolgáló keretrendszer létrehozásának ötletét is előterjesztette, hogy növelje a digitális egységes piac iránti bizalmat és e piac biztonságosságát. Az IKT kiberbiztonsági tanúsítása különösen

<sup>1</sup> Az Európai Bizottság és az Európai Külügyi Szolgálat közös közleménye: Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér (JOIN (2013)).

<sup>2</sup> 526/2013/EU rendelet az Európai Unió Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről.

<sup>3</sup> (EU) 2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

<sup>4</sup> Az Európai Bizottság közleménye Európa kibertámadásokkal szembeni ellenálló képességének erősítéséről, valamint a versenyképes és innovatív kiberbiztonsági ágazat támogatásáról, COM/2016/0410 final.

fontos a magas szintű kiberbiztonságot igénylő technológiák – így például az összekapcsolt és automatizált járművek, az elektronikus egészségügyi megoldások és az ipari automatikus vezérlőrendszerek (IACS) – fokozott használata miatt.

Ezeket a szakpolitikai intézkedéseket és bejelentéseket tovább erősítették a 2016. évi tanácsi következtetések, amelyek elismerték, hogy „a kiberfenyegetések és -sebezhetőségek folyamatosan alakulnak és fokozódnak, ami azt jelenti, hogy folytatni kell és szorosabbra kell fűzni az együttműködést, különösen a nagy léptékű, határokon átnyúló kiberbiztonsági incidensek kezelése ügyében”. A következtetések megerősítették, hogy „az ENISA-rendelet alkotja a kibertámadásokkal szembeni ellenálló képesség uniós keretrendszere sarokköveinek egyikét”<sup>5</sup>, és további lépések megtételére kérték fel a Bizottságot az európai szintű tanúsítás kérdésének kezelése érdekében.

A tanúsítási rendszer létrehozásához egy megfelelő uniós irányítási rendszer kiépítésére – többek között egy független uniós ügynökség alapos szakvéleményére lenne szükség. Ebben a tekintetben ez a javaslat – annak jellegéből adódóan – az ENISA-t azonosítja kiberbiztonsági ügyekben illetékes uniós szintű szervként, amelynek fel kell vállalnia az illetékes nemzeti szervek összefogásának és munkájuk összehangolásának szerepét a tanúsítás terén.

A digitális egységes piac stratégiájának 2017. májusi félidős értékeléséről szóló közleményében a Bizottság pontosította, hogy 2017 szeptemberére fogja felülvizsgálni az ENISA megbízatását. A felülvizsgálat célja, hogy meghatározza az Ügynökség szerepét a megváltozott kiberbiztonsági ökoszisztémában, és hogy a kiberbiztonsági szabványokra, a tanúsításra és a címkézésre vonatkozó intézkedéseket dolgozzon ki az IKT-alapú rendszerek – ideértve az összekapcsolt tárgyakat is – biztonságosabbá tétele érdekében<sup>6</sup>. Az Európai Tanács 2017. júniusi következtetéseiben<sup>7</sup> üdvözlöi a Bizottság arra irányuló szándékát, hogy szeptemberben felülvizsgálja a kiberbiztonsági stratégiát és az év végéig további célzott intézkedésekre tesz javaslatot.

A rendeletjavaslat olyan átfogó intézkedéscsomagot irányoz elő, amely a korábbi intézkedésekre épül, és egymást erősítő egyedi célkitűzéseket mozdít elő:

- a tagállamok és vállalkozások képességeinek és felkészültségének javítása;
- a tagállamok, uniós intézmények, hivatalok és szervek közötti együttműködés és koordináció javítása;
- a tagállami fellépések kiegészítését szolgáló uniós szintű képességek növelése, különösen a határon átnyúló kiberválságok esetében;
- a magánfelhasználók és a vállalkozások tudatosságának növelése a kiberbiztonsággal kapcsolatos kérdésekben;
- az IKT-termékek és -szolgáltatások kiberbiztonsági szintje átláthatóságának<sup>8</sup> növelése a digitális egységes piac és a digitális innováció iránti bizalom megerősítése érdekében; valamint

<sup>5</sup> A Tanács következtetései Európa kibertámadásokkal szembeni ellenálló képességének erősítéséről, valamint a versenyképes és innovatív kiberbiztonsági ágazat támogatásáról – 2016. november 15.

<sup>6</sup> A Bizottság közleménye a digitális egységes piaci stratégia végrehajtásának félidős értékeléséről, COM(2017) 228.

<sup>7</sup> Az Európai Tanács ülése (2017. június 22–23.) – Következtetések, EUCO 8/17.

<sup>8</sup> A kiberbiztonsági szint átláthatósága azt jelenti, hogy a felhasználók elegendő információhoz jutnak a kiberbiztonsági tulajdonságokra vonatkozóan, amelynek révén objektív módon képesek meghatározni egy adott IKT-termék, -szolgáltatás vagy -folyamat biztonsági szintjét.

- az uniós tanúsítási rendszerek és a kapcsolódó biztonsági követelmények és értékelési kritériumok tagállamok és ágazatok közötti összehangatlanságának elkerülése.

Az indokolás következő része a kezdeményezés alapvető okait fejti ki részletesebben az ENISA-ra és kiberbiztonsági tanúsításra irányuló javasolt intézkedésekre vonatkozóan.

## ENISA

Az ENISA olyan szakértői központként működik, amely az Unión belüli hálózat- és információbiztonság fokozását és a tagállamok kapacitásépítésének támogatását látja el.

Az ENISA 2004-ben alakult<sup>9</sup> azzal az általános céllal, hogy hozzájáruljon a hálózat- és információbiztonság magas szinten tartásához az Unióban. 2013-ban az 526/2013/EU rendelet 2020-ig új, hétéves megbízatást állapított meg az Ügynökség számára. Az Ügynökség hivatalai Görögországban találhatók: adminisztratív székhelye a krétai Iráklíóban, az alapvető tevékenységeket ellátó központja pedig Athénban van.

Az ENISA a többi ügynökséghez képest kicsi – alacsony költségvetéssel és személyi állománnyal rendelkezik. Megbízatása határozott időre szól.

Az ENISA hálózat- és információbiztonsági problémák kezelésében, a biztonsági eseményekre való reagálásban és különösen a problémák megelőzésében támogatja az európai intézményeket, a tagállamokat és a vállalatokat. Ezt a feladatát a stratégiája részeként azonosított öt területen, több tevékenységen keresztül látja el<sup>10</sup>:

- Szaktudás: információ és szakértelem biztosítása a főbb hálózat- és információbiztonsági kérdésekben.
- Politikaalkotás: az uniós politikai döntéshozatal és végrehajtás támogatása.
- Kapacitás: kapacitásépítés támogatása Unió-szerte (pl. képzések, ajánlások, tudatosságnövelő tevékenységek révén).
- Közösség: hálózat- és információbiztonsági közösség támogatása (pl. a számítógépes vészhelyzeteket elhárító csoportok [CERT-ek] támogatása, a pán-európai kibergyakorlatok koordinációja).
- Támogatás (pl. kapcsolatépítés az érdekeltekkel és a nemzetközi kapcsolatokat bevonása).

A kiberbiztonsági irányelvről folytatott tárgyalások során az Unió társjogalkotói úgy döntöttek, hogy fontos szerepköröket rendelnek az ENISA-hoz az irányelv végrehajtása terén. Az Ügynökség mindenekelőtt biztosítja a titkárságot a CSIRT-hálózat számára (a hálózat célja, hogy gyors és hatékony operatív együttműködést tegyen lehetővé a tagállamok között konkrét kiberbiztonsági eseményeknél és tájékoztasson a kockázatokról), és arra is felkérést kap, hogy segítse az együttműködési csoportot feladatai végrehajtásában. Ezen túlmenően az irányelv előírja az ENISA számára, hogy szakértelmével és tanácsaival, valamint a bevált módszerek megosztásának lehetővé tételével támogassa a tagállamok és a Bizottság munkáját.

Az ENISA-rendeletnek megfelelően a Bizottság elvégezte az Ügynökség értékelését, amely független tanulmányt, valamint nyilvános konzultációt is magában foglal. Az értékelés az Ügynökség relevanciáját, hatását, eredményességét, hatékonyságát, koherenciáját és uniós hozzáadott értékét vizsgálta a 2013–2016 közötti teljesítménye, irányítása, belső szervezeti felépítése és munkamódszerei viszonylatában.

<sup>9</sup> Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról (HL L 77., 2004.3.13., 1. o.).

<sup>10</sup> <https://www.enisa.europa.eu/publications/corporate/enisa-strategy>

A válaszadók többsége (74 %)<sup>11</sup> összességében pozitívan értékelte az ENISA teljesítményét a nyilvános konzultáció során. A válaszadók nagy része (az egyes célok esetében legalább 63 %) ezenfelül úgy vélte, hogy az ENISA teljesítette különböző céljait. A válaszadók mintegy fele (46 %-a) rendszeresen (havonta vagy még gyakrabban) igénybe veszi az ENISA szolgáltatásait és termékeit, 83 %-uk értékeli, hogy ezek uniós szintű szervtől származnak, 62 %-uk pedig elégedett a minőségükkel.

A válaszadók nagy többsége (88 %) azonban úgy vélte, hogy az uniós szinten rendelkezésre álló jelenlegi eszközök és mechanizmusok nem megfelelőek, vagy csak részben jelentenek megoldást az aktuális kiberbiztonsági problémák kezelésére. A válaszadók túlnyomó többsége (98 %) úgy véli, hogy szükség van egy uniós szervre az említett igények kiszolgálására, 99 %-uk pedig azt gondolja, hogy erre az ENISA a legalkalmasabb. Ezen túlmenően a válaszadók 67,5 %-a volt azon a véleményen, hogy az ENISA szerepet játszhatna az informatikai termékek és szolgáltatások biztonsági tanúsítását segítő harmonizált keretrendszer létrehozásában.

Az átfogó értékelés (amely a nyilvános konzultáció mellett számos személyes interjún, további célzott felméréseken és műhelytalálkozókra alapult) az alábbi következtetésekkel zárult:

- Az ENISA céljai ma is időszerűek. Figyelembe véve a gyors technológiai fejlesztéseket, a kialakuló fenyegetéseket és a növekvő globális kiberbiztonsági kockázatokat, egyértelműen szükség van az Unióban a kiberbiztonsági kérdésekkel kapcsolatos magas szintű technikai szakértelem előmozdítására és továbbfejlesztésére. A tagállamokban kapacitásokat kell kialakítani a fenyegetések megértése és az azokra való reagálás érdekében, a tematikus területek és intézmények érdekeltjeinek pedig együtt kell működniük.
- Kis költségvetése ellenére az Ügynökség hatékonyan használja fel erőforrásait és hajtja végre feladatait. A helyszínek Athén és Iráklio közötti megosztása ugyanakkor további igazgatási költségekkel is jár.
- Az eredményesség terén az ENISA részben teljesítette céljait. Az Ügynökség sikeresen járult hozzá a hálózat- és információbiztonság javításához Európában azáltal, hogy a 28 tagállamban<sup>12</sup> kapacitásépítést tett lehetővé, megerősítette az együttműködést a tagállamok és a hálózat- és információbiztonsággal foglalkozó érdekelték között, és szakértelmével, közösségben játszott építő szerepével és támogatásával segítette a politikák kialakítását. Az ENISA összességében kellő gondossággal összpontosított munkaprogramja végrehajtására, és megbízható

<sup>11</sup> 19 tagállamból 90 érdekelt fél (88 válasz és 2 állásfoglalás érkezett), köztük 15 tagállam nemzeti hatóságai és nyolc, az európai vállalkozások nagy részét képviselő ernyőszervezet reagált a megkeresésre.

<sup>12</sup> A nyilvános konzultáció válaszadóit felkérték arra, hogy tegyék meg észrevételeiket az ENISA 2013 és 2016 között elért főbb eredményeiről. A valamennyi csoportot képviselő válaszadók (összesen 55, amelyből 13 nemzeti hatóság, 20 a magánszektor képviselője, 22 egyéb kategóriába tartozik) szerint az ENISA az alábbi területeken ért el jelentős eredményeket: 1) a Cyber Europe gyakorlatainak összehangolása; 2) a CERT-ek/CSIRT-ek támogatása a koordinációt és információcserét ösztönző képzések és műhelytalálkozók révén; 3) ENISA-kiadványok (iránymutatások és ajánlások, fenyegetettségi helyzetjelentések, biztonsági eseményekre és válságkezelésre vonatkozó stratégiák stb.), amelyek hasznosnak bizonyultak a nemzetbiztonsági keretek létrehozása és naprakésszé tétele szempontjából, valamint fontos referenciaként szolgáltak a szakpolitikai döntéshozók és a kiberbiztonsági szakemberek számára; 4) a kiberbiztonsági irányelv népszerűsítésének támogatása; 5) kiberbiztonsággal kapcsolatos tudatosságnövelés a kiberbiztonsági hónap keretében.

partnere volt érdekeltjeinek egy olyan területen, amelyről csak a közelmúltban ismerték el, hogy erőteljes határokon átnyúló relevanciával bír.

- Az ENISA – legalábbis bizonyos mértékig – hatást ért el a hálózat- és információbiztonság tágabb területén, de összességében nem tudott erős márkanév kialakítani és elegendő ismertséget szerezni ahhoz, hogy Európa szakértői központjaként ismerjék el. Ennek oka, hogy az ENISA megbízatása széles körű, és az Ügynökség nem rendelkezett arányaiban elegendő erőforrással. Ezen túlmenően továbbra is az ENISA az egyetlen határozott idejű megbízatással rendelkező uniós ügynökség, ami korlátozza abban, hogy hosszú távú jövőképet fogalmazzon meg és fenntartható módon támogassa érdekeltjeit. Ez ellentétes a kiberbiztonsági irányelv rendelkezéseivel, amelyek határozatlan időre szóló feladatokat ruháznak az ENISA-ra. Végül az értékelés megállapította, hogy az eredményességi problémák részben azzal magyarázhatók, hogy az Ügynökség belső szakértők helyett inkább külső szakértőket alkalmazott, és nehézségek árán sikerült szakképzett személyzetet találnia és megtartania.
- Végül, de nem utolsósorban az értékelés arra a következtetésre jutott, hogy az ENISA hozzáadott értéke elsősorban azon képességében rejlik, hogy meg tudja erősíteni az együttműködést főként a tagállamok, és mindenekelőtt a kapcsolódó hálózat- és információbiztonsági közösségek (különösen a CSIRT-ek) között. Uniós szinten az ENISA az egyetlen szereplő, amelyik ilyen sokféle hálózat- és információbiztonsági érdekeltet támogat. Mivel azonban tevékenységeit szigorú prioritási elvek vezérlik, az ENISA munkaprogramja elsősorban a tagállami igények szerint alakul. Ennek eredményeképpen nem foglalkozik kellő mértékben az érdekeltek, különösképpen az ipar által támasztott igényekkel. Ez azzal is jár, hogy az Ügynökség, reaktív módon, legfontosabb érdekeltjei igényeinek kiszolgálására összpontosít, ami megakadályozza abban, hogy nagyobb hatást érjen el. Az Ügynökség által nyújtott hozzáadott érték ezért az érdekeltek eltérő igényeinek megfelelően alakult, és hatóköre aszerint változott, hogy az Ügynökség milyen mértékben tudott reagálni ezekre az igényekre (pl. a nagy és kis tagállamok, vagy a tagállamok és az ipar igényei közötti különbségek).

Összefoglalva: az érdekeltekkel folytatott konzultációk és az értékelés eredményei arra engednek következtetni, hogy az ENISA erőforrásait és megbízatását ki kell igazítani, hogy megfelelően tudjon reagálni az aktuális és jövőbeli kihívásokra.

Figyelembe véve ezeket a megállapításokat, a javaslat felülvizsgálja az ENISA jelenlegi megbízatását, és új feladatokat és funkciókat határoz meg számára azért, hogy hatékonyan és eredményesen támogassa a tagállamok, az uniós intézmények és más érdekeltek biztonságos uniós kibertér kialakítására irányuló erőfeszítéseit. Az új, javasolt megbízatás erőteljesebb és központibb szerepet kíván biztosítani az Ügynökség számára, mindenekelőtt azzal, hogy az Ügynökség támogatja a tagállamokat is a kiberbiztonsági irányelv végrehajtásában és bizonyos fenyegetések aktívabb elhárításában (operatív kapacitás), illetve azzal, hogy szakértői központtá válva támogatja a tagállamokat és a Bizottságot a kiberbiztonsági tanúsítás területén. A javaslat értelmében:

- az ENISA állandó megbízatást kapna, és ilyen módon stabil alappal rendelkezne a jövőre nézve. A megbízatás, a célok és feladatok továbbra is rendszeres felülvizsgálat tárgyát kell hogy képezzék;
- a javasolt megbízatás tovább pontosítja az ENISA szerepét az Unió kiberbiztonsági ügynökségeként és kiberbiztonsági ökoszisztémájának referenciapontjaként, amely szorosan együttműködik az ökoszisztéma többi érintett szervével;

- az Ügynökség szervezeti felépítését és irányítását, amelyet az értékelés során pozitívan ítélték meg, bizonyos mértékig felül fogják vizsgálni, különösen azért, hogy az Ügynökség munkája jobban tükrözze a szélesebb érdekcsoportok igényeit;
- a megbízatás javasolt hatálya pontosan körül van határolva – megerősíti azokat a területeket, ahol az Ügynökség egyértelműen hozzáadott értéket mutat, illetve olyan új területekkel egészül ki, ahol az új szakpolitikai prioritások és eszközök – mindenekelőtt a kiberbiztonsági irányelv, az uniós kiberbiztonsági stratégia felülvizsgálata, a kiberválsággal összefüggő együttműködésről szóló, készülő uniós kiberbiztonsági tervezet és az IKT biztonsági tanúsítás – vonatkozásában támogatásra van szükség:
  - **Az uniós szakpolitika kidolgozása és végrehajtása:** az ENISA feladata lenne, hogy proaktív módon járuljon hozzá a szakpolitika kidolgozásához a hálózat- és információbiztonság területén, valamint egyéb olyan szakpolitikai kezdeményezések kialakításához, amelyek különféle ágazatokat (pl. az energiaipart, a közlekedést, a pénzügyeket) érintő kiberbiztonsági elemeket tartalmaznak. Ezért erőteljes tanácsadói szerephez jutna, amelyet független véleményekkel és a szakpolitika és jog kidolgozásához és naprakésszé tételéhez szükséges előkészítő munka biztosítása révén valósíthatna meg. Az ENISA az elektronikus hírközlés, elektronikus azonosítás és bizalmi szolgáltatások területét érintő uniós politikát és jogot is támogatná azért, hogy ezzel hozzájáruljon a kiberbiztonság javításához. A végrehajtási szakaszban, különösképpen a hálózat- és információbiztonsággal foglalkozó együttműködési csoporttal összefüggően, az ENISA segítséget nyújtana a tagállamoknak abban, hogy következetes megközelítésre jussanak a kiberbiztonsági irányelv végrehajtásával kapcsolatban határokon és ágazatokon átnyúlóan, illetve egyéb releváns politikák és jogszabályok területén. A kiberbiztonsági politikák és jogszabályok rendszeres felülvizsgálatának támogatása érdekében az ENISA rendszeresen jelentést tenne az uniós jogi keretrendszer végrehajtásának állapotáról.
  - **Kapacitásépítés:** az ENISA hozzájárulna az uniós és nemzeti közigazgatási szervek képességeinek és szakértelmének javításához, többek között a biztonsági eseményekre való reagálás és a kiberbiztonsággal kapcsolatos szabályozói intézkedések felülvizsgálata terén. Az Ügynökségtől azt is elvárják, hogy támogassa az információmegosztási és elemző központok (ISACS) létrehozását több ágazatban azáltal, hogy bevált módszereket és iránymutatást nyújt az elérhető eszközökről és eljárásokról, emellett pedig megfelelően kezeli az információmegosztással kapcsolatos szabályozási kérdéseket.
  - **Tudás- és információmegosztás, tudatosságnövelés:** az ENISA az Unió információs központjává válna. Mindez a bevált módszerek és kezdeményezések népszerűsítését és megosztását vonná maga után Unió-szerte az uniós és nemzeti intézményektől, hivataloktól és szervektől származó kiberbiztonsági információk összevonása révén. Az Ügynökség a kritikus infrastruktúrák biztonságával kapcsolatos tanácsokat, iránymutatást és bevált módszereket is rendelkezésre bocsátaná. A határokon átnyúló jelentős kiberbiztonsági események következtében az ENISA továbbá jelentéseket készítene abból a célból, hogy Unió-szerte iránymutatást nyújtson a vállalkozások és a magánfelhasználók számára. A munkafolyamat – a



tagállami hatóságokkal egyeztetve – rendszeres tudatosságnövelő tevékenységek megszervezését is magában foglalná.

- **Piaci feladatok (szabványosítás, kiberbiztonsági tanúsítás):** az ENISA számos olyan feladatkört töltene be, amelyek kifejezetten a belső piacot támogatnák, és magában foglalna egy kiberbiztonsági piaci megfigyelőközpontot, amely elemzi a kiberbiztonsági piac releváns tendenciáit a kereslet és kínálat megfelelőbb kielégítése érdekében és támogatja az uniós politika kialakítását az IKT szabványosításának és kiberbiztonsági tanúsításának területein. Különös tekintettel a szabványosításra, az Ügynökség elősegítené a kiberbiztonsági szabványok kialakítását és használatát. Ezen túlmenően a jövőbeli tanúsítási keretrendszerrel kapcsolatban előírányzott feladatokat szintén végrehajtaná (lásd az alábbi szakaszt).
- **Kutatás és innováció:** az ENISA a kutatás-fejlesztés területén felmerülő feladatok rangsorolásával kapcsolatban szakértő tanácsokkal segítené az uniós és nemzeti hatóságok munkáját, a kiberbiztonsági szerződéses köz-magán társulással összefüggésben is. Az ENISA kutatási tanácsai a következő többéves pénzügyi keret részeként kialakítandó új Európai Kiberbiztonsági Kutató- és Kompetenciaközpont megvalósításában játszanak majd szerepet. Az ENISA – a Bizottság kérésére – a kutatási és innovációs uniós finanszírozási programok végrehajtásában is részt venne.
- **Operatív együttműködés és válságkezelés:** ennek a munkafolyamatnak a meglévő megelőző operatív képességek megerősítésére kell épülnie, mindenekelőtt a páns-európai kiberbiztonsági gyakorlatok (Cyber Europe) évenkénti megszervezésével történő javításával, valamint a CSIRT-hálózat titkársági feladatait ellátva (a kiberbiztonsági irányelv rendelkezései alapján) az operatív együttműködés támogatásán kell alapulnia azáltal, hogy biztosítja többek között a hálózat informatikai infrastruktúrájának és kommunikációs csatornáinak megfelelő működését. Ezzel összefüggésben strukturált együttműködésre lenne szükség az uniós számítógépes vészhelyzeteket elhárító csoporttal, a Számítástechnikai Bűnözés Elleni Európai Központtal (EC3) és a többi érdekelt uniós szervvel. Továbbá az uniós számítógépes vészhelyzeteket elhárító csoporttal való strukturált együttműködésnek (aminek szoros fizikai közelségben kell zajlania) olyan funkcióként kell működnie, amely technikai segítséget nyújt jelentős biztonsági események esetén, és támogatja az események elemzését. Azok a tagállamok, amelyek igénylik, segítséget kapnának az események kezeléséhez, és háttértámogatásban részesülnének a sebezhetőségek, informatikai hibák és biztonsági események elemzéséhez annak érdekében, hogy megerősítsék saját megelőző és reagálási képességüket.
- Az ENISA emellett szerepet játszana az Unió kiberbiztonsági tervezetében, amelyet e csomag részeként mutatnak be, és amely bizottsági ajánlásokat fogalmaz meg a tagállamok számára a nagy léptékű, határokon átnyúló kiberbiztonsági eseményekre és válsághelyzetekre adható, uniós szinten összehangolt reagálásra vonatkozóan<sup>13</sup>. Az ENISA megkönnyítené az egyes

<sup>13</sup>

A „tervezet” olyan kiberbiztonsági eseményekre fogják alkalmazni, amelynek hatása sokkal nagyobb annál, hogy bármelyik tagállam önállóan tudná kezelni, illetve két vagy több tagállam szempontjából is olyan átfogó és jelentős hatással vagy politikai jelentőséggel bír, amelyhez uniós politikai szinten időszerű összehangolt fellépésre és válaszra van szükség.

tagállamok közötti együttműködést a vészhelyzetek elhárítását illetően azáltal, hogy elemezné és összesítené a tagállamok és más szervezetek által önkéntes alapon rendelkezésre bocsátott információk alapján készített nemzeti helyzetjelentéseket.

- **Az IKT-termékek és -szolgáltatások kiberbiztonsági tanúsítása**

A bizalom és biztonság megteremtése és megőrzése érdekében az IKT-termékekbe és -szolgáltatásokba már a műszaki tervezés és fejlesztés korai szakaszaiban közvetlenül be kell építeni a biztonsági elemeket (beépített biztonság). Továbbá a vásárlóknak és felhasználóknak meg kell tudniuk állapítani az általuk beszerzett vagy megvásárolt termékek és szolgáltatások biztonsági szintjét.

A tanúsítás, amely a termékek, szolgáltatások és folyamatok független és akkreditált testület általi, meghatározott, szabványos kritériumokon alapuló formális értékeléséből és egy megfelelőségi tanúsítvány kiállításából áll, fontos szerepet játszik abban, hogy javuljon a termékek és szolgáltatások biztonsága és nőjön a beléjük vetett bizalom. Míg a biztonsági értékelések kifejezetten technikai jellegűek, a tanúsítás célja, hogy tájékoztassa és meggyőzze a vásárlókat és felhasználókat a megvásárolt vagy használt IKT-termékek és -szolgáltatások biztonsági tulajdonságairól. Mint már említettük, ez kifejezetten az új rendszereknél releváns, amelyek nagymértékben alkalmazzák a digitális technológiákat és magas szintű biztonságot igényelnek: ilyenek például az összekapcsolt és automatizált járművek, az elektronikus egészségügyi megoldások, az ipari automatikus vezérlőrendszerek (IACS)<sup>14</sup> vagy az intelligens energiahálózatok.

Az IKT-termékek és -szolgáltatások uniós kiberbiztonsági tanúsítása jelenleg nem mutat egységes képet. Számos nemzetközi kezdeményezés létezik, mint például az ún. közös kritériumok az információs technológiák biztonsági értékeléséről (ISO 15408); ezek a kritériumok alkotják a számítógépes biztonság értékelésére szolgáló nemzetközi szabványt. A szabvány harmadik fél értékelésén alapul, és hét biztonsági szintet (EAL) ír elő. A közös kritériumok és az azokat kísérő közös módszertan (CEM) adja a nemzetközi megállapodás – a közös kritériumok elismeréséről szóló megállapodás (CCRA) – technológiai alapját, ami garantálja, hogy a közös kritériumok alapján kiállított tanúsítványokat a CCRA összes aláírója elismeri. A CCRA jelenlegi verziójában azonban csak a 2. EAL szintig végzett értékeléseket ismerik el kölcsönösen. Ráadásul mindössze 13 tagállam írta alá a megállapodást.

Tizenkét tagállam tanúsító hatóságai kölcsönös elismerési megállapodást dolgozott ki a közös kritériumokon alapján, a megállapodással összhangban kiállított tanúsítványokra vonatkozóan<sup>15</sup>. Ezenkívül jelenleg több IKT-tanúsítási kezdeményezés létezik vagy áll kidolgozás alatt a tagállamokban. Ezek fontosak ugyan, de fennáll a kockázata, hogy az

<sup>14</sup> A Közös Kutatóközpont Főigazgatósága jelentést tett közzé, amely javaslatot tesz egy közös európai követelménykészlet- és átfogó iránymutatás-csomag kidolgozására az IACS összetevőinek kiberbiztonsági tanúsítására vonatkozóan. Elérhető a következő címen: <https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccfhttps://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf>

<sup>15</sup> A vezető tisztviselők információs rendszerek biztonságával foglalkozó csoportjának (SOG-IS) 12 tagállam és Norvégia a tagja; e csoport kidolgozott néhány védelmi profilt bizonyos termékekre, így például a digitális aláírásra, a digitális tachográfkészülékre és az intelligens kártyákra vonatkozóan. A résztvevők együtt dolgoznak a közös kritériumokon alapuló védelmi profilok szabványosításának koordinálásán, és ők irányítják az ilyen profilok kidolgozását. A tagállamok gyakran kérik a SOG-IS tanúsítását a nemzeti közbeszerzési pályázatoknál.

egységes piac szétagoltságához és átjárhatósági problémákhoz vezetnek. Következésképpen előfordulhat, hogy egy vállalatnak számos tanúsítási eljárásról kell átmennie a különböző tagállamokban ahhoz, hogy több piacon értékesíthesse termékét. Egy intelligens fogyasztásmérőt gyártó vállalatnak például, amely három tagállamban, pl. Németországban, Franciaországban és az Egyesült Királyságban kívánja értékesíteni termékeit, jelenleg három különféle tanúsítási rendszernek kell megfelelnie. Az Egyesült Államokban ez a Commercial Product Assurance (CPA), Franciaországban a Certification de Sécurité de Premier Niveau (CSPN), Németországban pedig egy közös kritériumokon alapuló egyedi védelmi profil.

Mindez magasabb költségeket és jelentős adminisztratív terhet ró a több tagállamban működő vállalatokra. Bár a tanúsítás költsége jelentős eltéréseket mutathat az érintett terméktől/szolgáltatástól, a biztonsági szint kívánt értékelésétől és/vagy a többi összetevőtől függően, mértéke általában tetemes a vállalatok számára. A BSI esetében az „intelligens fogyasztásmérő engedélyezési tanúsítványa” például több mint egymillió euróba kerül (a vizsgálat és a biztonság legmagasabb szintje, ami nemcsak egy termékre, de a köré épülő egész infrastruktúrára vonatkozik). Az intelligens fogyasztásmérők tanúsítási költsége mintegy 150 000 EUR az Egyesült Királyságban. Franciaországban hasonló vagy még magasabb költségekkel kell számolni.

A legfontosabb állami érdekeltek és magánszereplők elismerték, hogy az Unió egészére kiterjedő kiberbiztonsági tanúsítási rendszer hiányában a vállalatokat sok esetben egyedi módon kell tanúsítani minden tagállamban, ami a piac szétagoltságához vezet. Ami még ennél is fontosabb, hogy az IKT-termékekre és -szolgáltatásokra vonatkozó uniós harmonizációs jogszabályok hiányában a tagállami kiberbiztonsági tanúsítási szabványok és gyakorlatok terén mutatkozó különbségek miatt az Unióban 28 különálló, saját technikai követelményekkel, tesztelési módszerekkel és kiberbiztonsági tanúsítási eljárásokkal bíró biztonsági piac jönne létre a gyakorlatban. Ezek az eltérő nemzeti megközelítések jelentős visszaesést okozhatnak a digitális egységes piac megvalósítása terén, lelassítva vagy megakadályozva a kapcsolódó pozitív növekedési és munkahelyteremtési hatásokat, amennyiben Unió szinten nem történnek megfelelő lépések.

A fenti fejleményeket alapul véve a rendeletjavaslat létrehozza az európai kiberbiztonsági tanúsítási keretrendszert (a továbbiakban: keretrendszer) az IKT-termékekre és -szolgáltatásokra vonatkozóan, és meghatározza az ENISA alapvető funkcióit és feladatait a kiberbiztonsági tanúsítás területén. A jelenlegi javaslat meghatározza az európai kiberbiztonsági tanúsítási rendszerekre vonatkozó szabályok átfogó keretrendszerét. Nem vezet be közvetlenül működőképes tanúsítási rendszereket, ehelyett keretrendszert alakít ki bizonyos IKT-termékekre/-szolgáltatásokra vonatkozó egyedi tanúsítási rendszerek (európai kiberbiztonsági tanúsítási rendszerek) létrehozása számára. Az európai kiberbiztonsági tanúsítási rendszerek keretrendszerrel összhangban történő létrehozása lehetővé teszi majd egyfelől, hogy az ilyen rendszerek részeként kiállított tanúsítványok minden tagállamban érvényesek legyenek, illetve minden tagállam elismerje őket, másfelől, hogy kezelje a piac jelenlegi szétagoltságát.

Az európai kiberbiztonsági tanúsítási rendszer általános célja annak igazolása, hogy az ilyen rendszernek megfelelően tanúsított IKT-termékek és -szolgáltatások megfelelnek a meghatározott kiberbiztonsági követelményeknek. Ebbe beletartozna például a (tárolt, továbbított vagy más módon feldolgozott) adatok védelmének képessége a véletlen vagy illetéktelen tárolással, feldolgozással, hozzáféréssel, nyilvánosságra hozatallal, megsemmisítéssel, véletlen elvesztéssel vagy módosítással szemben. Az Unió kiberbiztonsági tanúsítási rendszerei a meglévő szabványokra hagyatkoznak azon technológiai

követelményekhez és értékelő eljárásokhoz kapcsolódóan, amelyeknek a termékeknek meg kell felelniük, és nem saját technológiai szabványokat dolgoznának ki<sup>16</sup>. Egy, az Unió egészére szóló terméktanúsítás, például az intelligens kártyákra vonatkozóan, amelyeket jelenleg a többoldalú (korábban már bemutatott) SOG-IS rendszerben, nemzetközi, közös kritériumokon alapuló szabványok alapján tesztelnek, azt jelentené, hogy a rendszer az egész Unióban érvényes.

A konkrét európai kiberbiztonsági tanúsítási rendszer kialakításánál figyelembe veendő konkrét biztonsági célkitűzések meghatározása mellett a javaslat előírja az ilyen rendszerek minimális tartalmi jellemzőit. Az ilyen rendszereknek többek között számos olyan konkrét elemet kell meghatározniuk, amelyek felvázolják a kiberbiztonsági tanúsítás hatályát és tárgyát. Ez magában foglalja az érintett termékek és szolgáltatások kategóriáinak azonosítását, a kiberbiztonsági követelmények részletes leírását (például a vonatkozó szabványokra vagy műszaki előírásokra való hivatkozással), a konkrét értékelési kritériumokat és módszereket, valamint a biztonság elérendő szintjét (alapvető, jelentős vagy magas).

Az európai kiberbiztonsági tanúsítási rendszereket az ENISA dolgozza ki az európai kiberbiztonsági tanúsítási csoport segítségével és megerősített együttműködésével (lásd alább), és végrehajtási jogi aktusok révén a Bizottság fogadja el. Ha igény merül fel egy kiberbiztonsági tanúsítási rendszer iránt, a Bizottság felkéri az ENISA-t, hogy dolgozza ki azt a konkrét IKT-termékekre vagy -szolgáltatásokra vonatkozóan. Az ENISA megerősített együttműködés keretében dolgozik majd együtt a csoportban képviselttel rendelkező nemzeti tanúsításfelügyeleti hatóságokkal. A tagállamok és a csoport javasolhatják a Bizottság számára, hogy kérje fel az ENISA-t egy adott rendszer elkészítésére.

A tanúsítási eljárás igen költséges lehet, ami magasabb árakat eredményezhet az ügyfelek és a fogyasztók számára. A tanúsítás iránti igény jelentős különbségeket mutathat a termékek és szolgáltatások sajátos felhasználási környezetétől és a technológiai változások gyors ütemétől függően. Az európai kiberbiztonsági tanúsítás igénybevételének ezért továbbra is önkéntesnek kell maradnia, kivéve, ha az IKT-termékek és -szolgáltatások biztonsági követelményeit előíró uniós vagy nemzeti jogszabályok erről eltérően rendelkeznek.

A harmonizáció biztosítása és a szétagoltság elkerülése érdekében azonban az európai kiberbiztonsági tanúsítási rendszer hatálya alá tartozó IKT-termékek és -szolgáltatások nemzeti kiberbiztonsági tanúsítási rendszereit vagy eljárásait a rendszer elfogadásáról szóló végrehajtási jogi aktusban megállapított időponttól nem alkalmazzák majd. A tagállamok továbbá nem vezethetnek be új nemzeti kiberbiztonsági tanúsítási rendszereket a meglévő európai kiberbiztonsági tanúsítási rendszer hatálya alá tartozó IKT-termékekre és -szolgáltatásokra vonatkozóan.

Az európai kiberbiztonsági tanúsítási rendszer elfogadását követően az IKT-termékek gyártói és az ilyen szolgáltatásokat kínáló szolgáltatók a termékeik vagy szolgáltatásaik tanúsítására irányuló kérelmet benyújthatják majd az általuk választott megfelelőségértékelő szervezetnek. A megfelelőségértékelő szervezeteket egy akkreditáló testületnek kell akkreditálnia, amennyiben azok megfelelnek bizonyos meghatározott követelményeknek. Az akkreditációt legfeljebb ötéves időtartamra adják meg, és az azonos feltételek mellett mindaddig megújítható, ameddig az adott megfelelőségértékelő szervezet teljesíti a meghatározott követelményeket. Az akkreditáló testületek visszavonják a megfelelőségértékelő szervezet akkreditációját, amennyiben az akkreditáció feltételei nem vagy már nem teljesülnek, illetve, ha a szervezet által hozott intézkedések megsértik e rendelet rendelkezéseit.

<sup>16</sup> Az európai szabványok esetében ez az európai szabványügyi szerveken keresztül történik, amit az Európai Bizottság a Hivatalos Lapban való közzététellel megerősít (lásd az 1025/2012/EU rendeletet).

A javaslat szerint az ellenőrzési, felügyeleti és végrehajtási feladatok a tagállamokra hárulnak. A tagállamoknak létre kell hozniuk egy tanúsításfelügyeleti hatóságot. A hatóság feladata lesz felügyelni, hogy a megfelelőségértékelő szervezetek, valamint a tagállam területén letelepedett ilyen szervezetek által kiállított tanúsítványok megfelelnek-e a rendelet előírásainak és a vonatkozó európai kiberbiztonsági tanúsítási rendszereknek. A nemzeti tanúsításfelügyeleti hatóságok illetékesek a tagállam területén letelepedett megfelelőségértékelő szervezetek által kiállított tanúsítványokkal kapcsolatos, természetes és jogi személyek által benyújtott panaszok kezelésére. A megfelelő mértékig kivizsgálják a panasz tárgyát, és észszerű határidőn belül tájékoztatják a panaszost a fejleményekről és a vizsgálat eredményéről. Ezen túlmenően együttműködnek a többi tanúsításfelügyeleti hatósággal vagy más hatóságokkal, például olyan módon, hogy megosztják az e rendelet előírásainak, illetve a konkrét európai kiberbiztonsági tanúsítási rendszereknek esetlegesen meg nem felelő IKT-termékekkel és -szolgáltatásokkal kapcsolatos információkat.

Végül pedig a javaslat létrehozza az európai kiberbiztonsági tanúsítási csoportot (a továbbiakban: csoport), amely az egyes tagállamok nemzeti tanúsításfelügyeleti hatóságaiból áll. A csoport fő feladata, hogy tanácsot adjon a Bizottságnak a kiberbiztonsági tanúsítási politikát érintő kérdésekben, és együttműködjön az ENISA-val az európai kiberbiztonsági tanúsítási rendszerek tervezetének kidolgozásában. Az ENISA segíteni fogja a Bizottságot a csoport titkárságának biztosításában, és naprakész, a nyilvánosság számára elérhető nyilvántartást vezet majd az európai kiberbiztonsági tanúsítási keretrendszer részeként jóváhagyott rendszerekről. Az ENISA a szabványtestületekkel is kapcsolatot tartana fenn, hogy biztosítsa a jóváhagyott rendszerekben használt szabványok megfelelőségét, és hogy azonosítsa a kiberbiztonsági szabványokat igénylő területeket.

Az európai kiberbiztonsági tanúsítási keretrendszer (a továbbiakban: a keretrendszer) számos előnnyel jár majd a magánfelhasználók és a vállalkozások számára. Különösen a következőket kell megemlíteni:

- A konkrét termékekhez vagy szolgáltatásokhoz kapcsolódó átfogó uniós kiberbiztonsági tanúsítási rendszerek „egyablakos” mechanizmusként felfunkcionálnak majd a vállalatok számára az uniós kiberbiztonsági tanúsítás területén. Az ilyen vállalatoknak lehetőségük lesz arra, hogy csak egyszer tanúsíttassák terméküket, és ennek révén minden tagállamban érvényes tanúsítványt szerezzenek. Nem kötelezik majd őket arra, hogy újból elvégeztessék a terméktanúsítást a különböző nemzeti tanúsító szerveknél. Mindez jelentősen csökkenti majd a vállalatok költségeit, elősegíti a határokon átnyúló tevékenységeket, és végső soron csökkenti és megakadályozza az érintett termékek belső piacának széttagoltságát.
- A keretrendszer elsőbbséget ad az európai kiberbiztonsági tanúsítási rendszereknek a nemzeti rendszerekkel szemben: e szabály értelmében egy európai kiberbiztonsági tanúsítási rendszer elfogadása minden létező párhuzamos nemzeti rendszert hatályon kívül helyez ugyanazokra az adott biztonsági szinttel rendelkező IKT-termékekre és -szolgáltatásokra vonatkozóan. Mindez még átláthatóbbá teszi a rendszert azáltal, hogy csökkenti az egymást átfedő vagy esetlegesen egymásnak ellentmondó nemzeti kiberbiztonsági tanúsítási rendszerek jelenlegi terjedését.
- A javaslat támogatja és kiegészíti a kiberbiztonsági irányelv végrehajtását olyan módon, hogy az irányelv hatálya alá tartozó vállalatokat egy nagyon hasznos eszközzel látja el annak igazolására, hogy az Unió egészében megfelelnek a hálózati és információbiztonsággal kapcsolatos előírásoknak. Az új kiberbiztonsági tanúsítási rendszerek kidolgozásakor a Bizottság és az ENISA különös figyelmet fog fordítani

arra az igényre, hogy biztosítsa, hogy a hálózat- és információbiztonsági követelmények visszaköszöjenek az ilyen rendszerekben.

- A javaslat az IKT-termékek és -szolgáltatások uniós kiberbiztonsági tanúsításához szükséges feltételek és alapvető követelmények harmonizálása révén támogatni fogja és elősegíti az európai kiberbiztonsági politika kidolgozását. Az európai kiberbiztonsági tanúsítási rendszerek közös szabványokat, illetve az értékelési és vizsgálati módszerek közös kritériumait fogják tartalmazni. Ez jelentősen – bár közvetetten – hozzá fog járulni a közös biztonsági megoldások elterjedéséhez az Unióban, és ilyen módon a belső piacot akadályozó tényezőket is felszámolja.
- A keretrendszer jellegéből adódóan biztosítja a szükséges rugalmasságot a kiberbiztonsági tanúsítási rendszerek számára. A konkrét kiberbiztonsági igényektől függően a termék- vagy szolgáltatástanúsítás magasabb vagy alacsonyabb biztonsági szinten is elvégezhető. Az európai kiberbiztonsági tanúsítási rendszereket ezt a rugalmasságot szem előtt tartva kell megtervezni, és ezért különböző biztonsági szinteket (azaz alapvető, jelentős vagy magas biztonsági szintet) garantálnak, így különböző célokra, illetve különböző környezetekben lehet használni őket.
- A fent említett elemek az IKT-termékek és -szolgáltatások kiberbiztonsági szintje kommunikációjának hatékony eszközeként vonzóbbá teszik majd a kiberbiztonsági tanúsítást a vállalkozások számára. Ha a kiberbiztonsági tanúsítás olcsóbbá, hatékonyabbá és kereskedelmi szempontból vonzóbbá válna, a vállalkozások nagyobb kedvet kapnának termékeik kiberbiztonsági kockázatokkal szembeni tanúsítására, és ilyen módon hozzájárulnának a hatékonyabb kiberbiztonsági gyakorlatok elterjedéséhez az IKT-termékek és -szolgáltatások tervezésében (beépített kiberbiztonság).

- **Összhang a szabályozási terület jelenlegi rendelkezéseivel**

A kiberbiztonsági irányelv értelmében a gazdaságunk és a társadalmunk számára létfontosságú ágazati szereplők, például az energiaipari, a közlekedés- és vízügyi, a banki szolgáltatók, a pénzügyi piaci infrastruktúra, az egészségügyi és a digitális infrastruktúra szereplői, valamint a digitális szolgáltatók (pl. a keresőmotorok, felhőalapú számítástechnikai szolgáltatások és az online piacterek) kötelesek intézkedéseket tenni a biztonsági kockázatok megfelelő kezelése érdekében. E javaslat új szabályai kiegészítik a kiberbiztonsági irányelv rendelkezéseit, és biztosítják a velük való összhangot annak érdekében, hogy tovább növeljék az Unióban a kibertámadásokkal szembeni ellenálló képességet fokozott képességek, együttműködés, kockázatkezelés és a kiberbiztonsággal kapcsolatos tudatosság révén.

Ezen túlmenően a kiberbiztonsági tanúsításra vonatkozó szabályok alapvető fontosságú eszközök a kiberbiztonsági irányelv hatálya alá tartozó vállalatok számára, mivel azok így képesek lesznek IKT-termékeik és -szolgáltatásaik tanúsítását elvégezni a kiberbiztonsági kockázatokkal szemben az Unió egészében érvényes és elismert kiberbiztonsági tanúsítási

rendszerek alapján. Emellett kiegészítik az eIDAS-rendeletben<sup>17</sup> és a rádióberendezésekről szóló irányelvben<sup>18</sup> említett biztonsági követelményeket.

- **Összhang az Unió egyéb szakpolitikáival**

Az (EU) 2016/679 rendelet (általános adatvédelmi rendelet, „GDPR”)<sup>19</sup> rendelkezéseket ír elő a tanúsítási mechanizmusok és adatvédelmi bélyegzők, illetve jelölések létrehozására vonatkozóan, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek e rendelet előírásainak. Jelen rendelet nem érinti az adatfeldolgozási műveletek általános adatvédelmi rendelet szerinti tanúsítását, még akkor sem, ha az ilyen műveletek termékekbe és szolgáltatásokba vannak beágyazva.

A rendeletjavaslat biztosítani fogja az összeegyeztethetőséget az akkreditálás és piacfelügyelet előírásáról szóló 765/2008/EK rendelettel<sup>20</sup> azáltal, hogy hivatkozik az említett keretrendszer nemzeti akkreditáló testületekre és megfelelőségértékelő szervezetekre vonatkozó szabályaira. Ami a felügyeleti hatóságokat illeti, a rendeletjavaslat előírja a tagállamok számára, hogy a szabályok felügyeletéért, nyomon követéséért és végrehajtásáért felelős nemzeti felügyeleti hatóságokat jelöljön ki. Ezeknek a szervezeteknek a 765/2008/EK rendeletben előírtak szerint a megfelelőségértékelési szervektől különálló szervezeteknek kell maradniuk.

## **2. JOGALAP, SZUBSZIDIARITÁS ÉS ARÁNYOSSÁG**

- **Jogalap**

Az uniós fellépés jogalapja az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikke, amely a tagállamok jogszabályainak közelítését tárgyalja, amely harmonizáció célja az EUMSZ 26. cikkében említett célkitűzések, nevezetesen a belső piac megfelelő működésének elérése.

A Bíróság (Egyesült Királyság kontra Európai Parlament és Tanács ügy, C-217/04) megerősítette az ENISA létrehozásának belső piaci jogalapját, amelyet az Ügynökség jelenlegi megbízatását megállapító 2013-as rendelet tovább erősített. Ezen túlmenően azok a tevékenységek, amelyek a tagállamok közötti együttműködés és koordináció növelésére irányuló célkitűzéseket tükrözik, illetve amelyek uniós szintű képességekkel bővítik a tagállamok fellépését, az operatív együttműködés kategóriájába tartoznak. A kiberbiztonsági irányelv (amelynek az EUMSZ 114. cikke a jogalapja) kifejezetten ezt határozza meg elérendő célként a CSIRT-hálózattal összefüggően, amelyben az „ENISA biztosítja a titkárságot, és aktívan támogatja a CSIRT-ek közötti együttműködést” (a 12. cikk

<sup>17</sup> 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.

<sup>18</sup> Az Európai Parlament és a Tanács 2014/53/EU irányelve (2014. április 16.) a rádióberendezések forgalmazására vonatkozó tagállami jogszabályok harmonizációjáról és az 1999/5/EK irányelv hatályon kívül helyezéséről.

<sup>19</sup> 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., 1–88. o.).

<sup>20</sup> 765/2008/EK rendelet a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről.

(2) bekezdése). A 12. cikk (3) bekezdésének f) pontja részletesen felvázolja az operatív együttműködés további formáinak meghatározását a CSIRT-hálózat feladataként, többek között az alábbiakkal kapcsolatban: i. a kockázatok és biztonsági események kategóriái; ii. korai előrejelzés; iii. kölcsönös segítségnyújtás; valamint iv. a koordináció elvei és módjai olyan esetekben, amikor a tagállamok határokon átnyúló kockázatokra és biztonsági eseményekre reagálnak.

- Az IKT-termékek és -szolgáltatások tanúsítási rendszereinek jelenlegi összehangolatlansága a tagállamokra nézve jogilag kötelező erejű és hatékony közös keretprogram hiányából is adódik. Ez gátolja az IKT-termékek és -szolgáltatások belső piacának létrejöttét, és akadályozza az európai ipar versenyképességét az ágazatban. E javaslat célja a meglévő széttagoltság és a kapcsolódó belső piaci akadályok kezelése azáltal, hogy közös keretrendszert biztosít az Unió egészében érvényes kiberbiztonsági tanúsítási rendszerek létrehozására.

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

A szubszidiaritás elve megköveteli az uniós fellépés szükségességének és hozzáadott értékének értékelését. A szubszidiaritás tiszteletben tartását már a jelenleg hatályos ENISA-rendelet<sup>21</sup> elfogadásakor elismerték.

A kiberbiztonság közös uniós érdek. A hálózatok és az információs rendszerek kölcsönös függése olyan jellegű, hogy az egyes szereplők (köztük az állami és a magánszféra szereplői, a magánfelhasználókat is ideértve) gyakran nem képesek elszigetelten szembenézni a fenyegetésekkel, kezelni a kockázatokat és a kiberbiztonsági események lehetséges hatásait. Egyfelől a tagállamokat érintő, a kritikus infrastruktúrák (a teljesség igénye nélkül az energia, a közlekedés és a víz) működtetését is befolyásoló kölcsönös függés nemcsak előnyössé, de szükségessé is teszi az európai szintű állami beavatkozást. Másfelől az uniós beavatkozás kedvező „továbbgyűrűző” hatással járhat a bevált gyakorlatok tagállamok közötti megosztása révén, ami az Unió fokozott kiberbiztonságát eredményezheti.

Összefoglalva, a jelenlegi helyzetben és a jövőbeni forgatókönyveket vizsgálva úgy tűnik, hogy az Unió kibertámadásokkal szembeni kollektív ellenálló képességének növeléséhez nem elegendők az uniós tagállamok egyedi fellépései és a kiberbiztonságra alkalmazott összehangolatlan megközelítés.

A jelenlegi kiberbiztonsági tanúsítási rendszerek összehangolatlanságának kezeléséhez is szükség van az uniós fellépésre. Az ilyen fellépés lehetővé tenné a gyártók számára, hogy a belső piac minden előnyével éljenek és jelentős költségmegtakarítást érjenek el a tesztelés és áttervezés területén. Noha a vezető tisztviselők információs rendszerek biztonságával foglalkozó csoportjának (SOG-IS) jelenlegi kölcsönös elismerési megállapodása például jelentős eredményeket ért el ebben a tekintetben, olyan fontos korlátokra is rámutatott, amelyek akadályozzák azt, hogy hosszabb távon alkalmasak legyen fenntartható megoldásokat nyújtani a belső piac teljes potenciáljának megvalósítását illetően.

A 2016. évi tanácsi következtetések<sup>22</sup> elismerik az uniós szintű fellépés hozzáadott értékét, egyfelől különösen a tagállamok közötti, másfelől a hálózat- és információbiztonsági

<sup>21</sup> Az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Unió Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről.

<sup>22</sup> A Tanács következtetései Európa kibertámadásokkal szembeni ellenálló képességének erősítéséről, valamint a versenyképes és innovatív kiberbiztonsági ágazat támogatásáról – 2016. november 15.



közösségek közötti együttműködés fokozása szempontjából, amely hozzáadott értékre az ENISA értékelése is egyértelműen rámutat.

- **Arányosság**

A javasolt intézkedések nem lépik túl a szakpolitikai célkitűzések eléréséhez szükséges mértéket. Ezen túlmenően az uniós beavatkozás hatálya nemzetbiztonsági kérdésekben nem akadályoz semmilyen további nemzeti fellépést. A szubszidiaritás és arányosság elve alapján ezért indokolt az uniós szintű fellépés.

- **A jogi aktus típusának megválasztása**

Ez a javaslat az 526/2013/EU rendeletet vizsgálja felül, amely meghatározza az ENISA jelenlegi megbízatását és feladatait. Továbbá, tekintettel arra, hogy az ENISA fontos szerepet játszik az Unió kiberbiztonsági tanúsítási keretrendszerének kialakításában és irányításában, új megbízatását és az említett keretrendszert egyetlen jogi eszközbe célszerű foglalni, amire a rendelet a legalkalmasabb eszköz.

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

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

A Bizottság az értékelési ütemtervnek<sup>23</sup> megfelelően az Ügynökség relevanciáját, hatását, eredményességét, hatékonyságát, koherenciáját és uniós hozzáadott értékét vizsgálta a 2013–2016 közötti teljesítménye, irányítása, belső szervezeti felépítése és munkamódszerei viszonylatában. A főbb megállapítások összefoglalása az alábbiakban olvasható (további információért lásd a témával foglalkozó, hatásvizsgálatot kísérő bizottsági szolgálati munkadokumentumot).

- **Relevancia:** figyelembe véve a technológiai fejlődést, a kialakuló fenyegetéseket és a fokozott kiberbiztonság iránti megnövekedett igényt az Unióban, az ENISA célkitűzései relevánsnak bizonyultak. A tagállamok és az Unió szervei valóban számítanak az Ügynökség kiberbiztonsági ügyekben rendelkezésre álló jelentős tapasztalatára. A tagállamokban ezen túlmenően kapacitásokat kell kialakítani a fenyegetések jobb megértése és az azokra való reagálás érdekében, a tematikus területek és intézmények érdekeltjeinek pedig együtt kell működniük. A kiberbiztonság továbbra is az Unió kulcsfontosságú szakpolitikai prioritása marad, amellyel kapcsolatban számítani lehet az ENISA reagálására; az ENISA határozott idejű megbízatással rendelkező uniós ügynökségként való működése azonban: i. nem teszi lehetővé a hosszú távú tervezést, valamint a tagállamok és uniós intézmények fenntartható támogatását; ii. joghézagot eredményezhet, mivel a kiberbiztonsági irányelv rendelkezései tartós jellegű<sup>24</sup> feladatokat bízna az ENISA-ra; iii. nincs összhangban azzal az elképzeléssel, amely fokozott uniós kiberbiztonsági ökoszisztémához kapcsolja az ENISA-t.

<sup>23</sup> [http://ec.europa.eu/smart-regulation/roadmaps/docs/2017\\_cnect\\_002\\_evaluation\\_enisa\\_en.pdf](http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf)

<sup>24</sup> Utalás a hálózati és információs rendszerek biztonságáról szóló irányelv (kiberbiztonsági irányelv) 7., 9., 11., 12. és 19. cikkére.

- **Eredményesség:** Az ENISA általánosságban véve teljesítette célkitűzéseit és végrehajtotta feladatait. Főbb tevékenységei (kapacitásépítés, szakértelem biztosítása, közösségépítés és a szakpolitika támogatása) révén hozzájárult ahhoz, hogy fejlettebb hálózat- és információbiztonság valósuljon meg Európában. Mindazonáltal minden említett területen van még hova fejlődni. Az értékelés arra a következtetésre jutott, hogy az ENISA hatékony, szoros és bizalomteljes kapcsolatot alakított ki egyes érdekelt felekkel, különösen a tagállamokkal és a CSIRT-ek közösségével. A kapacitásépítés terén végrehajtott beavatkozásokat különösen a kevesebb erőforrással rendelkező tagállamok esetében találták eredményesnek. A széles körű együttműködés ösztönzése az Ügynökség egyik fő erőssége: az érdekelt felek nagy többsége egyetért abban, hogy az ENISA pozitív szerepet játszik az együttműködés elősegítésében. Az ENISA-nak azonban nehézséget okozott, hogy jelentős hatást érjen el a hálózat- és információbiztonság tágabb területén. Ez részben annak is köszönhető, hogy a több részterületet érintő megbízatásához csak nehézségek árán talált emberi- és pénzügyi erőforrásokat. Az értékelés azt is megállapította, hogy az ENISA csak részben teljesítette a szakértelem biztosítására irányuló célkitűzését, ami a szakértők toborzásával kapcsolatos problémáknak tudható be (lásd még a hatékonyságot tárgyaló szakaszban).
- **Hatékonyság:** Kis költségvetése ellenére (amely a legalacsonyabbak között van az uniós ügynökségek között) az Ügynökség hozzá tudott járulni kitűzött céljaihoz, ami összességében azt mutatja, hogy hatékonyan gazdálkodik erőforrásaival. Az értékelés megállapította, hogy a folyamatok általánosságban véve hatékonyak bizonyultak, és az, hogy a szervezeten belül egyértelműen meghatározták a felelősségi köröket, azt eredményezte, hogy az Ügynökség megfelelően hajtotta végre feladatait. Az Ügynökség hatékonyságának egyik fő kihívása az volt, hogy nehezen sikerült szakképzett személyzetet találnia és azt megtartania. Az értékelés megállapításai szerint ez több tényező kombinációjával magyarázható, köztük azzal, hogy a közszeaktor számára általánosságban nehézséget jelent, hogy versenyre keljen a magánszeaktorral a magasan képzett szakértők alkalmazásában, az Ügynökség leginkább határozott idejű szerződéseket tud ajánlani a jelentkezőknek, illetve az ENISA elhelyezkedése csak keveseket vonzott, ami például a házastársak munkavállalási nehézségeiből is fakadt. További koordinációs erőfeszítéseket és többletköltségeket igényelt az Ügynökség helyszíneinek Athén és Iráklío közötti megosztása, azonban az, hogy a fő operatív részleget 2013-ban Athénba költöztették, növelte az Ügynökség működési hatékonyságát.
- **Koherencia:** Az ENISA tevékenységei általában véve összeegyeztethetők az érdekeltek politikáival és tevékenységeivel nemzeti és uniós szinten, ez utóbbi szintjén azonban összehangoltabb megközelítésre van szükség a kiberbiztonság területén. Az ENISA és a többi uniós szerv közötti együttműködés lehetőségeit nem használják ki teljes mértékben. Az Unió jogi és politikai helyzetének alakulása miatt most kevésbé koherens az Ügynökség jelenlegi megbízatása.
- **Unió hozzáadott érték:** Az ENISA hozzáadott értéke elsősorban azon képességében rejlik, hogy nemcsak a tagállamok között, hanem a kapcsolódó hálózat- és információbiztonsági közösségek között is meg tudja erősíteni az együttműködést. Uniós szinten az ENISA az egyetlen olyan szereplő, amelyik ilyen sokféle érdekelt együttműködését támogatja a hálózat- és információbiztonság területén. Az Ügynökség által nyújtott hozzáadott érték az érdekelt felek eltérő szükségleteinek és erőforrásainak megfelelően (pl. a nagy és kis tagállamok igényei; vagy a tagállamok és az ipar igényei közötti különbségek), valamint az Ügynökség tevékenységeinek

munkaprogram szerinti rangsorolását figyelembe véve eltérő volt. Az értékelés megállapította, hogy az ENISA esetleges megszüntetésével a tagállamok egy jó lehetőséget szalasztanak el. Az Ügynökség hiányában nem biztos, hogy a közösségépítés és a tagállamok közötti együttműködés ugyanilyen szinten zajlana a kiberbiztonság terén. Centralizált uniós ügynökség nélkül az összkép sokkal széttagoltabb lenne, és kétoldalú vagy regionális együttműködés töltené ki az ENISA által hagyott űrt.

Különös figyelmet fordítva az ENISA eddig elért és jövőbeli teljesítményére, a 2017. évi konzultáció alapján az alábbiak állapíthatók meg az Ügynökség munkájáról<sup>25</sup>:

- Az ENISA 2013 és 2016 között nyújtott teljesítményét általánosságban véve a válaszadók többsége (74 %) pozitívan értékelte. A válaszadók nagy része (az egyes célok esetében legalább 63 %) ezenfelül úgy vélte, hogy az ENISA teljesítette különböző céljait. A válaszadók mintegy fele (46 %-a) rendszeresen (havonta vagy még gyakrabban) igénybe veszi az ENISA szolgáltatásait és termékeit, 83 %-uk értékeli, hogy ezek uniós szintű szervtől származnak, 62 %-uk pedig elégedett a minőségükkel.
- A válaszadók számos hiányosságot és problémát azonosítottak az Unió kiberbiztonságának jövőjét illetően, ezek közül az öt legfontosabb (egy 16 elemet tartalmazó listából): a tagállamok közötti együttműködés; a nagy léptékű kibertámadások megelőzésére, észlelésére és megoldására alkalmas kapacitás; a tagállamok közötti együttműködés a kiberbiztonsággal kapcsolatos ügyekben; a különböző érdekelttek közötti együttműködés és információmegosztás, a köz- és a magánszféra közötti együttműködést is ideértve; a kritikus infrastruktúra védelme a kibertámadásokkal szemben.
- A válaszadók nagy többsége (88 %) úgy vélte, hogy az uniós szinten rendelkezésre álló jelenlegi eszközök és mechanizmusok nem megfelelőek vagy csak részben jelentenek megoldást az említett problémák kezelésére. A válaszadók túlnyomó többsége (98 %) úgy véli, hogy szükség van egy uniós szervre az említett igények kiszolgálására, 99 %-uk pedig azt gondolja, hogy erre az ENISA a legalkalmasabb.

### **Konzultáció az érdekelt felekkel**

- A Bizottság nyilvános konzultációt tartott 2016. április 12-e és július 5-e között az ENISA értékelése kapcsán, amelynek során 421 válasz érkezett be<sup>26</sup>. Az eredmények alapján a válaszadók 67,5 %-a volt azon a véleményen, hogy az ENISA szerepet játszhatna az informatikai termékek és szolgáltatások biztonsági tanúsítását segítő harmonizált keretrendszer létrehozásában.

<sup>25</sup> 19 tagállamból 90 érdekelt fél (88 válasz és 2 állásfoglalás érkezett), köztük 15 tagállam (egyebek mellett Franciaország, Olaszország, Írország és Görögország) nemzeti hatóságai és nyolc, az európai vállalkozások jelentős részét képviselő ernyőszervezet reagált a megkeresésre, így például az Európai Bankszövetség, a Digitális Európa (az európai digitális technológiai ágazatot képviselve) és az Európai Távközlési Hálózatüzemeltetők Egyesülete (ETNO). Az ENISA nyilvános konzultációja számos további információforrással egészült ki, például: i. részletes interjúk a kiberbiztonsági közösség mintegy 50 kulcsfontosságú szereplőjével; ii. a CSIRT-hálózatnak készített felmérés; iii. az ENISA igazgatótanácsának, felügyelőtestületének és érdekeltjei állandó csoportjának készített felmérés.

<sup>26</sup> 162 válasz érkezett magánfelhasználóktól, 33 a civil társadalom szereplőitől és fogyasztói szervezetektől; 186 válasz érkezett az iparág képviselőitől és 40 közigazgatási szervektől, köztük az elektronikus hírközlési adatvédelmi irányelv végrehajtásában illetékes hatóságoktól.

A kiberbiztonsági szerződéses köz-magán társulással<sup>27</sup> összefüggő 2016. évi konzultáció eredményei a tanúsítással foglalkozó résszel kapcsolatban azt mutatják, hogy:

- A válaszadók 50,4 %-a (121-en a 240-ből) nincs tisztában azzal, hogy a nemzeti tanúsítási rendszereket kölcsönösen elismerik-e a tagállamokban. A válaszadók 25,8 %-a (62-en a 240-ből) „nemmel”, míg 23,8 %-a (57-en a 240-ből) „igennel” válaszolt.
- A válaszadók 37,9 % -a (91-en a 240-ből) úgy véli, hogy a meglévő tanúsítási rendszerek nem felelnek meg az európai ipar igényeinek. Másfelől 17,5 %-uk (42-en a 240-ből) ellentétes álláspontot képviseltek (főként az európai piacon működő nemzetközi vállalatok).
- A válaszadók 49,6 %-a (119-en a 240-ből) azt állítja, hogy nem könnyű megfeleltetni egymásnak a szabványokat, tanúsítási rendszereket és címkéket. A válaszadók 37,9 %-a (91-en a 240-ből) azt válaszolta, hogy nem tudja, és mindössze 12,5 %-a (30-an a 240-ből) válaszolt „igennel”.

### **Szakértői vélemények összegyűjtése és felhasználása**

A Bizottság az alábbi független szakértők tanácsaira támaszkodott:

- tanulmány az ENISA értékeléséről (Ramboll/Carsa 2017; SMART 2016/0077);
- tanulmány „ICT Security Certification and labelling – Evidence gathering and impact assessment” címen (PriceWaterhouseCoopers 2017; SMART 2016/0029).

### **Hatásvizsgálat**

- A kezdeményezésről szóló hatásvizsgálati jelentés a következő fő problémákat tárta fel, amelyeket orvosolni kell:
- a kiberbiztonsági politikák és megközelítések összehangolatlansága a tagállamokban;
- szerteágazó erőforrások és összehangolatlan megközelítések a kiberbiztonsággal kapcsolatosan az uniós intézményekben, hivataloknál és szerveknél; valamint
- a magánfelhasználók és vállalatok nem megfelelő tájékozottsága, valamint egyre több nemzeti és ágazati tanúsítási rendszer megjelenése.

A jelentés az ENISA megbízatásával kapcsolatban a következő lehetséges lehetőségeket értékelte:

- a fennálló állapot megőrzése, azaz egy kibővített, ám időben továbbra is korlátozott megbízatással (alapfogatókönyv);
- az ENISA jelenlegi megbízatásának lejárta megújítása nélkül és az ENISA megszüntetése (nincs politikai beavatkozás);
- az ENISA megreformálása; valamint
- egy uniós kiberbiztonsági ügynökség létrehozása teljes operatív képességekkel.

<sup>27</sup>

240 érdekelt adott választ a nemzeti közigazgatás, a nagyvállalatok, a kkv-k, a mikrovállalkozások és a kutatási szervek képviselői közül a tanúsítással kapcsolatos szakasz kérdéseire.

A jelentés a kiberbiztonsági tanúsítással kapcsolatban a következő lehetséges lehetőségeket értékelte:

- nincs politikai beavatkozás (alapforgatókönyv);
- nem jogalkotási (ún. puha jogi) intézkedések;
- olyan uniós jogalkotási aktus, amely a SOG-IS rendszeren alapuló kötelező rendszert hoz létre valamennyi tagállam számára; valamint
- uniós általános informatikai kiberbiztonsági tanúsítási keretrendszer kialakítása.

Az elemzés arra a következtetésre jutott, hogy az ENISA megreformálása egy uniós általános informatikai kiberbiztonsági tanúsítási keretrendszerrel kombinálva az előnyben részesített lehetőség.

E két lehetőség együttes alkalmazása tűnik a leghatékonyabb módszernek ahhoz, hogy az EU elérhesse a kitűzött célokat: azaz fokozza a kiberbiztonsági képességeket, a felkészültséget, az együttműködést, a tudatosságnövelést, az átláthatóságot, és megelőzze a piac széttagozottságát. Az értékelés szerint az uniós kiberbiztonsági stratégiában és a kapcsolódó szakpolitikákban (például a kiberbiztonsági irányelvben), valamint a digitális egységes piaci stratégiában meghatározott politikai prioritásokkal is ez a megoldás van leginkább összhangban. A konzultációs folyamat során az is kiderült, hogy az előnyben részesített megoldás az érdekelt felek többségének támogatását élvezi. Emellett a hatásvizsgálati elemzés tanúsága szerint ezzel a megoldással az erőforrások észszerű felhasználása mellett lehet elérni a kitűzött célokat.

A Bizottság Szabályozói Ellenőrzési Testülete július 24-én eredetileg kedvezőtlen véleményt adott ki, de azt a hatásvizsgálat újbóli beterjesztése után 2017. augusztus 25-én kedvezőre változtatta. A módosított hatásvizsgálati jelentés további alátámasztó bizonyítékokkal, az ENISA értékelésével kapcsolatos végleges megállapításokkal, valamint a szakpolitikai alternatívákhoz és hatásaikhoz fűzött további magyarázatokkal gazdagodott. A végleges hatásvizsgálati jelentés 1. melléklete összefoglalást nyújt arról, hogy a Testület második véleményében tett észrevételei miként kerültek figyelembevételre. Különösen abban a tekintetben volt szükség a jelentés aktualizálására, hogy részletesebben bemutassa az uniós kiberbiztonsági összefüggéseket, ideértve az „Ellenálló képesség, elrettentés és védelem – erős kiberbiztonság kialakítása az EU-ban” című közös közleményben (JOIN(2017) 450) foglalt intézkedéseket, amelyek különös jelentőséggel bírnak az ENISA szempontjából: az EU kiberbiztonsági tervezetét és az Európai Kiberbiztonsági Kutatási és Kompetenciaközpontot – ez utóbbit az Ügynökség az EU kutatási szükségleteivel kapcsolatos tanácsadással fogja támogatni.

A jelentés kifejti, hogy az új feladatkörökre, a jobb munkakörülményekre és az ugyanezen a területen tevékenykedő uniós szervekkel való strukturális együttműködésre irányuló reform révén miként válik majd az Ügynökség vonzóbb munkáltatóvá, ami hozzá fog járulni a szakértők toborzásával kapcsolatos problémák megoldásához is. A jelentés 6. melléklete pedig az ENISA-val kapcsolatos szakpolitikai alternatívák költségbecslésének felülvizsgált változatát tartalmazza. Ami a tanúsítás témáját illeti, a felülvizsgált jelentés részletesebben kifejti és egy ábrával is illusztrálja a javasolt megoldást, és becsléseket ad az új tanúsítási keretrendszerrel kapcsolatos költségekről mind a tagállamok, mind a Bizottság vonatkozásában. A felülvizsgált jelentés azzal kapcsolatban is részletesebb magyarázattal szolgál, hogy miért az ENISA lett a keretrendszer meghatározó szereplője: ennek oka egyrészt az idevágó tapasztalataiban keresendő, másrészt pedig abban, hogy ez az egyetlen uniós szintű kiberbiztonsági ügynökség. Végezetül a tanúsítással kapcsolatos fejezetek is átdolgozásra kerültek annak érdekében, hogy világosabb legyen, mi a különbség a jelenlegi

SOG-IS rendszerhez képest, milyen előnyökkel járnak a különféle szakpolitikai alternatívák, és hogy a jóváhagyott európai tanúsítási rendszerben kerül majd meghatározásra, hogy milyen típusú IKT-termékek és -szolgáltatások fogják a tárgyát képezni.

## **Célravezető szabályozás és egyszerűsítés**

### *Tárgyaltalan*

### **Az alapvető jogokra gyakorolt hatás**

A kiberbiztonság alapvető szerepet játszik az egyének magánéletének és személyes adatainak az Európai Unió Alapjogi Chartájának 7. és 8. cikkének megfelelő védelmében. Kiberbiztonsági események esetén a magánélet és a személyes adatok védelme egyértelműen veszélynek van kitéve. A kiberbiztonság ezért a magánélet és a személyes adataink bizalmas kezelésének szükséges feltétele. Ebből a szempontból a javaslat – az európai kiberbiztonság megerősítésének céljával – a magánülethez és a személyes adatokhoz való alapvető jog védelmét szolgáló meglévő jogszabályok fontos kiegészítése. A kiberbiztonság az elektronikus hírközlés titkosságának védelme és ennél fogva a véleménynyilvánítás és a tájékozódás szabadságának és egyéb kapcsolódó jogok – például a gondolatszabadság, a lelkiismereti és a vallásszabadság – gyakorlásának szempontjából szintén fontos.

## **4. KÖLTSÉGVETÉSI VONZATOK**

*Lásd a pénzügyi részből szóló ismertetőt*

## **5. EGYÉB ELEMEK**

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

A Bizottság nyomon fogja követni a rendelet alkalmazását, és ötévente megküldi értékelési jelentését az Európai Parlament, a Tanács és az Európai Gazdasági és Szociális Bizottság számára. Az értékelési jelentések nyilvánosak lesznek, és részletesen ismertetik majd a rendelet tényleges alkalmazását és végrehajtását.

- **A javaslat egyes rendelkezéseinek részletes magyarázata**

A rendelet I. címe az általános rendelkezéseket tartalmazza: a tárgyat (1. cikk), a fogalommeghatározásokat (2. cikk), az egyéb uniós eszközökből, így például a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 európai parlamenti és tanácsi irányelvből (kiberbiztonsági irányelv), a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről szóló 765/2008/EK európai parlamenti és tanácsi rendeletből és az európai szabványosításról szóló 1025/2012/EU európai parlamenti és tanácsi rendeletből vett releváns fogalmakra való utalásokkal.

A rendelet II. címe az ENISA-hoz, azaz az Unió kiberbiztonsági ügynökségéhez kapcsolódó legfontosabb rendelkezéseket tartalmazza.

E cím I. fejezete ismerteti az Ügynökség megbízatását (3. cikk), célkitűzéseit (4. cikk) és feladatait (5–11. cikk).

A II. fejezet az ENISA szervezeti felépítését vázolja fel, és kulcsfontosságú rendelkezéseket tartalmaz szerkezetéről (12. cikk). Rendelkezik az igazgatótanács (1. szakasz, 13–17. cikk), a felügyelőtestület (2. szakasz, 18. cikk) összetételéről, az ügyvezető igazgatóról (3. szakasz, 19. cikk), szavazásuk szabályairól és funkcióikról. Ezen túlmenően az érdekelték állandó csoportjának összetételéről és szerepéről (4. szakasz, 20. cikk) is megállapít rendelkezéseket. Végül, de nem utolsósorban e fejezet 5. szakasza részletezi az Ügynökség működési szabályait, műveleti programozását, az összeférhetetlenséget, az átláthatóságot, a titoktartást és a dokumentumokhoz való hozzáférést is ideértve (21–25. cikk).

A III. fejezet az Ügynökség költségvetésének létrehozásáról és szerkezetéről (26. és 27. cikk), valamint a végrehajtását irányító szabályokról (28. és 29. cikk) szól. A fejezet kitér a csalás, a korrupció és az egyéb jogellenes tevékenységek elleni küzdelemre irányuló rendelkezésekre is (30. cikk).

A IV. fejezet az Ügynökség személyi állományával foglalkozik. A személyzeti szabályok, az alkalmazási feltételek, valamint a kiváltságok és mentességek általános rendelkezéseit (31. és 32. cikk) is magában foglalja. Részletezi továbbá az Ügynökség ügyvezető igazgatójának alkalmazását és kinevezését (33. cikk). Végül, de nem utolsósorban, magában foglalja a kirendelt nemzeti szakértőket, illetve az Ügynökség alkalmazásában nem álló egyéb személyzet (34. cikk) alkalmazását irányító rendelkezéseket.

Végül az V. fejezet az Ügynökségre vonatkozó általános rendelkezéseket tartalmazza. Meghatározza az Ügynökség jogállását (35. cikk), és rendelkezéseket állapít meg a felelősséggel, nyelvhasználati szabályokkal, a személyes adatok védelmével (36–38. cikk), valamint a minősített és nem minősített érzékeny adatokra vonatkozó biztonsági szabályokkal kapcsolatos kérdésekben (40. cikk). Ismerteti az Ügynökség harmadik országokkal és nemzetközi szervezetekkel való együttműködésére irányadó szabályokat (39. cikk). Végül, de nem utolsósorban az Ügynökség székhelyére és működési feltételeire, valamint az ombudsman által végzett igazgatási ellenőrzésre vonatkozó rendelkezéseket is tartalmazza (41. és 42. cikk).

A rendelet III. címe általános szabályként (*lex generalis*) létrehozza az európai kiberbiztonsági tanúsítási keretrendszert (a továbbiakban: keretrendszer) az IKT-termékekre és -szolgáltatásokra (1. cikk) vonatkozóan. A cím meghatározza az európai kiberbiztonsági tanúsítási rendszerek általános célját, amely annak garantálásában áll, hogy az IKT-termékek és -szolgáltatások megfeleljenek a konkrét kiberbiztonsági követelményeknek, azaz hogy meghatározott biztonsági szinten ellenálljanak az olyan cselekményeknek, amelyek veszélyeztetik a rajtuk tárolt, továbbított vagy kezelt adatok vagy a kapcsolódó funkciók és szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét és bizalmasságát (43. cikk). Ezen túlmenően felsorolja az európai kiberbiztonsági tanúsítási rendszerek által kezelendő biztonsági célkitűzéseket (45. cikk), például többek között az adatok védelmére való képességüket a véletlen vagy illetéktelen hozzáféréssel, nyilvánosságra hozatallal, megsemmisítéssel vagy módosítással szemben, valamint az ilyen rendszerek tartalmi elemeit, például az alkalmazási körük részletes meghatározását, a biztonsági célkitűzéseket, az értékelési kritériumokat stb. (47. cikk).

A III. cím meghatározza továbbá az európai kiberbiztonsági tanúsítási rendszerek fő joghatásait, nevezetesen i. a nemzeti szintű végrehajtási kötelezettséget és a tanúsítás önkéntes jellegét; ii. az európai kiberbiztonsági tanúsítási rendszerek érvénytelenítő hatását a nemzeti rendszerekre vonatkozóan ugyanazon termékek vagy szolgáltatások tekintetében (48. és 49. cikk).

A cím ezen túlmenően az európai kiberbiztonsági tanúsítási rendszerek elfogadási eljárását, valamint a Bizottság, az ENISA és az európai kiberbiztonsági tanúsítási csoportjának (a

továbbiakban: csoport) szerepét (44. cikk) is meghatározza. Végül pedig a megfelelőségértékelő szervezetekre (a rájuk vonatkozó követelményekkel, hatáskörökkel, feladatokkal), valamint a nemzeti tanúsításfelügyeleti hatóságokra, illetve a szankciókra vonatkozó rendelkezéseket is megállapítja.

Ez a cím rendelkezik a csoport létrehozásáról is, amely létfontosságú szerv, és amely a nemzeti tanúsításfelügyeleti hatóságok képviselőiből áll, akiknek fő feladata, hogy az ENISA-val közösen kidolgozzák az európai kiberbiztonsági tanúsítási rendszereket, és tanácsokkal lássák el a Bizottságot a kiberbiztonsági tanúsítási politikát érintő általános vagy konkrét kérdésekben.

A rendelet IV. címe a záró rendelkezéseket foglalja magában, amelyek a hatáskör-átruházás gyakorlatát, az értékelési követelményeket, a hatályon kívül helyezést és a jogutódlást, valamint a hatálybalépést tárgyalják.



## Javaslat

**AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE**

**az ENISA-ról, az „Európai Unió Kiberbiztonsági Ügynökségről”,  
az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és  
kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági  
jogszabály”)**

(EGT-vonatkozású szöveg)

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,  
tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 114. cikkére,  
tekintettel az Európai Bizottság javaslatára,  
a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,  
tekintettel az Európai Gazdasági és Szociális Bizottság véleményére<sup>28</sup>,  
tekintettel a Régiók Bizottságának véleményére<sup>29</sup>,  
rendes jogalkotási eljárás keretében,  
mivel:

- (1) A hálózati és információs rendszerek és a távközlési hálózatok és szolgáltatások létfontosságú szerepet töltenek be a társadalom működésében, és a gazdasági növekedés gerincét képezik. Az információs és kommunikációs technológiák sokrétű funkciókat ellátó összetett rendszerek alapjait képezik – ide tartozik például a társadalmi tevékenységek elősegítése, a gazdaság olajozott működésének lehetővé tétele olyan meghatározó szektorokban, mint az egészségügy, az energetika, a pénzügy és a közlekedés, valamint a belső piac működésének megkönnyítése.
- (2) A hálózati és információs rendszerek használata szerte az EU-ban széles körben elterjedt, mind a magánszemélyek, mind a vállalkozások, mind pedig a közigazgatási szervek körében. Folyamatosan nő azoknak a termékeknek és szolgáltatásoknak a száma, amelyek alapvető jellemzői a digitalizálás és a hálózatba rendeződés, és a dolgok internete is egyre elterjedtebbé válik, így a következő évtizedben várhatóan több millió, ha nem több milliárd összekapcsolt digitális eszközt fognak az EU-ban használatba venni. Egyre több berendezés kapcsolódik az internethez, de mivel ezen eszközök alapértelmezetten nincsenek megfelelő biztonsági és ellenálló képességi szintet biztosító elemekkel ellátva, kiberbiztonsági szempontból nem teljesen megbízhatók. A tanúsítás korlátozott használata következtében így sem az intézményi, sem a magánfelhasználók nem rendelkeznek kellő információval az IKT-termékek és -szolgáltatások kiberbiztonsági jellemzőiről, ami a digitális megoldásokba vetett bizalom megrendüléséhez vezethet.

<sup>28</sup> HL C [...], [...], [...] o.

<sup>29</sup> HL C [...], [...], [...] o.

- (3) Minél nagyobb méreteket ölt a digitalizálás és a hálózatba rendeződés, annál nagyobbak a kiberbiztonsági kockázatok is, melyek a társadalmat egészében véve sebezhetőbbé teszik a kiberfenyegetésekkel szemben, az egyes felhasználókra leselkedő veszélyeket pedig súlyosbítják, ideértve a kiszolgáltatott helyzetben lévő felhasználókat, például a gyerekeket is. A társadalmat fenyegető kockázatok csökkentése érdekében az uniós kiberbiztonság fokozására irányuló minden lehetséges intézkedést meg kell hozni azért, hogy a hálózati és információs rendszerek, a távközlési hálózatok, valamint a magánszemélyek, a közigazgatási szervek és a vállalkozások (a kkv-któl a kritikus infrastruktúrák üzemeltetőiig terjedő vállalkozói spektrum) által használt digitális termékek, szolgáltatások és eszközök jobban védve legyenek a kiberfenyegetésekkel szemben.
- (4) Egyre gyakoribbak a kibertámadások, és az összekapcsoltság következtében a kiberfenyegetéseknek és -támadásoknak egyre kiszolgáltatottabbá váló gazdaság és társadalom fokozottabb védelmet igényel. Míg a kibertámadások általában nem ismernek országhatárokat, a kiberbiztonsági hatóságok szakpolitikai válaszingázakódései, akárcsak a bünüldözési hatáskörök, túlnyomórésznt nemzeti szintűek. A nagyszabású kiberbiztonsági események az egész EU-ban megzavarhatják a legalapvetőbb szolgáltatások nyújtását. Ezért hatékony uniós szintű reagálásra és válságkezelésre van szükség, melynek alapját célirányos szakpolitikai intézkedések és az európai szolidaritást és kölcsönös segítségnyújtást szolgáló gazdagabb eszköztárnak kell képeznie. Ennek megfelelően a politika formálói, a gazdasági élet szereplői és a felhasználók számára egyaránt fontos, hogy megbízható uniós adatok alapján rendszeres értékelés készüljön az EU kiberbiztonságának és ellenálló képességének mindenkori helyzetéről, továbbá szisztematikus legyen a jövőben várható fejlemények, kihívások és fenyegetések előrejelzése uniós és globális szinten egyaránt.
- (5) Az Unió előtt álló egyre nagyobb kiberbiztonsági kihívások leküzdéséhez átfogó intézkedéscsomagra van szükség, amely a korábbi uniós fellépésekre épül, és előmozdítja az egymást kölcsönösen erősítő célkitűzéseket. Idetartozik az is, hogy fokozni kell a tagállamok és a vállalkozások képességeit és felkészültségét, valamint javítani kell az együttműködést és a koordinációt a tagállamok, illetve az uniós intézmények, hivatalok és szervek között. Továbbá, tekintettel a kiberfenyegetések határok nélküli jellegére, a tagállami intézkedések kiegészítése céljával fokozni kell az uniós szintű képességeket, különösen a több országot érintő nagyszabású kiberbiztonsági események és válságok esetére. További erőfeszítésekre van szükség annak érdekében is, hogy a magánszemélyek és a vállalkozások jobban tisztában legyenek a kiberbiztonsági kérdésekkel. Emellett a digitális egységes piacba vetett bizalmat is növelni kell azáltal, hogy az IKT-termékek és -szolgáltatások biztonsági szintjéről átlátható információkat bocsátanak rendelkezésre. Ezt a célt könnyebben el lehet érni az egész EU-ra kiterjedő tanúsítással, amely valamennyi tagállam piacán, minden ágazatban közös kiberbiztonsági követelményeket és értékelési kritériumokat biztosít.
- (6) Az Európai Parlament és a Tanács 2004-ben azzal a céllal fogadta el az ENISA létrehozásáról szóló 460/2004/EK rendeletet<sup>30</sup>, hogy hozzájáruljon az Unión belüli magas szintű és hatékony hálózat- és információbiztonság biztosításához, valamint – a magánszemélyek, a fogyasztók, a vállalkozások és a közigazgatási szervek érdekeit

<sup>30</sup>

Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról (HL L 77., 2004.3.13., 1. o.).

szem előtt tartva – a hálózat- és információbiztonsági kultúra kialakításához. Az Európai Parlament és a Tanács 2008-ban az 1007/2008/EK rendelettel<sup>31</sup> az Ügynökség megbízási idejét 2012 márciusig meghosszabbította. Az 580/2011/EK rendelet<sup>32</sup> ezt a dátumot 2013. szeptember 13-ra módosította. Az Európai Parlament és a Tanács 2013-ban elfogadta az ENISA-ról és a 460/2004/EK rendelet hatályon kívül helyezéséről szóló 526/2013/EU rendeletet<sup>33</sup>, amely az Ügynökség megbízási idejének végét 2020 júniusában határozta meg.

- (7) Az Európai Unió már eddig is fontos lépéseket tett a kiberbiztonság és a digitális technológiákba vetett bizalom növelése érdekében. 2013-ban uniós szintű kiberbiztonsági stratégia elfogadására került sor, amely irányt szabott az Unió kiberbiztonsági fenyegetésekre és kockázatokra adott politikai válaszlépései kidolgozásának. Az európaiak online védelmének javítása érdekében tett erőfeszítései gyanánt az Unió 2016-ban elfogadta az első kiberbiztonsági jogalkotási aktust, a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 irányelvet (a továbbiakban: kiberbiztonsági irányelv). A kiberbiztonsági irányelv nemzeti képességekre vonatkozó követelményeket határozott meg a kiberbiztonság területén, kialakította az első mechanizmusokat a tagállamok közötti stratégiai és operatív együttműködés elmélyítése érdekében, és a biztonsági intézkedésekre és a biztonsági események bejelentésére vonatkozó kötelezettségeket vezetett be a gazdaság és a társadalom számára létfontosságú területeken, mint például az energia, a közlekedés, a vízellátás, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, a digitális infrastruktúra, valamint a kulcsfontosságú digitális szolgáltatók (keresőprogramok, felhőalapú számítástechnikai szolgáltatások, online piacterek). Az ENISA kulcsfontosságú szerepet kapott ezen irányelv végrehajtásának támogatásában. Emellett a kiberbűnözés elleni hatékony küzdelem az európai biztonsági stratégiában is kiemelt fontosságot élvez, hiszen hozzájárul a magas szintű kiberbiztonság elérésének általános céljához.
- (8) Ismert tény, hogy a 2013-as uniós kiberbiztonsági stratégia elfogadása és az Ügynökség megbízatásának legutóbbi felülvizsgálata óta az általános politikai kontextus jelentősen megváltozott, a még bizonytalanabb és kevésbé biztonságos globális környezet következtében is. Ezért az új uniós kiberbiztonsági politika keretében felül kell vizsgálni az ENISA megbízatását a megváltozott kiberbiztonsági ökoszisztémában betöltött szerepének meghatározása érdekében, és biztosítani kell, hogy hatékonyan hozzájáruljon a radikálisan új fenyegetésekből fakadó kiberbiztonsági kihívásokra adott uniós reagáláshoz, hiszen ehhez, amint az az Ügynökség értékeléséből is kiderült, jelenlegi megbízatása nem elegendő.
- (9) Az e rendelet által létrehozott Ügynökség az 526/2013/EU rendelettel korábban létrehozott ENISA jogutódja. Az Ügynökségnek az e rendelettel és az egyéb

<sup>31</sup> Az Európai Parlament és a Tanács 1007/2008/EK rendelete (2008. szeptember 24.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendeletnek az Ügynökség megbízási ideje tekintetében történő módosításáról (HL L 293., 2008.10.31., 1. o.).

<sup>32</sup> Az Európai Parlament és a Tanács 580/2011/EU rendelete (2011. június 8.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendeletnek az ügynökség megbízási ideje tekintetében történő módosításáról (HL L 165., 2011.6.24., 3. o.).

<sup>33</sup> Az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Unió Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről (HL L 165., 2013.6.18., 41. o.).

kiberbiztonsági uniós jogszabályokkal ráruházott feladatokat többek között szakértelem rendelkezésre bocsátása és tanácsadás révén, valamint uniós információs és tudásközpontként működve kell ellátnia. Célja, hogy előmozdítsa a bevált módszerek cseréjét a tagállamok és a magánszektor érdekelt felei között, szakpolitikai javaslatokat kínáljon az Európai Bizottságnak és a tagállamoknak, mintegy hivatkozási alapként működve az uniós ágazati szakpolitikai kezdeményezések számára a kiberbiztonsági kérdésekben, és elősegítse egyfelől a tagállamok közötti, másfelől a tagállamok, valamint az európai uniós intézmények, hivatalok és szervek közötti operatív együttműködést.

- (10) Az Európai Tanács 2003. december 13-i ülésén elfogadott 2004/97/EK, Euratom határozat keretében a tagállamok képviselői úgy határoztak, hogy az ENISA székhelye Görögországban lesz, egy, a görög kormány által meghatározandó városban. Az Ügynökségnek otthont adó tagállamnak a lehető legkedvezőbb feltételeket kell biztosítania az Ügynökség zavartalan és hatékony működéséhez. Az Ügynökség feladatainak megfelelő és hatékony ellátása, a munkaerő felvétele és a személyzet megtartása, továbbá a hálózatépítési tevékenységek hatékonyságának fokozása érdekében elengedhetetlen, hogy az Ügynökség székhelye megfelelő helyen legyen, ahol többek között megfelelő közlekedési csatlakozások és létesítmények állnak rendelkezésre az Ügynökség személyzetének tagjait kísérő házasársak és gyermekek részére. A szükséges szabályokat az Ügynökség igazgatótanácsának jóváhagyását követően az Ügynökség és az annak otthont adó tagállam közötti megállapodásban kell rögzíteni.
- (11) Tekintettel az Unió előtt álló, egyre fokozódó kiberbiztonsági kihívásokra, növelni kell az Ügynökség számára elkülönített pénzügyi és emberi erőforrásokat annak érdekében, hogy azok mértéke megfeleljen az Ügynökség kiemelt szerepének, feladatainak és az európai digitális ökoszisztémát védő szervezetek kötelékében betöltött kulcsfontosságú szerepének.
- (12) Az Ügynökségnek magas szintű szakértelmet kell kialakítania és fenntartania, és olyan hivatkozási alapként kell működnie, amely függetlensége, az általa nyújtott tanácsok és az általa terjesztett információk minősége, eljárásainak és működési módszereinek átláthatósága, valamint a feladatai ellátásában tanúsított gondossága révén bizalmat kelt az egységes piac iránt. Az Ügynökségnek proaktívan hozzá kell járulnia a nemzeti és uniós erőfeszítésekhez, és feladatait az uniós intézményekkel, szervekkel és hivatalokkal, valamint a tagállamokkal teljes körű együttműködés keretében kell végeznie. Ezenkívül a magánszektorral, valamint a többi érintett érdekelt féllel is együtt kell működnie, és a tőlük kapott észrevételeket is figyelembe kell vennie. Feladatainak leírásával meg kell határozni, hogy az Ügynökségnek hogyan kell céljait elérnie, de egyben rugalmasságot is biztosítani kell működéséhez.
- (13) Az Ügynökségnek tanáccsal, véleményezéssel és elemzések készítésével kell segítenie a Bizottságot valamennyi olyan uniós kérdésben, amely a kiberbiztonságot – beleértve a kritikus infrastruktúrák védelmét és a kibertámadásokkal szembeni ellenálló képességet – érintő szakpolitikák és jogszabályok kidolgozásához, illetve azok aktualizálásához és felülvizsgálatához kapcsolódik. Az Ügynökségnek hivatkozási alapként kell szolgálnia, amely tanácsadást folytat és szakértelmet biztosít az olyan uniós ágazatspecifikus szakpolitikai és jogi kezdeményezésekkel kapcsolatban, amelyek kiberbiztonsági kérdéseket is érintenek.
- (14) Az Ügynökség alapvető feladata, hogy elősegítse az idevágó jogi keretrendszer következetes végrehajtását, különösen a kiberbiztonsági irányelv eredményes

alkalmazását, ami alapvető fontosságú a kibertámadásokkal szembeni ellenálló képesség javításához. Tekintettel a kiberbiztonsági fenyegetések gyorsan változó természetére, egyértelmű, hogy a tagállamokat több szakpolitikai területet is felölelő, átfogóbb megközelítéssel kell támogatni a kibertámadásokkal szembeni ellenálló képességük kialakítása érdekében.

- (15) Az Ügynökségnek segítenie kell a tagállamok és az uniós intézmények, szervek és hivatalok arra irányuló munkáját, hogy kiépítsék, illetve fokozzák a kiberbiztonsági problémák és biztonsági események megelőzésével, észlelésével és az azokra való reagálással kapcsolatos képességeket és felkészültségüket, valamint támogatnia kell a hálózati és információs rendszerek biztonságát érintő erőfeszítéseiket. Különösen a nemzeti szinten működő, számítógép-biztonsági eseményekre reagáló csoportok, az ún. CSIRT-ek kialakítását és fejlesztését kell támogatnia annak érdekében, hogy azok Unió-szerte általánosan jó fejlettségi szintet érjenek el. Az Ügynökségnek a hálózati és információs rendszerek biztonságára, kiváltképpen a kiberbiztonságra vonatkozó uniós és tagállami stratégiák kidolgozásához és aktualizálásához is hozzá kell járulnia, és segítenie kell azok széles körű elterjesztésében, csakúgy mint végrehajtásuk nyomon követésében. Továbbá képzéseket és képzési anyagokat kell biztosítania az állami szervek számára, és adott esetben az oktatók képzéséről is gondoskodnia kell annak érdekében, hogy segítse a tagállamokat saját szakképzési kapacitásaik kifejlesztésében.
- (16) Az Ügynökségnek ugyancsak segítenie kell a kiberbiztonsági irányelvvel létrehozott együttműködési csoportot feladatai végrehajtásában, különösen szakértelmével, tanácsadással és a bevált módszerek cseréjének megkönnyítésével, kiváltképpen ami az alapvető szolgáltatásokat nyújtó szereplők tagállamok általi azonosítását illeti, vagyis melyek azok a szereplők, amelyek a biztonsági kockázatok és események terén fennálló, határokon átnyúló függőségek vonatkozásában relevánsak.
- (17) A köz- és a magánszektor közötti, valamint a magánszektoron belüli együttműködés ösztönzése céljából, különösen a kritikus infrastruktúrák védelmének támogatása érdekében az Ügynökségnek elő kell segítenie az ágazati információmegosztási és analitikai központok létrehozását azáltal, hogy megosztja a rendelkezésre álló eszközökkel és az eljárásokkal kapcsolatban bevált módszereket, illetve iránymutatást nyújt e téren, továbbá útmutatással szolgál az információk megosztásával kapcsolatos szabályozási kérdésekben.
- (18) Az Ügynökségnek össze kell gyűjtenie és elemeznie kell a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) és az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportja (CERT-EU) által készített nemzeti jelentéseket, és meg kell határoznia az információcsere közös szabályait, nyelvét és terminológiáját. Munkájába a magánszektor is be kell vonnia a kiberbiztonsági irányelv keretében, amely a CSIRT-hálózat létrehozásával meghatározta az önkéntes alapon történő, operatív szintű technikai információcsere alapjait.
- (19) Az Ügynökségnek a nagyszabású, határokon átnyúló kiberbiztonsági események és válsághelyzetek esetén hozzá kell járulnia az uniós szintű reagáláshoz. Ideértendő a megfelelő információk összegyűjtése, valamint a CSIRT-hálózat és a műszaki közösség, továbbá a válságkezelésért felelős döntéshozók közötti közvetítés is. Az Ügynökség ezenkívül technikai szempontból is támogatni tudná a biztonsági események kezelését azáltal, hogy elősegíti a megfelelő technikai megoldások tagállamok közötti cseréjét, valamint a nyilvánosság tájékoztatásához szükséges

információkat bocsát rendelkezésre. Az ilyen jellegű együttműködés módozatainak tesztelése révén az Ügynökségnek éves kiberbiztonsági gyakorlatok keretében támogatnia kell ezt a folyamatot.

- (20) Operatív feladatainak ellátásához az Ügynökségnek a CERT-EU szakértelmét is fel kell használnia, mégpedig szoros fizikai közelségben folytatott, strukturált együttműködésen keresztül. A strukturált együttműködés elősegíti a szükséges szinergiákat és az ENISA szakértelemének kiépítését. Adott esetben a két szervezet között külön megállapodásokat kell létrehozni az együttműködés gyakorlati megvalósításának meghatározására.
- (21) Operatív feladatainak megfelelően az Ügynökségnek képesnek kell lennie a tagállamok támogatására, például tanácsadással vagy technikai segítségnyújtással, valamint a fenyegetések és biztonsági események elemzésével. A Bizottság a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló ajánlásában azt tanácsolja a tagállamoknak, hogy jóhiszeműen működjenek együtt, és indokolatlan késedelem nélkül osszák meg egymással és az ENISA-val a nagyszabású kiberbiztonsági eseményekkel és válsághelyzetekkel kapcsolatos információkat. Ezek az információk az ENISA segítségével lesznek operatív feladatainak ellátása során.
- (22) Az uniós helyzetismeret támogatását célzó, rendes technikai szintű együttműködés részeként az Ügynökségnek rendszeresen el kell készítenie a kiberbiztonsági eseményekről és fenyegetésekről szóló uniós kiberbiztonsági technikai helyzetjelentést a nyilvánosan hozzáférhető információk, a saját elemzése és azon jelentések alapján, amelyeket a tagállami CSIRT-ek (önkéntes alapon) vagy a kiberbiztonsági irányelvvel létrehozott egyedüli kapcsolattartó pontok, az Europol Számítástechnikai Bűnözés Elleni Európai Központja (EC3), a CERT-EU és adott esetben az Európai Külügyi Szolgálaton (EKSZ) belül az Európai Unió Helyzetelemző Központja (INTCEN) rendelkezésre bocsátottak. A helyzetjelentést az érintett tanácsi és bizottsági szervek, az Unió külügyi és biztonságpolitikai főképviselője és a CSIRT-hálózat rendelkezésére kell bocsátani.
- (23) A több tagállamot érintő, jelentős hatású biztonsági eseményekkel kapcsolatos, az Ügynökség által támogatott vagy az Ügynökség által – kérésre, illetve az érintett tagállamok hozzájárulásával – végzett utólagos technikai vizsgálatoknak a jövőbeni események megelőzésére kell összpontosítaniuk, és azokat a vétkesség vagy a felelősség megállapítására irányuló bírósági vagy közigazgatási eljárások sérelme nélkül kell végezni.
- (24) Az Európai Unió működéséről szóló szerződés 346. cikke, illetve a közrenddel kapcsolatos más okok sérelme nélkül az érintett tagállamoknak biztosítaniuk kell az Ügynökség számára a vizsgálatokhoz szükséges információkat és segítségnyújtást.
- (25) A tagállamok felkérhetik a biztonsági esemény által érintett vállalkozásokat arra, hogy – a kereskedelmi szempontból érzékeny információk védeleméhez való joguk sérelme nélkül – a szükséges információk és segítségnyújtás biztosításával működjenek együtt az Ügynökséggel.
- (26) A kiberbiztonság területén jelentkező kihívások jobb megértése érdekében, valamint a tagállamoknak és az uniós intézményeknek nyújtott hosszú távú stratégiai tanácsadás céljából az Ügynökségnek elemeznie kell mind a már ismert, mind az új keletű kockázatokat. E célból az Ügynökségnek a tagállamokkal és adott esetben a statisztikai hivatalokkal és más szervekkel együttműködésben össze kell gyűjtenie a

releváns információkat, elemzéseket kell készítenie az új technológiákról, valamint tematikus értékeléseket kell végeznie a technológiai innovációknak a hálózat- és információbiztonságra, azon belül is különösen a kiberbiztonságra gyakorolt várható társadalmi, jogi, gazdasági és szabályozási hatásairól. Az Ügynökségnek továbbá a fenyegetések és biztonsági események elemzésével támogatnia kell a tagállamokat és az uniós intézményeket, hivatalokat és szerveket az új tendenciák azonosításában és a kiberbiztonsággal kapcsolatos problémák megelőzésében.

- (27) Az Ügynökségnek – az Unió ellenálló képességének növelése érdekében – tanácsadással, iránymutatással és a bevált módszerek terjesztésével kiválóságra kell törekednie az internetes infrastruktúra és a kritikus infrastruktúrák biztonságának területén. Annak érdekében, hogy a kiberbiztonsági kockázatokra és a lehetséges ellenintézkedésekre vonatkozó információk strukturált formában könnyebben hozzáférhetők legyenek, az Ügynökségnek uniós információs platformot, vagyis egy olyan egyablakos portált kell létrehoznia és fenntartania, ahol a nyilvánosság hozzájuthat az uniós és nemzeti intézményektől, hivataloktól és szervektől származó kiberbiztonsági információkhoz.
- (28) Az Ügynökségnek hozzá kell járulnia a kiberbiztonsági kockázatokkal kapcsolatos tudatosság növeléséhez, és magánszemélyeknek és szervezeteknek címzett, egyedi felhasználói iránymutatást kell nyújtania a már bevált módszerekkel kapcsolatban. Az egyéni felhasználók és szervezetek szintjén azáltal is hozzá kell járulnia a bevált módszerek és megoldások előmozdításához, hogy összegyűjti és elemzi a jelentős biztonsági eseményekre vonatkozó, nyilvánosan elérhető információkat, valamint jelentéseket készít abból a célból, hogy útmutatást nyújtson a vállalkozások és a magánszemélyek számára, valamint javítsa a felkészültség és az ellenálló képesség általános szintjét. Emellett a tagállamokkal és az uniós intézményekkel, szervekkel és hivatalokkal folytatott együttműködésben rendszeresen kampányokat kell szerveznie a végfelhasználók tájékoztatása és oktatása érdekében, melyek célja a biztonságosabb egyéni online magatartásformák elősegítése, valamint a virtuális térben potenciálisan jelenlévő veszélyek tudatosítása – ideértve az adathalászatot, a botneteket, a pénzügyi és banki csalásokat is magában foglaló kiberbűnözést is –, továbbá az alapvető hitelesítési és adatvédelmi tanácsadás nyújtása. Az Ügynökségnek központi szerepet kell játszania az eszközök biztonságosságával kapcsolatos végfelhasználói tudatosság minél gyorsabb növelésében.
- (29) A kiberbiztonsági ágazatban működő vállalkozások, valamint a kiberbiztonsági megoldások felhasználóinak támogatása érdekében az Ügynökségnek létre kell hoznia és fenn kell tartania egy „piaci megfigyelőközpontot”, vagyis mind a keresleti, mind a kínálati oldalon rendszeres elemzéseket kell végeznie, és széles körben ismertetnie kell a kiberbiztonsági piac főbb tendenciáit.
- (30) Célkitűzéseinek maradéktalan elérése érdekében az Ügynökségnek kapcsolatot kell kialakítania a megfelelő intézményekkel, hivatalokkal és szervekkel, többek között a CERT-EU-val, az Europol keretében működő Számítástechnikai Bűnözés Elleni Európai Központtal (EC3), az Európai Védelmi Ügynökséggel (EDA), a nagy méretű informatikai rendszerek operatív irányításával foglalkozó európai ügynökséggel (eu-LISA), az Európai Repülésbiztonsági Ügynökséggel (EASA) és a kiberbiztonságban érintett bármely más uniós ügynökségekkel. Kapcsolatot kell fenntartania továbbá az adatvédelmi hatóságokkal is a szakismeretek és a bevált módszerek megosztása érdekében, valamint azért, hogy tanácsokat tudjon adni a kiberbiztonság azon vonatkozásaival kapcsolatban, amelyek hatással lehetnek a hatóságok munkájára. A nemzeti és uniós bűnüldöző és adatvédelmi hatóságok képviselőinek lehetőséget

kell biztosítani arra, hogy képviseltesék magukat az Ügynökséghez tartozó érdekelt állandó csoportjában. Az Ügynökségnek a bűnüldözési szervekkel a munkájukra esetlegesen hatást gyakorló hálózat- és információbiztonsági kérdésekre vonatkozóan folytatott együttműködés során tiszteletben kell tartania a meglévő információs csatornákat és a létező hálózatokat.

- (31) Az Ügynökségnek mint a CSIRT-hálózat titkárságát biztosító tagnak támogatnia kell a tagállami CSIRT-ek és az CERT-EU operatív együttműködését, a CSIRT-hálózatnak a kiberbiztonsági irányelvben meghatározott egyéb releváns feladatainak ellátásához nyújtott támogatás mellett. Elő kell mozdítania és támogatnia kell továbbá a megfelelő CSIRT-ek közötti együttműködést a legalább két CSIRT-et is érintő vagy potenciálisan érintő, az általuk kezelt vagy védett hálózatokat vagy infrastruktúrát érő biztonsági események, támadások és zavarok esetén, figyelembe véve ugyanakkor a CSIRT-hálózat eljárási standardjait.
- (32) A kiberbiztonsági eseményekre való reagálással kapcsolatos uniós felkészültség javítása érdekében az Ügynökségnek évente kiberbiztonsági gyakorlatokat kell szerveznie uniós szinten, és, amennyiben erre igény van, támogatnia kell a tagállamokat és az uniós intézményeket, hivatalokat és szerveket a gyakorlatok megszervezésében.
- (33) Az Ügynökségnek a kiberbiztonsági tanúsítás terén kialakított szakértelmét ki kell alakítania és fenn kell tartania a kapcsolódó uniós szakpolitika támogatása érdekében. Elő kell mozdítania a kiberbiztonsági tanúsítás Unión belüli elterjesztését, többek között azáltal, hogy hozzájárul az uniós szintű kiberbiztonsági tanúsítási keretrendszer létrehozásához és fenntartásához annak érdekében, hogy átláthatóbbá tegye az IKT-termékek és -szolgáltatások által nyújtott kiberbiztonság szintjét, erősítve ezáltal a digitális belső piacba vetett bizalmat.
- (34) A hatékony kiberbiztonsági szakpolitikáknak a köz- és a magánszektorban egyaránt kellően kidolgozott kockázatértékelési módszereken kell alapulniuk. A kockázatértékelési módszereket különböző szinteken használják, és eredményes alkalmazásukat illetően nincs közös gyakorlat. A kockázatértékeléssel és az interoperabilis kockázatkezelési megoldásokkal kapcsolatban bevált módszereknek a köz- és a magánszektorbeli szervezetekben való ösztönzése, illetve kialakítása fokozza az Unió kiberbiztonságát. E célból az Ügynökségnek uniós szinten támogatnia kell az érdekelt együttműködését, azáltal, hogy előmozdítja az európai és nemzetközi szabványok kidolgozására és alkalmazására irányuló erőfeszítéseket egyfelől a kockázatkezeléssel, másfelől az elektronikus termékek, rendszerek, hálózatok és szolgáltatások mérhető biztonságával kapcsolatban, melyek a szoftverekkel együtt a hálózati és információs rendszerek alkotóelemei.
- (35) Az Ügynökségnek ösztönöznie kell a tagállamokat és a szolgáltatókat általános biztonsági előírásaik javítására, hogy minden internetfelhasználó megtehesse a személyes kiberbiztonságához szükséges lépéseket. Különösen fontos, hogy a szolgáltatók és a termékek gyártói visszavonják vagy újrahasznosítsák azokat a termékeket és szolgáltatásokat, amelyek nem felelnek meg a kiberbiztonsági szabványoknak. Az ENISA az illetékes hatóságokkal együttműködve tájékoztatást adhat a belső piacon kínált termékek és szolgáltatások kiberbiztonsági szintjéről, és figyelmeztetéseket is kiadhat, amelyekben a szolgáltatókat és a gyártókat szolgáltatásaik és termékeik biztonságának fokozására – ideértve a kiberbiztonságot is – szólítja fel.



- (36) Az Ügynökségnek teljes mértékben figyelembe kell vennie a folyamatban lévő – különösen a különböző uniós kutatási kezdeményezések keretében végzett – kutatási, fejlesztési és technológiaértékelési tevékenységeket azért, hogy igény esetén tanácsot tudjon adni az uniós intézmények, szervek és hivatalok, valamint adott esetben a tagállamok számára a hálózat- és információbiztonság, különösen a kiberbiztonság területét érintő kutatási igényekkel kapcsolatban.
- (37) A kiberbiztonsági problémák globális kérdések. Szorosabb nemzetközi együttműködésre van szükség a biztonsági szabványok javítása – és ezen belül a közös viselkedési normák meghatározása – érdekében, valamint a hálózat- és információbiztonsági kérdésekre adott reagálás tekintetében a gyorsabb nemzetközi együttműködést elősegítő információcsere javítása és egy azokra vonatkozó közös globális megközelítésmód kialakítása érdekében. Az Ügynökségnek e célból támogatnia kell az uniós szerepvállalás fokozását és a harmadik országokkal és a nemzetközi szervezetekkel folytatott együttműködést, adott esetben a szükséges szakértelmet és elemzéseket biztosítva az érintett uniós intézmények, szervek és hivatalok számára.
- (38) Az Ügynökségnek képesnek kell lennie arra, hogy eleget tegyen a tagállamok és az uniós intézmények, hivatalok és szervek tanácsadásra és segítségnyújtásra vonatkozó eseti megkereséseinek, amennyiben azok az Ügynökség célkitűzéseinek hatályába tartoznak.
- (39) A Ügynökség irányítását illetően alkalmazni kell bizonyos elveket az EU decentralizált ügynökségeivel foglalkozó intézményközi munkacsoport által 2012 júliusában elfogadott együttes nyilatkozatnak és közös megközelítésnek való megfelelés érdekében, melyek célja az ügynökségek tevékenységeinek gördülékennyé tétele és teljesítményük javítása. Az együttes nyilatkozatnak és a közös megközelítésnek adott esetben az Ügynökség munkaprogramjában, az Ügynökség értékeléseiben, valamint az Ügynökség jelentéstételi és adminisztratív gyakorlatában is érvényesülnie kell.
- (40) Az Ügynökség tevékenységének általános irányát a tagállamok és a Bizottság képviselőiből álló igazgatótanácsnak kell megszabnia, és arról is az igazgatótanácsnak kell gondoskodnia, hogy az Ügynökség e rendelettel összhangban ellássa kijelölt feladatait. Az igazgatótanácsot fel kell ruházni mindazokkal a hatáskörökkel, amelyek a költségvetés meghatározásához és végrehajtásának ellenőrzéséhez, a vonatkozó pénzügyi szabályzat elfogadásához, az Ügynökség átlátható határozathozatali eljárásainak kialakításához, az Ügynökség egységes programozási dokumentumának elfogadásához, saját eljárási szabályzatának elfogadásához, az ügyvezető igazgató kinevezéséhez, az ügyvezető igazgató hivatali idejének meghosszabbításához és az ügyvezető igazgató felmentéséhez szükségesek.
- (41) Az Ügynökség megfelelő és hatékony működése érdekében a Bizottságnak és a tagállamoknak biztosítaniuk kell, hogy az igazgatótanács tagjainak kinevezendő személyek a funkcionális területeken megfelelő szakértelemmel és tapasztalattal rendelkezzenek. Az igazgatótanács munkájának folytonosságát biztosítandó, a Bizottságnak és a tagállamoknak is törekedniük kell arra, hogy képviselőik ne cserélődjenek túl gyakran az igazgatótanácsban.
- (42) Az Ügynökség zavartalan működése azt kívánja, hogy az ügyvezető igazgató kinevezése érdemei, igazolt igazgatási és vezetői készségei, valamint a kiberbiztonság területén szerzett szakmai hozzáértése és tapasztalatai alapján történjék, és hogy az ügyvezető igazgató feladatait teljes mértékben független módon végezze. Az

ügyvezető igazgatónak – a Bizottsággal folytatott előzetes konzultációt követően – javaslatot kell tennie az Ügynökség munkaprogramjára, és meg kell tennie mindazokat a lépéseket, amelyek az Ügynökség munkaprogramja megfelelő végrehajtásának biztosításához szükségesek. Az ügyvezető igazgatónak továbbá el kell készítenie az igazgatótanácshoz benyújtandó éves jelentést, össze kell állítania az Ügynökség bevételeire és kiadásaira vonatkozó kimutatás tervezetét, és végre kell hajtania a költségvetést. Az ügyvezető igazgató részére továbbá lehetőséget kell biztosítani arra, hogy egyes konkrét – így különösen tudományos, műszaki, jogi vagy társadalmi-gazdasági – kérdésekben eseti munkacsoportokat hozzon létre. Az ügyvezető igazgatónak biztosítania kell, hogy az eseti munkacsoportok tagjainak kiválasztása a lehető legmagasabb szintű szakértelem alapján, a csoport feladatkörének sajátosságaihoz igazodva a tagállami közigazgatási szervek, az uniós intézmények és a magánszektor – beleértve az ipart, a felhasználókat és a hálózat- és információbiztonság területén működő tudományos szakembereket – közötti reprezentatív egyensúly kellő figyelembevételével történjék.

- (43) A felügyelőtestületnek hozzá kell járulnia az igazgatótanács hatékony működéséhez. Az igazgatótanács határozataival kapcsolatos előkészítő munkája részeként alaposan meg kell vizsgálnia a kapcsolódó információkat, fel kell derítenie a rendelkezésre álló lehetőségeket, valamint tanácsot és megoldásokat kell kínálnia az igazgatótanács vonatkozó határozatainak előkészítéséhez.
- (44) A magánszektorral, a fogyasztói szervezetekkel és más érdekelttel való rendszeres párbeszéd biztosítása céljából az Ügynökségen belül tanácsadó szervként indokolt létrehozni az érdekeltek állandó csoportját. Az érdekeltek állandó csoportjának, amelyet az ügyvezető igazgató javaslata alapján az igazgatótanács állít fel, az a feladata, hogy az érdekeltek számára fontos kérdésekre összpontosítson, illetve felhívja az Ügynökség figyelmét ezekre. Az érdekeltek állandó csoportjának összetételét és a csoportra bízott feladatokat, melyek közül a legfontosabb a munkaprogram-tervezet véleményezése, úgy kell meghatározni, hogy az érdekelt felek az Ügynökség munkájában megfelelő módon képviselve legyenek.
- (45) Az Ügynökségnek szabályokat kell kidolgoznia az összeférhetlenségek megelőzésére és kezelésére. Alkalmaznia kell továbbá a dokumentumokhoz való nyilvános hozzáférésről szóló 1049/2001/EK európai parlamenti és tanácsi rendeletben<sup>34</sup> meghatározott idevágó uniós rendelkezéseket is. A személyes adatokat a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 45/2001/EK európai parlamenti és tanácsi rendeletnek<sup>35</sup> megfelelően kell kezelnie. Be kell tartania továbbá az uniós intézményekre vonatkozó rendelkezéseket, valamint az információk – különösen a nem minősített bizalmas adatok és az EU-minősített adatok – kezelésére vonatkozó nemzeti jogszabályokat is.
- (46) Teljes mértékű autonómiájának és függetlenségének biztosítása érdekében, valamint, hogy további és új, többek között váratlan, sürgős feladatokat is teljesíteni tudjon, az Ügynökség számára elégséges és önálló költségvetést kell biztosítani, melynek bevételei elsősorban az Unió és az Ügynökség munkájában részt vevő harmadik országok hozzájárulásából származnak. Személyzete többségének közvetlenül az

<sup>34</sup> Az Európai Parlament és a Tanács 1049/2001/EK rendelete (2001. május 30.) az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről (HL L 145., 2001.5.31., 43. o.).

<sup>35</sup> HL L 8., 2001.1.12., 1. o.

Ügynökség megbízatásának operatív végrehajtásával kell foglalkoznia. Lehetőséget kell biztosítani arra, hogy az Ügynökségnek otthont adó tagállam vagy bármely más tagállam az Ügynökség bevételeihez önkéntes alapon hozzájáruljon. Az Unió általános költségvetését terhelő támogatások vonatkozásában továbbra is az uniós költségvetési eljárást kell alkalmazni. Ezenkívül az átláthatóság és az elszámoltathatóság érdekében a Számvevőszéknek ellenőriznie kell az Ügynökség elszámolásait.

- (47) A megfelelőségértékelés annak kimutatására szolgáló eljárás, hogy teljesültek-e az adott termékkel, eljárással, szolgáltatással, rendszerrel, személlyel vagy szervezettel kapcsolatban meghatározott követelmények. E rendelet alkalmazásában a tanúsítást a megfelelőségértékelés egy típusának kell tekinteni, amelyet egy-egy termék, eljárás, szolgáltatás, rendszer vagy ezek kombinációjának („IKT-termékek és -szolgáltatások”) kiberbiztonsági jellemzői vonatkozásában a termék gyártójával vagy a szolgáltatóval nem azonos független harmadik fél végez. A tanúsítás önmagában nem garantálja, hogy a tanúsított IKT-termékek és -szolgáltatások kiberbiztonsági szempontból megfelelőek. Inkább olyan eljárásról és technikai módszertanról van szó, amelynek célja annak igazolása, hogy az IKT-termékeket és -szolgáltatásokat bevizsgálták, és azok megfelelnek bizonyos – máshol, például a műszaki szabványokban meghatározott – kiberbiztonsági követelményeknek.
- (48) A kiberbiztonsági tanúsítás fontos szerepet játszik az IKT-termékek és -szolgáltatások iránti bizalom és azok biztonságosságának növelésében. A digitális egységes piac és különösen az adatközpontú gazdaság és a dolgok internete csak akkor lehet sikeres, ha a felhasználók általában véve bízhatnak abban, hogy az ilyen termékek és szolgáltatások kiberbiztonsági szintje megüt egy bizonyos mértéket. A hálózatba kapcsolt és automatizált járművek, az elektronikus orvostechikai eszközök, az ipari automatikus vezérlőrendszerek és az intelligens hálózatok olyan ágazatokra példák, amelyekben a tanúsítást már széles körben alkalmazzák vagy a közeljövőben valószínűleg alkalmazni fogják. A kiberbiztonsági irányelv által szabályozott ágazatok szintén olyan ágazatok, amelyekben a kiberbiztonsági tanúsítás kritikus fontosságú.
- (49) Az „Európa kibertámadásokkal szembeni ellenálló képességének erősítése, valamint a versenyképes és innovatív kiberbiztonsági ágazat támogatása” című 2016-os közleményében a Bizottság megállapította, hogy magas színvonalú, megfizethető és interoperabilis kiberbiztonsági termékekre és megoldásokra van szükség. Az IKT-termékek és -szolgáltatások egységes piacon való elérhetősége földrajzilag igen szétagtagolt. Ennek az az oka, hogy az európai kiberbiztonsági iparág nagyrészt aszerint alakult, hogy az egyes országokban mekkora volt a kereslet a kormányok részéről. Emellett az interoperabilis megoldások (műszaki szabványok), módszerek és az egész Unióra kiterjedő tanúsítási mechanizmusok hiánya is problémát jelent a kiberbiztonság egységes piacán. Ez egyrészt megnehezíti az európai vállalkozások számára, hogy megállják a helyüket a nemzeti, európai és globális versenyben. Másrészt pedig csökkent a magánfelhasználók és a vállalkozások számára hozzáférhető, működő és használható kiberbiztonsági technológiák kínálatát. A digitális egységes piaci stratégia végrehajtásának féldős értékelésében a Bizottság is kiemelte, hogy olyan hálózatba kapcsolt termékekre és rendszerekre van szükség, amelyek biztonságosak, és jelezte, hogy az európai IKT-biztonsági keretrendszer bevezetése, amellyel meghatározásra kerülnek az Unióban az IKT-biztonsági tanúsítás megszervezésének szabályai, két szempontból is jó szolgálatot tehet: segíthet megőrizni az internetbe vetett bizalmat és megoldást jelenthet a kiberbiztonsági piac jelenlegi szétagtagoltságára.
- (50) Jelenleg az IKT-termékek és -szolgáltatások esetében csak korlátozott mértékben alkalmazzák a kiberbiztonsági tanúsítást. Ha igen, akkor is főként tagállami szinten

vagy az ágazat kezdeményezésére kialakított rendszerek keretében kerül sor erre. A valamely nemzeti kiberbiztonsági hatóság által kiadott tanúsítványt tehát főszabály szerint a többi tagállam nem ismeri el. A vállalatoknak így működésük helye szerint több tagállamban is tanúsíttatniuk kell termékeiket és szolgáltatásaikat, ha például nemzeti közbeszerzési eljárásokban kívánnak részt venni. Mindemellett, míg egyre újabb és újabb rendszerek jönnek létre, a horizontális kiberbiztonsági kérdések tekintetében – például a dolgok internetét illetően – nincs egységes és holisztikus megközelítés. A meglévő rendszerek az érintett termékek köre, a biztonsági szintek, az alapvető kritériumok és a gyakorlati felhasználás tekintetében jelentős hiányosságokat és különbségeket mutatnak.

- (51) Történtek már lépések annak érdekében, hogy Európában kölcsönösen elismerjék a tanúsítványokat. Ezek azonban csak részben voltak sikeresek. E tekintetben a legfontosabb példa a vezető tisztviselők információs rendszerek biztonságával foglalkozó csoportján (SOG-IS) belül elfogadott kölcsönös elismerési megállapodás. Bár a megállapodás a biztonsági tanúsítás terén a legjelentősebb példa az együttműködésre és a kölcsönös elismerésre, magas költségei és korlátozott alkalmazási köre számottevő hiányosságnak számítanak. Eddig csak néhány digitális termék esetében fejlesztettek ki védelmi profilt, ilyen például a digitális aláírás, a digitális menetíró készülék és az intelligens kártyák. A legnagyobb hátrány azonban az, hogy a SOG-IS csoport csak az uniós tagállamok egy részét foglalja magában. Így a kölcsönös elismerési megállapodás is csak korlátozott hatékonyságú lehet a belső piac szempontjából.
- (52) A fentiek alapján szükségesnek mutatkozik egy olyan európai kiberbiztonsági tanúsítási keretrendszer létrehozása, amely megállapítja, hogy milyen fő horizontális követelményeket kell kidolgozni az európai kiberbiztonsági tanúsítási rendszerekre vonatkozóan, és lehetővé teszi az IKT-termékek és -szolgáltatások tanúsítványainak valamennyi tagállamban történő elismerését és használatát. Az európai keretrendszernek kettős célt kell szolgálnia: egyrészt növelnie kell az ilyen rendszerek alapján tanúsított IKT-termékek és -szolgáltatások iránti bizalmat. Másrészt az is célja, hogy ne legyenek egymásnak ellentmondó vagy egymással átfedő nemzeti kiberbiztonsági tanúsítványok, vagyis csökkenjenek a digitális egységes piacon működő vállalkozások költségei. A rendszereknek megkülönböztetésmentesnek kell lenniük, és nemzetközi és/vagy uniós szabványokon kell alapulniuk, kivéve, ha ezek a szabványok nem hatékonyak vagy nem alkalmasak az EU e tekintetben kitűzött legitim céljainak teljesítésére.
- (53) A Bizottságot fel kell hatalmazni arra, hogy európai kiberbiztonsági tanúsítási rendszereket fogadjon el az IKT-termékek és -szolgáltatások meghatározott csoportjaira vonatkozóan. Ezeket a rendszereket a nemzeti tanúsításfelügyeleti hatóságoknak kell megvalósítaniuk és felügyelniük, és az e rendszerek keretében kiadott tanúsítványokat az egész Unióban érvényesnek kell tekinteni és el kell ismerni. Az ágazat vagy más magánszervezetek által működtetett tanúsítási rendszerek nem tartoznak a rendelet hatálya alá. Az ilyen rendszereket működtető szervezetek azonban javasolhatják, hogy a Bizottság vizsgálja meg, hogy azok európai rendszer alapjául szolgálhatnak-e és akként jóváhagyhatók-e.
- (54) E rendelet rendelkezései nem érintik az IKT-termékek és -szolgáltatások tanúsítására vonatkozó egyedi szabályokat megállapító uniós jogszabályokat. Így például az általános adatvédelmi rendelet tanúsítási mechanizmusok és adatvédelmi védjegyek, illetve jelölések létrehozásáról rendelkezik, melyek annak igazolására szolgálnak, hogy az adatkezelők és az adatfeldolgozók a műveletek során teljesítették az említett

rendelet előírásait. Az ilyen tanúsítási mechanizmusok és adatvédelmi védjegyek, illetve jelölések célja, hogy az érintettek gyorsan meg tudják állapítani, hogy a releváns termékek és szolgáltatások milyen szintű adatvédelemmel vannak ellátva. Jelen rendelet nem érinti az adatfeldolgozási műveletek általános adatvédelmi rendelet szerinti tanúsítását, még akkor sem, ha az ilyen műveletek termékekbe és szolgáltatásokba vannak beágyazva.

- (55) Az európai kiberbiztonsági tanúsítási rendszerek célja annak biztosítása, hogy az ilyen rendszerek keretében tanúsított IKT-termékek és -szolgáltatások megfeleljenek a meghatározott követelményeknek. E követelmények az olyan tevékenységekkel szembeni ellenálló képességet érintik egy adott biztonsági szinten, amelyek célja, hogy veszélyeztessék az e rendelet szerinti termékek, eljárások, szolgáltatások és rendszerek által tárolt vagy továbbított vagy feldolgozott adatok, illetve az említett termékek, eljárások, szolgáltatások és rendszerek által biztosított vagy elérhetővé tett kapcsolódó funkciók vagy szolgáltatások hozzáférhetőségét, hitelességét, sértetlenségét és titkosságát. Lehetetlenség ebben a rendeletben az összes IKT-termék és -szolgáltatás vonatkozásában részletesen meghatározni a kiberbiztonsági követelményeket. Az IKT-termékek és -szolgáltatások, valamint a kapcsolódó kiberbiztonsági igények olyan különbözők, hogy nagyon nehéz minden eshetőségre érvényes általános kiberbiztonsági követelményeket kialakítani. Ezért a tanúsítás céljára tág és általános kiberbiztonság-fogalmat kell elfogadni, amelyet az európai kiberbiztonsági tanúsítási rendszerek kidolgozása során figyelembe veendő, egyedi kiberbiztonsági célkitűzések egészítenek ki. Az, hogy ezeket a célkitűzéseket egyes IKT-termékek és -szolgáltatások esetében hogyan kell elérni, részleteiben a Bizottság által elfogadott egyedi tanúsítási rendszerek szintjén kerül meghatározásra, például szabványokra vagy műszaki előírásokra való hivatkozás révén.
- (56) A Bizottságot fel kell hatalmazni arra, hogy felkérhesse az ENISA-t meghatározott IKT-termékekkel vagy -szolgáltatásokkal kapcsolatos rendszerekre irányuló javaslatok kidolgozására. A Bizottságnak ezt követően felhatalmazást kell kapnia arra, hogy végrehajtási jogi aktusok útján – az ENISA által javasolt rendszer alapján – elfogadja az európai kiberbiztonsági tanúsítási rendszert. Figyelemmel az e rendelet általános céljára és a benne megállapított biztonsági célkitűzésekre, a Bizottság által elfogadott európai kiberbiztonsági tanúsítási rendszereknek az egyes rendszerek tárgyát, alkalmazási körét és működését érintő bizonyos elemeket meg kell határozniuk. Ezeknek többek között a következőket kell magukban foglalniuk: a kiberbiztonsági tanúsítás hatályát és tárgyát, ideértve a hatálya alá tartozó IKT-termékek és -szolgáltatások kategóriáit, a kiberbiztonsági követelmények részletes leírását, például szabványokra vagy műszaki előírásokra való hivatkozások révén, az egyedi értékelési kritériumokat és értékelési módszereket, valamint a biztonság tervezett szintjét (alapvető, jelentős és/vagy magas).
- (57) Az uniós és nemzeti jogszabályok eltérő rendelkezései hiányában az európai kiberbiztonsági tanúsítás igénybevételének továbbra is önkéntes alapon kell történnie. E rendelet céljainak elérése és a belső piac széttagoltságának megakadályozása érdekében azonban az európai kiberbiztonsági tanúsítási rendszer hatálya alá tartozó IKT-termékekre és -szolgáltatásokra vonatkozó nemzeti kiberbiztonsági tanúsítási rendszerek és eljárások a Bizottság által a végrehajtási jogi aktusban meghatározott időponttól kezdve nem keletkeztethetnek joghatást. Emellett a tagállamok nem vezethetnek be olyan új nemzeti tanúsítási rendszereket, amelyek már valamelyik hatályos európai kiberbiztonsági tanúsítási rendszer tárgyát képező IKT-termékek és -szolgáltatások tekintetében szolgálnak kiberbiztonsági tanúsítási rendszerként.

- (58) Amint egy európai kiberbiztonsági tanúsítási rendszer elfogadásra kerül, az IKT-termékek gyártói és az IKT-szolgáltatások nyújtói számára lehetővé kell tenni, hogy termékeiket vagy szolgáltatásaikat egy általuk választott megfelelőségértékelő szervezethez tanúsításra benyújtsák. A megfelelőségértékelő szervezeteket egy akkreditáló testületnek akkreditálnia kell, amennyiben azok megfelelnek az e rendeletben meghatározott bizonyos követelményeknek. Az akkreditáció legfeljebb öt évre szól, és azonos feltételek mellett megújítható, feltéve, hogy az adott megfelelőségértékelő szervezet teljesíti a követelményeket. Az akkreditáló testületeknek vissza kell vonniuk a megfelelőségértékelő szervezet akkreditációját, amennyiben az akkreditáció feltételei nem, vagy már nem teljesülnek, vagy ha a megfelelőségértékelő szervezet által hozott intézkedések megsértik ezt a rendeletet.
- (59) Elő kell írni valamennyi tagállam számára, hogy jelöljön ki egy kiberbiztonsági tanúsításfelügyeleti hatóságot, amely felügyeli, hogy az adott tagállam területén székhellyel rendelkező megfelelőségértékelő szervezetek és az általuk kibocsátott tanúsítványok megfelelnek-e a rendelet és a vonatkozó kiberbiztonsági tanúsítási rendszerek követelményeinek. A nemzeti tanúsításfelügyeleti hatóságok feladata, hogy kezeljék a természetes vagy jogi személyek által az adott tagállam területén székhellyel rendelkező megfelelőségértékelő szervezetek által kiadott tanúsítványokkal kapcsolatban benyújtott panaszokat, megfelelő mértékben kivizsgálják a panasz tárgyát, és észszerű időn belül tájékoztassák a panaszost a vizsgálat előrehaladásáról és eredményéről. Ezen túlmenően együtt kell működniük a többi nemzeti tanúsításfelügyeleti hatósággal és más hatóságokkal, többek között azáltal, hogy megosztják az azzal kapcsolatos információkat, ha bizonyos IKT-termékek és -szolgáltatások nem felelnek meg e rendelet vagy az egyes kiberbiztonsági rendszerek követelményeinek.
- (60) Az európai kiberbiztonsági tanúsítási keretrendszer következetes alkalmazása érdekében létre kell hozni a nemzeti tanúsításfelügyeleti hatóságokból álló európai kiberbiztonsági tanúsítási csoportot (a továbbiakban: csoport). A csoport fő feladata, hogy tanácsot adjon és segítséget nyújtson a Bizottságnak az európai kiberbiztonsági tanúsítási keretrendszer következetes végrehajtásának és alkalmazásának biztosítása érdekében, segítse az Ügynökség munkáját és szorosan együttműködjön vele a kiberbiztonsági tanúsítási rendszerekre irányuló javaslatok kidolgozásában; ajánlást fogalmazzon meg arra vonatkozóan, hogy a Bizottság kérje fel az Ügynökséget európai kiberbiztonsági tanúsítási rendszerekre irányuló javaslatok kidolgozására, és fogadjon el a Bizottságnak címzett véleményeket a meglévő európai kiberbiztonsági tanúsítási rendszerek fenntartásával és felülvizsgálatával kapcsolatban.
- (61) A jövőbeli uniós kiberbiztonsági rendszerek ismertebbé és elfogadottabbá tétele érdekében az Európai Bizottság általános vagy ágazatspecifikus kiberbiztonsági iránymutatásokat adhat ki, például a helyes kiberbiztonsági módszerekről vagy a felelősségteljes kiberbiztonsági magatartásról, kiemelve a tanúsított IKT-termékek és -szolgáltatások használatának kedvező hatását.
- (62) Az Ügynökség által a kiberbiztonsági tanúsítással kapcsolatban nyújtott támogatás magában foglalja a Tanács Biztonsági Bizottságával és az illetékes nemzeti testülettel való kapcsolattartást is, a minősített hálózatokban alkalmazandó termékek kriptográfiai jóváhagyását illetően.
- (63) A megfelelőségértékelő szervezetek akkreditációjára vonatkozó kritériumok pontosítása érdekében a Bizottságnak felhatalmazást kell kapnia arra, hogy az Európai Unió működéséről szóló szerződés 290. cikkének megfelelően jogi aktusokat fogadjon

el. A Bizottságnak az előkészítő munka során megfelelő konzultációkat kell folytatnia, többek között szakértői szinten. Ezeket a konzultációkat a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban meghatározott elvekkel összhangban kell folytatni. A felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlamentnek és a Tanácsnak a tagállamok szakértőivel egyidejűleg kell kézhez kapnia minden dokumentumot, és szakértőik rendszeresen részt vehetnek a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein.

- (64) E rendelet végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni, ha e rendelet úgy rendelkezik. Ezeket a végrehajtási hatásköröket a 182/2011/EU rendeletnek megfelelően kell gyakorolni.
- (65) Vizsgálóbizottsági eljárással kell elfogadni azon végrehajtási jogi aktusokat, amelyek az IKT-termékek és -szolgáltatások európai kiberbiztonsági tanúsítási rendszereire és az Ügynökség által végzett vizsgálatok módszertanára vonatkoznak, valamint arra, hogy a nemzeti tanúsításfelügyeleti hatóságok milyen feltételek mellett, milyen formátumban és milyen eljárások útján jelentik be a Bizottságnak az akkreditált megfelelőségértékelő szervezeteket.
- (66) Az Ügynökség működését független értékelésnek kell alávetni. Az értékelés során figyelembe kell venni, hogy az Ügynökség milyen mértékben érte el célkitűzéseit, milyen munkamódszereket használ, és feladatai relevánsak-e. Az értékelésnek ki kell terjednie az európai kiberbiztonsági tanúsítási keretrendszer hatására, eredményességére és hatékonyságára is.
- (67) Az 526/2013/EU rendeletet hatályon kívül kell helyezni.
- (68) Mivel e rendelet céljait a tagállamok nem tudják kielégítően megvalósítani, és azok inkább uniós szinten valósíthatók meg jobban, az Unió az Európai Unióról szóló szerződés 5. cikkében meghatározott szubszidiaritás elvének megfelelően intézkedéseket fogadhat el. Az említett cikkben foglalt arányosság elvének megfelelően ez a rendelet nem lépi túl az említett célok eléréséhez szükséges mértéket,

ELFOGADTA EZT A RENDELETET:

# I. CÍM

## ÁLTALÁNOS RENDELKEZÉSEK

### 1. cikk

#### ***A rendelet tárgya és hatálya***

A belső piac megfelelő működésének biztosítása és ezzel egyidejűleg a kiberbiztonság, a kiberbiztonsági támadásokkal szembeni ellenálló képesség és az Unión belül a kiberbiztonságba vetett bizalom magas szintjének elérése érdekében e rendelet:

- a) megállapítja az ENISA, az „Európai Unió Kiberbiztonsági Ügynökség” (a továbbiakban: Ügynökség) céljait, feladatait és felépítési szempontjait, valamint
- b) meghatározza az európai kiberbiztonsági tanúsítási rendszerek létrehozásának keretrendszerét annak érdekében, hogy az Unión belül biztosítsa az IKT-termékek és -szolgáltatások megfelelő kiberbiztonsági szintjét. Ez a keretrendszer az egyéb uniós jogi aktusokban az önkéntes vagy kötelező tanúsításra vonatkozóan előírt különös rendelkezések sérelme nélkül alkalmazandó.

### 2. cikk

#### ***Fogalommeghatározások***

E rendelet alkalmazásában:

1. „kiberbiztonság”: mindazon tevékenységek, amelyek a hálózati és információs rendszereknek, azok felhasználóinak és az érintett személyeknek a kiberfenyegetésekkel szembeni védelméhez szükségesek;
2. „hálózati és információs rendszer”: az (EU) 2016/1148 irányelv 4. cikkének 1. pontja szerinti rendszer;
3. „a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia”: az (EU) 2016/1148 irányelv 4. cikkének 3. pontja szerinti keretrendszer;
4. „alapvető szolgáltatásokat nyújtó szereplő”: az (EU) 2016/1148 irányelv 4. cikkének 4. pontjában szereplő fogalommeghatározás szerinti közjogi vagy magánjogi szervezet;
5. „digitális szolgáltató”: az (EU) 2016/1148 irányelv 4. cikkének 6. pontjában szereplő fogalommeghatározás szerinti minden olyan jogi személy, amely digitális szolgáltatást nyújt;
6. „biztonsági esemény”: az (EU) 2016/1148 irányelv 4. cikkének 7. pontjában szereplő fogalommeghatározás szerinti minden esemény;
7. „biztonsági esemény kezelése”: az (EU) 2016/1148 irányelv 4. cikkének 8. pontjában szereplő fogalommeghatározás szerinti minden eljárás;
8. „kiberfenyegetés”: bármely olyan lehetséges körülmény vagy esemény, amely kedvezőtlen hatást gyakorolhat a hálózati és információs rendszerekre, azok felhasználóira és az érintett személyekre;
9. „európai kiberbiztonsági tanúsítási rendszer”: uniós szinten meghatározott átfogó szabályok, műszaki követelmények, szabványok és eljárások összessége, melyek az adott tanúsítási rendszer hatálya alá tartozó információs és kommunikációs technológiai (IKT) termékek és szolgáltatások tanúsítására vonatkoznak;



10. „európai kiberbiztonsági tanúsítvány”: valamely megfelelőségértékelő szervezet által annak igazolására kiállított dokumentum, hogy egy adott IKT-termék vagy -szolgáltatás megfelel az európai kiberbiztonsági tanúsítási rendszerben meghatározott egyedi követelményeknek;
11. „IKT-termék és -szolgáltatás”: a hálózati és információs rendszerek bármely eleme vagy elemeinek csoportja;
12. „akkreditáció”: a 765/2008/EK rendelet 2. cikkének 10. pontjában szereplő fogalommeghatározás szerinti akkreditálás;
13. „nemzeti akkreditáló testület”: a 765/2008/EK rendelet 2. cikkének 11. pontjában szereplő fogalommeghatározás szerinti nemzeti akkreditáló testület;
14. „megfelelőségértékelés”: a 765/2008/EK rendelet 2. cikkének 12. pontjában szereplő fogalommeghatározás szerinti megfelelőségértékelés;
15. „megfelelőségértékelő szervezet”: a 765/2008/EK rendelet 2. cikkének 13. pontjában szereplő fogalommeghatározás szerinti megfelelőségértékelő szervezet;
16. „szabvány”: az 1025/2012/EU rendelet 2. cikkének 1. pontjában szereplő fogalommeghatározás szerintsabvány.

## II. CÍM

### ENISA – az „Európai Unió Kiberbiztonsági Ügynökség”

#### I. FEJEZET

#### MEGBÍZATÁS, CÉLKITŰZÉSEK ÉS FELADATOK

##### 3. cikk

##### *Megbízatás*

- (1) Az Ügynökség elvégzi az e rendelet által az Unión belüli magas szintű kiberbiztonsághoz való hozzájárulás érdekében ráruházott feladatokat.
- (2) Az Ügynökség ellátja a kiberbiztonsággal kapcsolatos tagállami törvényi, rendeleti és közigazgatási rendelkezések közelítésére vonatkozó intézkedéseket meghatározó uniós jogi aktusok által ráruházott feladatokat is.
- (3) Az Ügynökség céljai és feladatai nem sértik a kiberbiztonsággal kapcsolatos tagállami hatásköröket, sem általában a közbiztonsággal, a közvédelemmel és a nemzetbiztonsággal kapcsolatos tevékenységeket, sem pedig az állam büntetőjogi területeken folytatott tevékenységét.

##### 4. cikk

##### *Célkitűzések*

- (1) Az Ügynökség – függetlensége, az általa biztosított tanácsadás, segítségnyújtás és információk tudományos és technikai minősége, átlátható működési eljárásai és módszerei, valamint a feladatai ellátásában tanúsított gondosság alapján – kiberbiztonsági szakértői központként működik.
- (2) Az Ügynökség segíti az uniós intézményeket, hivatalokat és szerveket, valamint a tagállamokat a kiberbiztonsággal kapcsolatos szakpolitikák kidolgozásában és végrehajtásában.
- (3) Az Ügynökség támogatja az Unión belüli kapacitásépítést és felkészültséget azáltal, hogy segíti az Uniót, a tagállamokat, valamint a köz- és a magánszféra érdekelt feleit hálózati és információs rendszereik védelmének fokozásában, a kiberbiztonsági készségek és kompetenciák fejlesztésében, valamint a kibertámadásokkal szembeni ellenálló képesség kialakításában.
- (4) Az Ügynökség a kiberbiztonsággal kapcsolatos kérdésekben előmozdítja az uniós szintű együttműködést és koordinációt a tagállamok, az uniós intézmények, hivatalok és szervek, valamint az érintett felek között, beleértve a magánszektor is.
- (5) Az Ügynökség fokozza az uniós szintű kiberbiztonsági képességeket annak érdekében, hogy kiegészítse a kiberfenyegetések megelőzése és az azokra való reagálás terén tett tagállami intézkedéseket, különösen a több országot érintő biztonsági események esetében.
- (6) Az Ügynökség előmozdítja a tanúsítás használatát, többek között azáltal, hogy e rendelet III. címével összhangban hozzájárul az uniós szintű kiberbiztonsági tanúsítási keretrendszer létrehozásához és fenntartásához annak érdekében, hogy

átláthatóbbá tegye az IKT-termékek és -szolgáltatások által nyújtott kiberbiztonság szintjét, és megerősítse ezzel a digitális belső piacba vetett bizalmat.

- (7) Az Ügynökség elősegíti, hogy a magánszemélyek és a vállalkozások a kiberbiztonsághoz kapcsolódó kérdésekben nagy mértékben tájékozottak legyenek.

#### *5. cikk*

### ***Az uniós szakpolitika és jogszabályok kidolgozásával és végrehajtásával kapcsolatos feladatok***

Az Ügynökség az alábbi tevékenységekkel járul hozzá az uniós szakpolitika és jogszabályok kidolgozásához és végrehajtásához:

- (1) segítségnyújtás és tanácsadás, különösen a kiberbiztonság területére vonatkozó uniós szakpolitika és jogszabályok kidolgozásával és felülvizsgálatával kapcsolatos független vélemények és előkészítő munka révén, de a kiberbiztonsági kérdéseket érintő ágazatspecifikus szakpolitikai és jogi kezdeményezésekkel kapcsolatban is;
- (2) segítségnyújtás a tagállamok számára a kiberbiztonsággal kapcsolatos uniós szakpolitika és jogszabályok következetes végrehajtásában, különösen az (EU) 2016/1148 irányelv vonatkozásában, többek között vélemények, iránymutatások, tanácsadás nyújtása, továbbá a kockázatkezeléssel, a biztonsági események bejelentésével és az információk megosztásával kapcsolatban bevált módszerek megosztása révén; valamint az e téren bevált módszerek illetékes hatóságok közötti cseréjének elősegítése;
- (3) szakértelemmel és segítségnyújtással való hozzájárulás az (EU) 2016/1148 irányelv 11. cikke szerinti együttműködési csoport munkájához;
- (4) az alábbi tevékenységek támogatása:
  1. az elektronikus azonosítás és a bizalmi szolgáltatások területére vonatkozó uniós szakpolitika kidolgozása és végrehajtása, különösen tanácsadással és technikai iránymutatásokkal, valamint a bevált módszerek illetékes hatóságok közötti cseréjének elősegítésével;
  2. az elektronikus hírközlés magasabb biztonsági szintjének előmozdítása, többek között szakértelem rendelkezésre bocsátása és tanácsadás révén, valamint a bevált módszerek illetékes hatóságok közötti cseréjének elősegítésével;
- (5) az uniós szakpolitikai tevékenységek rendszeres felülvizsgálatához nyújtott támogatás a vonatkozó jogi keretrendszer végrehajtásának állapotáról szóló éves jelentés formájában, a következők tekintetében:
  - a) az egyes tagállamok biztonsági eseményeire vonatkozó bejelentések, amelyekről az egyedüli kapcsolattartó pontok az (EU) 2016/1148 irányelv 10. cikkének (3) bekezdése alapján tájékoztatták az együttműködési csoportot;
  - b) a bizalmi szolgáltatókkal összefüggésben a biztonság megsértésére és az adatok sértetlenségének megszűnésére vonatkozó bejelentések, amelyekről a 910/2014/EU rendelet 19. cikkének (3) bekezdése alapján a felügyeleti szervek tájékoztatják az Ügynökséget;

- c) a nyilvános hírközlő hálózatokat vagy nyilvánosan hozzáférhető elektronikus hírközlési szolgáltatásokat biztosító vállalkozások által a biztonság megsértésével kapcsolatban benyújtott bejelentések, amelyekről [az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló irányelv] 40. cikke értelmében az illetékes hatóságok tájékoztatják az Ügynökséget.

## 6. cikk

### Kapacitásépítési feladatok

- (1) Az Ügynökség támogatja:
- a) a tagállamokat a kiberbiztonsági problémák és események megelőzésének, észlelésének, elemzésének és az ilyen problémákra és eseményekre való reagálási képességnek a javítására irányuló erőfeszítéseikben azáltal, hogy biztosítja számukra a szükséges ismereteket és szaktudást;
  - b) az uniós intézményeket, szerveket és hivatalokat a kiberbiztonsági problémák és események megelőzésének, észlelésének, elemzésének és az ilyen problémákra és eseményekre való reagálási képességnek a javítására irányuló erőfeszítéseikben az uniós intézmények, ügynökségek és szervek hálózatbiztonsági vészhelyzeteket elhárító csoportjának (CERT-EU) számára nyújtott megfelelő támogatás révén;
  - c) a tagállamokat, kérésükre, a számítógép-biztonsági eseményekre reagáló csoportok (ún. CSIRT-ek) tagállami szintű kialakításában az (EU) 2016/1148 irányelv 9. cikkének (5) bekezdése alapján;
  - d) a tagállamokat, kérésükre, az (EU) 2016/1148 irányelv 7. cikkének (2) bekezdése alapján a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia kidolgozásában; az Ügynökség a bevált módszerek népszerűsítése érdekében az Unió egészében elősegíti e stratégiák elterjesztését és végrehajtásuk nyomon követését;
  - e) az uniós intézményeket a kiberbiztonsággal kapcsolatos uniós stratégiák kidolgozásában és felülvizsgálatában, elősegítve azok elterjesztését és végrehajtásuk nyomon követését;
  - f) a tagállami és az uniós CSIRT-ek képességeinek fejlesztését többek között a párbeszéd és az információcsere elősegítése révén annak biztosítása érdekében, hogy a technológia mindenkor állásának megfelelően valamennyi CSIRT rendelkezzen egy sor közösen megállapított minimumképességgel, és a bevált módszerek szerint működjön;
  - g) a tagállamokat a 7. cikk (6) bekezdésében említett, uniós szintű nagyszabású éves kiberbiztonsági gyakorlatok megszervezésével, valamint a gyakorlatok értékelésén és a levont tanulságokon alapuló szakpolitikai ajánlások kidolgozásával;
  - h) az érintett állami szerveket a kiberbiztonsággal kapcsolatos képzések biztosításával, adott esetben az érdekelt felekkel együttműködve;
  - i) az együttműködési csoportot, a bevált módszerek megosztása révén, különös tekintettel az alapvető szolgáltatásokat nyújtó szereplők tagállamok általi meghatározásával kapcsolatban, a kockázatok és biztonsági események terén fennálló, határokon átnyúló függőségekkel összefüggésben is, az (EU) 2016/1148 irányelv 11. cikke (3) bekezdésének l) pontja alapján.

- (2) Az Ügynökség – különösen az (EU) 2016/1148 irányelv II. mellékletében felsorolt ágazatokban – elősegíti az ágazati információmegosztási és analitikai központok létrehozását és folyamatosan támogatja azokat azáltal, hogy megosztja a rendelkezésre álló eszközökkel és az eljárásokkal kapcsolatban bevált módszereket, illetve iránymutatást nyújt e téren, továbbá útmutatással szolgál az információk megosztásával kapcsolatos szabályozási kérdésekben.

#### 7. cikk

##### **Az uniós szintű operatív együttműködéssel kapcsolatos feladatok**

- (1) Az Ügynökség támogatja az illetékes állami szervek és az érdekelttek közötti operatív együttműködést.
- (2) Az Ügynökség operatív szinten együttműködik és szinergiák kialakítására törekszik az uniós intézményekkel, szervekkel és hivatalokkal, köztük a CERT-EU-val, a kiberbűnözés elleni szolgálatokkal, valamint a magánélet és személyes adatok védelmével foglalkozó felügyeleti hatóságokkal a közös problémák kezelése érdekében, többek között a következők által:
- a) a szakismeretek és a bevált módszerek megosztása;
  - b) a felmerülő kiberbiztonsági kérdésekkel kapcsolatos tanácsadás és iránymutatások;
  - c) a Bizottsággal folytatott konzultációt követően gyakorlati szabályok megállapítása az egyes feladatok végrehajtására vonatkozóan.
- (3) Az (EU) 2016/1148 irányelv 12. cikkének (2) bekezdése alapján az Ügynökség biztosítja a CSIRT-hálózat titkárságát, és aktívan elősegíti a hálózat tagjai közötti információmegosztást és együttműködést.
- (4) Az Ügynökség hozzájárul a CSIRT-hálózaton belüli operatív együttműködéshez, támogatást nyújtva a tagállamoknak a következők terén:
- a) a biztonsági események megelőzésére, észlelésére és az azokra való reagálásra irányuló képességeik javításának módjával kapcsolatos tanácsadás;
  - b) kérésükre technikai segítségnyújtás jelentős vagy lényeges hatású biztonsági események esetében;
  - c) a sebezhetőségek, informatikai hibák és biztonsági események elemzése.

E feladatok ellátása során az Ügynökség és a CERT-EU strukturált együttműködést folytat a szinergiák kihasználása érdekében, különösen ami az operatív szempontokat illeti.

- (5) Két vagy több érintett tagállam kérésére – és kizárólag a jövőbeni biztonsági események megelőzésére vonatkozó tanácsadás céljából – az Ügynökség támogatást nyújt az (EU) 2016/1148 irányelv értelmében jelentős vagy lényeges hatású biztonsági eseményeknek az érintett vállalkozások általi bejelentését követő utólagos technikai vizsgálatához, vagy maga hajtja végre ezt a vizsgálatot. Az Ügynökség az érintett tagállamok egyetértésével a Bizottság kellően indokolt kérésére is végez ilyen vizsgálatot a kettőnél több tagállamot érintő biztonsági események esetében.

A vizsgálat tárgyát és a vizsgálat lefolytatása során követendő eljárást az érintett tagállamok és az Ügynökség határozza meg az ugyanazon biztonsági eseménnyel kapcsolatos, folyamatban lévő bünygyi nyomozás sérelme nélkül. A vizsgálat az

Ügynökség által összeállított végleges technikai jelentéssel zárul, amely elsősorban az érintett tagállamok és vállalkozás(ok) által benyújtott és az érintett tagállamokkal egyeztetett információkon és észrevételeken alapul. A jelentésről a jövőbeli biztonsági események megelőzésére vonatkozó ajánlásokra összpontosító összefoglalást kell készíteni, amelyet meg kell osztani a CSIRT-hálózattal.

- (6) Az Ügynökség évente kiberbiztonsági gyakorlatokat szervez uniós szinten, és kérésükre támogatja a tagállamokat, valamint az uniós intézményeket, hivatalokat és szerveket saját gyakorlataik megszervezésében. Az uniós szintű éves gyakorlatoknak technikai, operatív és stratégiai elemeket is magukban kell foglalniuk, és segíteniük kell a nagyszabású, határokon átnyúló kiberbiztonsági eseményekre való uniós szintű, együttműködésen alapuló reagálás előkészítését. Az Ügynökség emellett hozzájárul és adott esetben segítséget nyújt az ágazati kiberbiztonsági gyakorlatok megszervezéséhez a megfelelő ágazati információmegosztási és analitikai központokkal együtt, és ez utóbbiak számára lehetővé teszi az uniós szintű kiberbiztonsági gyakorlatokban való részvételt.
- (7) Az Ügynökség rendszeres uniós kiberbiztonsági technikai helyzetjelentést készít a biztonsági eseményekről és fenyegetésekről, amelyek nyilvánosan hozzáférhető információkon, az Ügynökség saját elemzésén, valamint többek között a következő szervezetek által rendelkezésre bocsátott jelentéseken alapulnak: a tagállami CSIRT-ek (önkéntes alapon) vagy a kiberbiztonsági irányelvvel létrehozott egyedüli kapcsolattartó pontok (kiberbiztonsági irányelv, 14. cikk (5) bekezdés), az Europol Számítástechnikai Bűnözés Elleni Európai Központja (EC3) és a CERT-EU.
- (8) Az Ügynökség hozzájárul a kiberbiztonsággal kapcsolatos nagyszabású, határokon átnyúló biztonsági eseményekre vagy válságokra adott, együttműködésen alapuló uniós vagy tagállami szintű reagálás kidolgozásához, elsősorban az alábbiak révén:
  - a) a tagállami forrásokból származó jelentések összesítése a közös helyzetismeret kialakításához való hozzájárulás céljából;
  - b) a CSIRT-hálózat és az uniós technikai és politikai döntéshozók közötti hatékony információcsere és a megfelelő beavatkozási szint meghatározására irányuló mechanizmusok biztosítása;
  - c) a biztonsági események vagy válságok technikai kezelésének támogatása, beleértve a technikai megoldások tagállamok közötti megosztásának elősegítését;
  - d) a biztonsági eseménnyel vagy a válsággal kapcsolatos nyilvános kommunikáció támogatása;
  - e) az együttműködési tervek tesztelése a biztonsági eseményekre vagy válságokra való reagálás képességének tekintetében.

#### 8. cikk

#### **A piaccal, a kiberbiztonsági tanúsítással és a szabványosítással kapcsolatos feladatok**

Az Ügynökség:

- a) támogatja és előmozdítja az IKT-termékek és -szolgáltatások – e rendelet III. címében meghatározott – kiberbiztonsági tanúsítására vonatkozó uniós szakpolitika kidolgozását és végrehajtását, az alábbiak révén:

1. európai kiberbiztonsági tanúsítási rendszerekre irányuló javaslatok kidolgozása IKT-termékekre és -szolgáltatásokra vonatkozóan e rendelet 44. cikkének megfelelően;
  2. a Bizottság támogatása az európai kiberbiztonsági tanúsítási csoport titkárságának e rendelet 53. cikke szerinti biztosításában;
  3. az IKT-termékek és -szolgáltatások kiberbiztonsági előírásaira vonatkozó iránymutatások összeállítása és közzététele, illetve bevált módszerek kialakítása a nemzeti tanúsításfelügyeleti hatóságokkal és az ágazattal együttműködve;
- b) előmozdítja a kockázatkezelésre és az IKT-termékek és -szolgáltatások biztonságára vonatkozó európai és nemzetközi szabványok kidolgozását és használatát, valamint a tagállamokkal együttműködésben tanácsot ad és iránymutatásokat készít az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra vonatkozó biztonsági követelményekkel kapcsolatos műszaki területekkel, valamint a már hatályos szabványokkal, köztük a tagállamok nemzeti szabványaival kapcsolatban az (EU) 2016/1148 irányelv 19. cikkének (2) bekezdése alapján;
- c) rendszeresen elemzi a kiberbiztonsági piac keresleti és kínálati oldalára jellemző főbb tendenciákat, és gondoskodik ezen elemzések terjesztéséről az Unió kiberbiztonsági piacának megerősítése céljából.

#### *9. cikk*

#### **Az ismeretekkel, a tájékoztatással és a tudatosság növelésével kapcsolatos feladatok**

Az Ügynökség:

- a) elemzéseket készít a kialakulóban lévő technológiákról, és tematikus értékeléseket végez a technológiai innovációknak a kiberbiztonságra gyakorolt várható társadalmi, jogi, gazdasági és szabályozási hatásairól;
- b) elvégzi a kiberbiztonsági fenyegetések és események hosszú távú stratégiai elemzését az új tendenciák azonosítása és a kiberbiztonsággal kapcsolatos problémák megelőzése érdekében;
- c) a tagállami hatóságok szakértőivel együttműködésben tanácsot és útmutatást ad, illetve bevált módszereket bocsát rendelkezésre a hálózati és információs rendszerek biztonságával, különösen az internetes infrastruktúra és az (EU) 2016/1148 irányelv II. mellékletében felsorolt ágazatokat támogató infrastruktúrák biztonságával kapcsolatban;
- d) az uniós intézmények, hivatalok és szervek által a kiberbiztonsággal kapcsolatban rendelkezésre bocsátott információkat összegyűjti, strukturálja és a nyilvánosság számára elérhetővé teszi egy külön erre a célra létrehozott portálon;
- e) növeli a kiberbiztonsági kockázatokkal kapcsolatos tudatosságot, és magánszemélyeknek és szervezeteknek címzett, egyedi felhasználói iránymutatást ad a már bevált módszerekkel kapcsolatban;
- f) összegyűjti és elemzi a jelentős biztonsági eseményekkel kapcsolatos nyilvánosan hozzáférhető információkat, valamint jelentéseket készít annak érdekében, hogy Unió-szerte iránymutatást lehessen nyújtani a vállalkozások és a magánszemélyek számára;

- g) rendszeres tájékoztató kampányokat szervez a tagállamokkal, valamint az uniós intézményekkel, szervekkel és hivatalokkal együttműködésben a kiberbiztonság fokozása és láthatóságának növelése érdekében.

#### *10. cikk*

#### **A kutatással és az innovációval kapcsolatos feladatok**

A kutatás és az innováció tekintetében az Ügynökség:

- a) tanácsokkal látja el az Uniót és a tagállamokat a tekintetben, hogy a kiberbiztonság területén milyen kutatási szükségleteknek és prioritásoknak kell eleget tenni egyrészt ahhoz, hogy hatékonyan lehessen reagálni a jelenlegi és jövőbeli kockázatokra és fenyegetésekre, beleértve az új és kialakulóban lévő információs és kommunikációs technológiákat érintő kockázatok és fenyegetések is, másrészt pedig ahhoz, hogy eredményesen lehessen alkalmazni a kockázatmegelőző technológiákat;
- b) részt vesz a kutatás és az innováció finanszírozását célzó programok megvalósítási szakaszában, amennyiben a Bizottság felruházta az ehhez szükséges felhatalmazással, vagy kedvezményezettként.

#### *11. cikk*

#### **A nemzetközi együttműködéssel kapcsolatos feladatok**

Az Ügynökség a kiberbiztonsággal kapcsolatos kérdésekre vonatkozó nemzetközi együttműködés elősegítése érdekében hozzájárul a harmadik országokkal és nemzetközi szervezetekkel folytatandó együttműködésre irányuló uniós erőfeszítésekhez azáltal, hogy:

- a) szükség esetén megfigyelőként részt vesz a nemzetközi gyakorlatok szervezésében, valamint az ilyen gyakorlatok eredményeiről elemzést és jelentést készít az igazgatótanácsnak;
- b) a Bizottság kérésére elősegíti a bevált módszerek megosztását az érintett nemzetközi szervezetek között;
- c) kérésre szakértelemmel támogatja a Bizottságot.

## **II. FEJEZET AZ ÜGYNÖKSÉG FELÉPÍTÉSE**

#### *12. cikk*

#### **Szerkezet**

Az Ügynökség igazgatási és irányítási struktúráját a következők alkotják:

- a) az igazgatótanács, amely a 14. cikkben meghatározott feladatokat látja el;
- b) a felügyelőtestület, amely a 18. cikkben meghatározott feladatokat látja el;
- c) az ügyvezető igazgató, aki a 19. cikkben meghatározott feladatokat látja el, valamint



- d) az érdekeltek állandó csoportja, amely a 20. cikkben meghatározott feladatokat látja el.

## **1. SZAKASZ IGAZGATÓTANÁCS**

### *13. cikk*

#### ***Az igazgatótanács összetétele***

- (1) Az igazgatótanács tagállamonként egy-egy képviselőből és a Bizottság által kijelölt két képviselőből áll. Valamennyi képviselő rendelkezik szavazati joggal.
- (2) Az igazgatótanács minden egyes tagja rendelkezik egy póttaggal, aki képviseli őt távollétében.
- (3) Az igazgatótanács tagjait és a póttagokat a kiberbiztonság terén szerzett ismereteik alapján nevezik ki, a megfelelő vezetői, igazgatási és költségvetési készségek figyelembevételével. Az igazgatótanács munkájának folytonosságát biztosítandó, a Bizottság és a tagállamok törekednek arra, hogy képviselőik ne cserélődjenek túl gyakran az igazgatótanácsban. A Bizottság és a tagállamok arra törekednek, hogy a nők és férfiak egyenlő arányban legyenek képviselve az igazgatótanácsban.
- (4) Az igazgatótanács tagjainak és póttagjainak hivatali ideje négy év. A hivatali idő megújítható.

### *14. cikk*

#### ***Az igazgatótanács feladatai***

- (1) Az igazgatótanács:
  - a) meghatározza az Ügynökség működésének általános irányát, és gondoskodik arról, hogy az Ügynökség az e rendeletben megállapított szabályoknak és elveknek megfelelően végezze tevékenységét. Biztosítja továbbá, hogy az Ügynökség munkája összhangban legyen a tagállamok által és az Unió szintjén folytatott tevékenységekkel;
  - b) elfogadja az Ügynökség 21. cikkben említett egységes programozási dokumentumának tervezetét, mielőtt a dokumentumot benyújtánák a Bizottsághoz véleményezésre;
  - c) a Bizottság véleményének figyelembevételével, a tagok szavazatainak kétharmados többségével és a 17. cikknek megfelelően elfogadja az Ügynökség egységes programozási dokumentumát;
  - d) a tagok szavazatainak kétharmados többségével elfogadja az Ügynökség éves költségvetését, és ellátja az Ügynökség költségvetéséhez kapcsolódó, a III. fejezet szerinti egyéb feladatokat;
  - e) értékeli, majd elfogadja az Ügynökség tevékenységéről szóló összevont éves jelentést, és a következő év július 1-jéig megküldi mind a jelentést, mind az értékelését az Európai Parlament, a Tanács, a Bizottság és a Számvevőszék részére. Az éves jelentésnek tartalmaznia kell az elszámolásokat, és ismertetnie kell, hogy az Ügynökség teljesítette-e teljesítménymutatóit. Az éves jelentést közzé kell tenni;

- f) elfogadja az Ügynökségre vonatkozó pénzügyi szabályzatot a 29. cikknek megfelelően;
- g) csalás elleni stratégiát fogad el, amely – figyelemmel a végrehajtandó intézkedések költség-haszon elemzésére – arányos a csalási kockázatokkal;
- h) az összeférhetetlenségek megelőzésére és kezelésére vonatkozó szabályokat fogad el az igazgatótanács tagjai tekintetében;
- i) biztosítja az Európai Csalás Elleni Hivatal (OLAF) vizsgálataiból és a különböző belső vagy külső ellenőrzési jelentésekből és értékelésekből következő megállapítások és ajánlások megfelelő nyomon követését;
- j) elfogadja eljárási szabályzatát;
- k) a (2) bekezdésnek megfelelően az Ügynökség személyzete vonatkozásában gyakorolja a tisztviselők személyzeti szabályzatában a kinevezésre jogosult hatóságra, illetve az Európai Unió egyéb alkalmazottaira vonatkozó alkalmazási feltételekben a munkaszerződések megkötésére jogosult hatóságra ruházott hatásköröket („a kinevezésre jogosult hatóság hatáskörei”);
- l) a személyzeti szabályzat 110. cikkében előírt eljárással összhangban szabályokat fogad el a személyzeti szabályzat és az egyéb alkalmazottakra vonatkozó alkalmazási feltételek végrehajtásával kapcsolatban;
- m) e rendelet 33. cikkének megfelelően kinevezi az ügyvezető igazgatót, és adott esetben meghosszabbítja hivatali idejét, vagy felmenti hivatalából;
- n) kinevez egy tisztviselőt, aki a számvitelért felelős, és aki feladatai ellátása során teljes mértékben függetlenül jár el (lehet a Bizottság számvitelért felelős tisztviselője is);
- o) meghozza az Ügynökség belső felépítésének kialakításával és szükség szerint annak módosításával kapcsolatos összes döntést, az Ügynökség tevékenységével kapcsolatos igények és a hatékony és eredményes költségvetési gazdálkodás figyelembevételével;
- p) a 7. és a 39. cikknek megfelelően engedélyezi munkamegállapodások megkötését.

- (2) Az igazgatótanács a személyzeti szabályzat 110. cikkével összhangban, a személyzeti szabályzat 2. cikkének (1) bekezdése és az egyéb alkalmazottakra vonatkozó alkalmazási feltételek 6. cikke alapján határozat elfogadása útján kinevezésre jogosult hatósági hatásköröket ruház az ügyvezető igazgatóra, és meghatározza azon feltételeket, amelyek mellett a hatáskör-átruházás felfüggeszthető. Az ügyvezető igazgató jogosult e hatáskörök további átruházására.
- (3) Amennyiben rendkívüli körülmények szükségessé teszik, az igazgatótanács határozatban ideiglenesen felfüggesztheti a kinevezésre jogosult hatóság hatásköreinek az ügyvezető igazgatóra történő átruházását és az utóbbi általi további átruházását, és azokat maga gyakorolhatja, vagy valamelyik tagjára vagy a személyzetnek az ügyvezető igazgatótól eltérő tagjára ruházhatja.

#### *15. cikk*

##### ***Az igazgatótanács elnöke***

Az igazgatótanács a tagok szavazatainak kétharmados többségével négy évre elnököt és elnökhelyettest választ tagjai közül; e személyek hivatali ideje egy alkalommal megújítható. Ha azonban igazgatótanács tagjuk hivatali idejük alatt bármikor megszűnik, ugyanezen a napon hivatali idejük is automatikusan megszűnik. Az elnökhelyettes hivatalból helyettesíti az elnököt abban az esetben, ha az elnök nem tudja ellátni feladatait.

#### *16. cikk*

##### ***Az igazgatótanács ülései***

- (1) Az igazgatótanács üléseit az elnök hívja össze.
- (2) Az igazgatótanács évente legalább két rendes ülést tart. Az igazgatótanács az elnök kérésére, a Bizottság kérésére vagy tagjai legalább egyharmadának kérésére rendkívüli ülést is tart.
- (3) Az ügyvezető igazgató – szavazati jog nélkül – részt vesz az igazgatótanács ülésein.
- (4) Az érdekeltek állandó csoportjának tagjai az elnök felkérésére szavazati jog nélkül részt vehetnek az igazgatótanács ülésein.
- (5) Az igazgatótanács tagjai és a póttagok – az eljárási szabályzatra figyelemmel – tanácsadók és szakértők segítségét is igénybe vehetik az üléseken.
- (6) Az igazgatótanács számára az Ügynökség biztosítja a titkárságot.

#### *17. cikk*

##### ***Az igazgatótanács szavazási szabályai***

- (1) Az igazgatótanács tagjainak többségi szavazatával határoz.
- (2) Az egységes programozási dokumentum, az éves költségvetés, az ügyvezető igazgató kinevezése, hivatali idejének meghosszabbítása vagy hivatalból való felmentése tekintetében a teljes létszámú igazgatótanács szavazatainak kétharmados többsége szükséges.
- (3) Minden tag egy szavazattal rendelkezik. Valamely tag távolléte esetén a póttag jogosult a távol lévő tag szavazati jogának gyakorlására.
- (4) Az elnök részt vesz a szavazásban.
- (5) Az ügyvezető igazgató nem vesz részt a szavazásban.
- (6) Az igazgatótanács eljárási szabályzata részletesen rendelkezik a szavazás szabályairól és különösen arról, hogy egy tag milyen feltételek mellett járhat el egy másik tag nevében.

## **2. SZAKASZ FELÜGYELŐTESTÜLET**

#### *18. cikk*

##### ***Felügyelőtestület***

- (1) Az igazgatótanács munkáját felügyelőtestület támogatja.

- (2) A felügyelőtestület:
- a) előkészíti az igazgatótanács által elfogadandó határozatokat;
  - b) az igazgatótanáccsal együtt gondoskodik az OLAF által végzett vizsgálatokból, valamint a különböző belső vagy külső ellenőrzési jelentésekből és értékelésekből következő megállapítások és ajánlások megfelelő nyomon követéséről;
  - c) az ügyvezető igazgató 19. cikkben meghatározott feladatainak sérelme nélkül segítséget nyújt és tanácsot ad az ügyvezető igazgató számára az igazgatótanács adminisztratív és költségvetési ügyekben hozott határozatainak végrehajtásában a 19. cikk értelmében.
- (3) A felügyelőtestület összetétele a következő: az igazgatótanácsi tagok közül kinevezett öt tag, köztük az igazgatótanács elnöke, aki betöltheti a felügyelőtestület elnöki tisztségét is, valamint a Bizottság egyik képviselője. Az ügyvezető igazgató részt vesz a felügyelőtestület ülésein, de szavazati joggal nem rendelkezik.
- (4) A felügyelőtestület tagjainak hivatali ideje négy év. A hivatali idő megújítható.
- (5) A felügyelőtestület legalább háromhavonta ülésezik. A felügyelőtestület elnöke a tagok kérésére további üléseket hív össze.
- (6) A felügyelőtestület eljárási szabályzatát az igazgatótanács állapítja meg.
- (7) Sürgős esetekben a felügyelőtestület az igazgatótanács nevében meghozhat bizonyos ideiglenes határozatokat, különösen az igazgatási irányítást érintő kérdésekben, ideértve a kinevezésre jogosult hatóság hatásköreinek átruházásának felfüggesztését és a költségvetési kérdéseket is.

### **3. SZAKASZ**

#### **ÜGYVEZETŐ IGAZGATÓ**

##### *19. cikk*

##### ***Az ügyvezető igazgató feladatai***

- (1) Az Ügynökséget az ügyvezető igazgató vezeti, aki feladatai ellátása során függetlenül jár el. Az ügyvezető igazgató a tevékenységéért az igazgatótanácsnak tartozik felelősséggel.
- (2) Az ügyvezető igazgató, amennyiben erre felkérést kap, beszámol az Európai Parlamentnek feladatai ellátásáról. A Tanács is felkérheti az ügyvezető igazgatót, hogy számoljon be feladatai ellátásáról.
- (3) Az ügyvezető igazgató feladatai a következők:
- a) az Ügynökség napi ügyvitele;
  - b) az igazgatótanács által elfogadott határozatok végrehajtása;
  - c) az egységes programozási dokumentum tervezetének elkészítése és annak benyújtása az igazgatótanácshoz jóváhagyatás céljából a Bizottsághoz való benyújtást megelőzően;
  - d) az egységes programozási dokumentum végrehajtása, majd beszámolás az igazgatótanácsnak;

- e) összevont éves jelentés készítése az Ügynökség tevékenységéről és annak benyújtása az igazgatótanácshoz értékelésre és elfogadásra;
- f) az utólagos értékelések megállapításain alapuló cselekvési terv elkészítése és kétfévente jelentéstétel az eredményekről a Bizottságnak;
- g) cselekvési terv elkészítése a belső vagy külső ellenőrzési jelentésekből, valamint az Európai Csalás Elleni Hivatal (OLAF) vizsgálataiból származó megállapítások nyomán meghozandó intézkedésekről, évente két alkalommal jelentéstétel az eredményekről a Bizottságnak, valamint rendszeresen az igazgatótanácsnak;
- h) az Ügynökség pénzügyi szabályzata tervezetének elkészítése;
- i) az Ügynökség tervezett bevételekre és kiadásokra vonatkozó kimutatástervezetének elkészítése és költségvetésének végrehajtása;
- j) az Unió pénzügyi érdekeinek védelme a csalásra, a korrupcióra és más jogellenes tevékenységekre irányuló megelőző intézkedések alkalmazásával, hatékony ellenőrzésekkel és – ha szabálytalanságok feltárására kerül sor – a helytelenül kifizetett összegek visszatéríttetésével, valamint szükség esetén hatékony, arányos és visszatartó erejű közigazgatási vagy pénzügyi szankciókkal;
- k) az Ügynökség csalásellenes stratégiájának elkészítése és az igazgatótanács elé terjesztése jóváhagyás céljából;
- l) kapcsolat kialakítása és fenntartása az üzleti élet szereplőivel és a fogyasztói szervezetekkel, az érdekeltekkel folytatott rendszeres párbeszéd biztosítása érdekében;
- m) az e rendeletben az ügyvezető igazgatóra vonatkozóan előírt további feladatok.

(4) Szükség esetén és az Ügynökség megbízatása által kijelölt keretek között, valamint az Ügynökség céljaival és feladataival összhangban az ügyvezető igazgató eseti munkacsoportokat hozhat létre, amelyek többek között az illetékes tagállami hatóságok szakértőiből állnak. Az igazgatótanácsot erről előzetesen tájékoztatni kell. A munkacsoportok összetételével, a munkacsoportban részt vevő szakértőknek az ügyvezető igazgató általi kinevezésével, valamint a munkacsoportok működésével kapcsolatos eljárásokat az Ügynökség belső működési szabályzatában kell meghatározni.

(5) Az ügyvezető igazgató dönt arról, hogy az Ügynökség feladatainak hatékony és eredményes végrehajtása céljából szükséges-e munkatársakat rendelni egy vagy több tagállamba. A helyi irodára vonatkozó döntést megelőzően az ügyvezető igazgató megszerzi a Bizottság, az igazgatótanács és az érintett tagállam(ok) előzetes hozzájárulását. Az idevágó határozatban oly módon kell megállapítani a helyi iroda által ellátandó tevékenységek körét, hogy megelőzhetők legyenek a szükségtelen költségek és az Ügynökségen belüli igazgatási feladatkörök közötti indokolatlan átfedések. Szükség esetén erről megállapodásra kell jutni az érintett tagállammal vagy tagállamokkal.

## **4. SZAKASZ**

### **AZ ÉRDEKELTEK ÁLLANDÓ CSOPORTJA**

#### *20. cikk*

#### ***Az érdekeltek állandó csoportja***

- (1) Az igazgatótanács az ügyvezető igazgató javaslatára létrehozza az érdekeltek állandó csoportját, amely egyfelől a releváns érdekelt feleket – IKT-ágazat, a nyilvános elektronikus hírközlő hálózatokat és nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat biztosító vállalkozások, a fogyasztói csoportok és a kiberbiztonság területén tevékenykedő tudományos szakemberek – képviselő elismert szakértőkből, másfelől pedig az [Európai Elektronikus Hírközlési Kódex létrehozásáról szóló] irányelv értelmében bejelentett nemzeti szabályozó hatóságok, valamint a bűnüldöző hatóságok és a magánélet védelmével foglalkozó felügyeleti hatóságok képviselőiből áll.
- (2) Az érdekeltek állandó csoportjának létszámával, közelebbről annak összetételével, tagjainak az igazgatótanács általi kinevezésével, az ügyvezető igazgató javaslatával, valamint a csoport működésével kapcsolatos eljárásokat az Ügynökség belső működési szabályzatában kell meghatározni, és azokat nyilvánosságra kell hozni.
- (3) Az érdekeltek állandó csoportjában az elnöki teendőket az ügyvezető igazgató vagy az általa eseti alapon kinevezett személy látja el.
- (4) Az érdekeltek állandó csoportja tagjainak hivatali ideje két és fél évre szól. Az érdekeltek állandó csoportjának nem lehetnek olyan tagjai, akik az igazgatótanácsnak is tagjai. Az érdekeltek állandó csoportjának ülésein jelen lehetnek, és munkájában részt vehetnek a Bizottságtól és a tagállamokból érkező szakértők. Az érdekeltek állandó csoportjának üléseire és az e csoport munkájában való részvételre az ügyvezető igazgató által relevánsnak ítélt egyéb szervek képviselői is meghívhatók, akik nem tagjai az érdekeltek állandó csoportjának.
- (5) Az érdekeltek állandó csoportja tanácsadással segíti az Ügynökséget tevékenységeinek ellátásában. A csoport különösen az Ügynökség munkaprogramjára vonatkozó javaslat elkészítéséhez és a releváns érdekeltekkel a munkaprogramot érintő valamennyi kérdéstről folytatandó párbeszéd biztosításához ad tanácsot az ügyvezető igazgatónak.

## **5. SZAKASZ**

### **MŰKÖDÉS**

#### *21. cikk*

#### ***Egységes programozási dokumentum***

- (1) Az Ügynökség a többéves és éves munkaprogramját tartalmazó egységes programozási dokumentumnak megfelelően végzi munkáját, amelynek az Ügynökség valamennyi tervezett tevékenységét magában kell foglalnia.

- (2) Az ügyvezető igazgató – az 1271/2013/EU felhatalmazáson alapuló bizottsági rendelet<sup>36</sup> 32. cikkével összhangban és a Bizottság által meghatározott iránymutatások figyelembevételével – minden évben elkészíti a többéves és éves programozást tartalmazó egységes programozási dokumentum tervezetét, amely a megfelelő humán- és pénzügyi erőforrások tervezésére is kiterjed.
- (3) Az igazgatótanács minden évben november 30-ig elfogadja az (1) bekezdésben említett egységes programozási dokumentumot, és a rákövetkező évben legkésőbb január 31-ig továbbítja azt az Európai Parlamentnek, a Tanácsnak és a Bizottságnak; hasonlóképpen gondoskodik a dokumentum később aktualizált változatainak továbbításáról is.
- (4) Az egységes programozási dokumentum az Európai Unió általános költségvetésének végleges elfogadását követően válik véglegessé, és szükség esetén annak megfelelően ki kell igazítani.
- (5) Az éves munkaprogramban a részletes célkitűzéseket és az elvárt eredményeket, valamint a kapcsolódó teljesítménymutatókat kell meghatározni. Emellett – a tevékenység alapú költségvetés-tervezés és irányítás elveivel összhangban – ismertetni kell benne a finanszírozandó fellépéseket, és meg kell jelölni az egyes fellépésekhez rendelt pénzügyi és humán erőforrásokat. Az éves munkaprogramnak összhangban kell állnia a (7) bekezdésben említett többéves munkaprogrammal. Egyértelműen jeleznie kell, hogy az előző pénzügyi évhez képest az Ügynökség mely feladata új, változott vagy szűnt meg.
- (6) Amikor az Ügynökség új feladatot kap, az igazgatótanács módosítja az elfogadott éves munkaprogramot. Az éves munkaprogram minden lényeges módosítását ugyanazzal az eljárással kell elfogadni, mint az eredeti éves munkaprogramot. Az igazgatótanács az éves munkaprogram nem lényeges módosítására vonatkozó hatáskörét az ügyvezető igazgatóra ruházhatja.
- (7) A többéves munkaprogramnak az átfogó stratégiai programozást kell meghatároznia, ideértve a célkitűzéseket, az elvárt eredményeket és a teljesítménymutatókat is. Ismertetnie kell az erőforrások programozását, ideértve a többéves költségvetést és a személyzeti tervet is.
- (8) Az erőforrások programozását évente aktualizálni kell. A stratégiai programozást indokolt esetben – és különösen az 56. cikkben említett értékelés kimenetelének figyelembevétele céljából – aktualizálni kell.

## *22. cikk*

### ***Érdekeltségi nyilatkozat***

- (1) Az igazgatótanács tagjai, az ügyvezető igazgató és a tagállamok által ideiglenesen kirendelt tisztviselők mindegyike kötelezettségvállalási nyilatkozatot tesz, továbbá nyilatkozik arról, hogy van-e olyan közvetlen vagy közvetett érdeke, amelyről feltehető, hogy függetlenségét befolyásolhatja. A nyilatkozatnak pontosnak és teljes

---

<sup>36</sup>

A Bizottság 1271/2013/EU felhatalmazáson alapuló rendelete (2013. szeptember 30.) a 966/2012/EU, Euratom európai parlamenti és tanácsi rendelet 208. cikkében említett szervekre vonatkozó pénzügyi keretszabályzatról (HL L 328., 2013.12.7., 42. o.).

körűnek kell lennie, azt évente írásban kell megtenni, és szükség esetén aktualizálni kell.

- (2) Az igazgatótanács tagjai, az ügyvezető igazgató és az eseti munkacsoportok munkájában részt vevő külső szakértők mindegyike legkésőbb az adott ülés kezdetén pontosan és teljeskörűen nyilatkozik az egyes napirendi pontokkal kapcsolatos minden olyan érdekéről, amelyről feltehető, hogy függetlenségét befolyásolhatja, a kérdéses napirendi pontok megvitatásában való részvételtől és az azokról való szavazástól pedig tartózkodik.
- (3) Az Ügynökség belső működési szabályzatában megállapítja az (1) és a (2) bekezdésben említett érdekeltségi nyilatkozatokkal kapcsolatos szabályokra vonatkozó gyakorlati rendelkezéseket.

### *23. cikk* **Átláthatóság**

- (1) Az Ügynökség tevékenységét magas fokú átláthatóság mellett, a 25. cikknek megfelelően végzi.
- (2) Az Ügynökség biztosítja, hogy a nyilvánosság és minden érdekelt fél – különösen az Ügynökség munkájának eredményeiről – megfelelő, tárgyilagos, megbízható és könnyen hozzáférhető tájékoztatást kapjon. Az Ügynökség továbbá köteles a nyilvánosság elé tárni a 22. cikkel összhangban tett érdekeltségi nyilatkozatokat.
- (3) Az igazgatótanács az ügyvezető igazgató javaslatára engedélyezheti, hogy meghatározott érdekelt felek az Ügynökség egyes tevékenységeiben megfigyelőként részt vegyenek.
- (4) Az Ügynökség belső működési szabályzatában megállapítja az (1) és a (2) bekezdésben említett átláthatósági szabályok végrehajtására vonatkozó gyakorlati rendelkezéseket.

### *24. cikk* **Titoktartás**

- (1) A 25. cikk sérelme nélkül az Ügynökség nem adhatja tovább harmadik felek részére az általa kezelt vagy hozzá beérkezett olyan információkat, amelyek tekintetében indokolással ellátott kérelmet nyújtottak be bizalmas kezelés iránt, az információk teljes egészére vagy egy részére vonatkozóan.
- (2) Az igazgatótanács tagjai, az ügyvezető igazgató, az érdekeltek állandó csoportjának tagjai, az eseti munkacsoportok munkájában részt vevő külső szakértők és az Ügynökség személyzetének tagjai – beleértve a tagállamok által ideiglenesen kirendelt tisztviselőket is – feladataik megszűnte után is az Európai Unió működéséről szóló szerződés (EUMSZ) 339. cikke szerinti titoktartási kötelezettségek hatálya alá tartoznak.
- (3) Az Ügynökség belső működési szabályzatában megállapítja az (1) és (2) bekezdésben említett titoktartási szabályok végrehajtására vonatkozó gyakorlati rendelkezéseket.
- (4) Amennyiben az Ügynökség feladatainak ellátásához szükséges, az igazgatótanács lehetővé teszi az Ügynökség számára, hogy minősített adatokat is kezeljen. Ebben az



esetben az igazgatótanács a Bizottság szolgálataival egyetértésben belső működési szabályzatot fogad el az (EU, Euratom) 2015/443<sup>37</sup> és az (EU, Euratom) 2015/444<sup>38</sup> bizottsági határozatban megállapított biztonsági elvek alkalmazásáról. Ennek a szabályzatnak a minősített adatok cseréjére, feldolgozására és tárolására vonatkozó rendelkezéseket kell tartalmaznia.

#### 25. cikk

##### ***Dokumentumokhoz való hozzáférés***

- (1) Az 1049/2001/EK rendelet az Ügynökség birtokában lévő dokumentumokra is vonatkozik.
- (2) Az igazgatótanács az Ügynökség létrejöttét követő hat hónapon belül elfogadja az 1049/2001/EK rendelet végrehajtására vonatkozó rendelkezéseket.
- (3) Az Ügynökség által az 1049/2001/EK rendelet 8. cikke alapján elfogadott határozatokkal szemben az EUMSZ 228. cikke alapján az ombudsmannál panasz tehető, illetve az EUMSZ 263. cikke alapján az Európai Unió Bíróságánál kereset indítható.

### III. FEJEZET

## A KÖLTSÉGVETÉS MEGÁLLAPÍTÁSA ÉS SZERKEZETE

#### 26. cikk

##### ***A költségvetés megállapítása***

- (1) Az ügyvezető igazgató minden évben elkészíti és a létszámterv tervezetével együtt továbbítja az igazgatótanácsnak az Ügynökség következő pénzügyi évre tervezett bevételeire és kiadásaira vonatkozó kimutatás tervezetét. A bevételeknek és a kiadásoknak egyensúlyban kell lenniük.
- (2) Az igazgatótanács a tervezett bevételekről és kiadásokról szóló kimutatás (1) bekezdésben említett tervezete alapján minden évben elkészíti az Ügynökség következő költségvetési évre vonatkozó tervezett bevételeiről és kiadásairól szóló kimutatást.
- (3) Az igazgatótanács minden évben január 31-ig megküldi a (2) bekezdésben említett, az egységes programozási dokumentum részét képező kimutatást a Bizottságnak és azoknak a harmadik országoknak, amelyekkel az Unió a 39. cikk értelmében megállapodást kötött.
- (4) A Bizottság e kimutatás alapján bevezeti az Unió költségvetésének tervezetébe a létszámtervhez szükségesnek ítélt hozzájárulásokat és az általános költségvetést terhelő hozzájárulás összegét, majd az EUMSZ 313. és 314. cikkének megfelelően a tervezetet benyújtja az Európai Parlamentnek és a Tanácsnak.

<sup>37</sup> [A Bizottság \(EU, Euratom\) 2015/443 határozata \(2015. március 13.\) a Bizottságon belüli biztonságról](#) (HL L 72., 2015.3.17., 41. o.).

<sup>38</sup> [A Bizottság \(EU, Euratom\) 2015/444 határozata \(2015. március 13.\) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról](#) (HL L 72., 2015.3.17., 53. o.).

- (5) Az Európai Parlament és a Tanács engedélyezi az Ügynökségnek juttatandó hozzájárulásokra vonatkozó előirányzatokat.
- (6) Az Európai Parlament és a Tanács elfogadja az Ügynökség létszámtervét.
- (7) Az igazgatótanács az egységes programozási dokumentummal együtt elfogadja az Ügynökség költségvetését. A költségvetés az Unió általános költségvetésének végleges elfogadását követően válik véglegessé. Az igazgatótanács az Ügynökség költségvetését és egységes programozási dokumentumát szükség szerint az Unió általános költségvetéséhez igazítja.

#### *27. cikk*

##### ***A költségvetés szerkezete***

- (1) Az Ügynökség bevételei az egyéb források sérelme nélkül a következőkből származnak:
  - a) az uniós költségvetésből kapott hozzájárulás;
  - b) a meghatározott kiadási tételekhez rendelt bevételek az Ügynökség 29. cikkben említett pénzügyi szabályzatával összhangban;
  - c) uniós finanszírozás hozzájárulási megállapodások vagy eseti vissza nem térítendő támogatások formájában a 29. cikkben említett pénzügyi szabályzattal, valamint az Unió szakpolitikáit támogató kapcsolódó jogi aktusokban foglalt rendelkezésekkel összhangban;
  - d) hozzájárulások azon harmadik országoktól, amelyek a 39. cikk értelmében részt vesznek az Ügynökség munkájában;
  - e) a tagállamok által pénzben vagy természetben nyújtott önkéntes hozzájárulások; az önkéntes hozzájárulást nyújtó tagállamok azonban nem tarthatnak igényt semmilyen különös jogra vagy ellenszolgáltatásra e hozzájárulásért cserébe.
- (2) Az Ügynökség kiadásait a személyzeti, az adminisztratív, a műszaki támogatási, az infrastrukturális és a működési kiadások, valamint a harmadik felekkel kötött szerződésekből eredő kiadások alkotják.

#### *28. cikk*

##### ***A költségvetés végrehajtása***

- (1) Az Ügynökség költségvetésének végrehajtásáért az ügyvezető igazgató felel.
- (2) A Bizottság belső ellenőre ugyanazokkal a hatáskörökkel rendelkezik az Ügynökséggel szemben, mint a Bizottság szervezeti egységeivel szemben.
- (3) A mindenkorai pénzügyi évet követő év március 1-jéig (N+1. év március 1.) az Ügynökség számvitelért felelős tisztviselője megküldi az előzetes beszámolót a Bizottság számvitelért felelős tisztviselőjének és a Számvevőszéknek.
- (4) Az Ügynökség előzetes beszámolójára vonatkozó számvevőszéki észrevételek kézhezvételét követően az Ügynökség számvitelért felelős tisztviselője saját felelősségére elkészíti az Ügynökség végleges beszámolóját.
- (5) Az ügyvezető igazgató a végleges beszámolót véleményezésre benyújtja az igazgatótanácshoz.

- (6) Az ügyvezető igazgató N+1. év március 31-ig megküldi az Európai Parlamentnek, a Tanácsnak, a Bizottságnak és a Számvevőszéknek a költségvetési és pénzügyi gazdálkodásról szóló jelentést.
- (7) A számvitelért felelős tisztviselő N+1. év július 1-jéig megküldi a végleges beszámolót és az igazgatótanács véleményét az Európai Parlamentnek, a Tanácsnak, a Bizottság számvitelért felelős tisztviselőjének és a Számvevőszéknek.
- (8) A végleges beszámoló továbbításával egyidejűleg a számvitelért felelős tisztviselő az e végleges beszámolóra vonatkozó teljességi nyilatkozatot is benyújtja a Számvevőszéknek, egy másolati példányt pedig a Bizottság számvitelért felelős tisztviselőjének.
- (9) Az ügyvezető igazgató a következő év november 15-ig közzéteszi a végleges beszámolót.
- (10) Az ügyvezető igazgató N+1. év szeptember 30-ig válaszol a Számvevőszéknek az észrevételekre, és e válaszról másolatot küld az igazgatótanácsnak és a Bizottságnak.
- (11) Az ügyvezető igazgató az Európai Parlament kérésére a költségvetési rendelet 165. cikke (3) bekezdésének megfelelően benyújtja az Európai Parlamenthez a szóban forgó pénzügyi évre vonatkozó mentesítési eljárás szabályszerű lefolytatásához szükséges valamennyi információt.
- (12) Az Európai Parlament a Tanács ajánlása alapján N+2. év május 15. előtt mentesíti az ügyvezető igazgatót az N. év költségvetésének végrehajtására vonatkozó felelőssége alól.

#### *29. cikk*

#### ***Pénzügyi szabályzat***

A Bizottsággal folytatott konzultációt követően az igazgatótanács elfogadja az Ügynökségre vonatkozó pénzügyi szabályzatot. Ezek a szabályok nem térhetnek el az 1271/2013/EU rendeletről, kivéve, ha az eltérés az Ügynökség működéséhez kifejezetten szükséges, és ahhoz a Bizottság előzetesen hozzájárult.

#### *30. cikk*

#### ***Csalás elleni küzdelem***

- (1) A csalás, korrupció és más jogellenes tevékenységek elleni, a 883/2013/EU, Euratom európai parlamenti és tanácsi rendelet<sup>39</sup> értelmében folyó küzdelem elősegítése érdekében az Ügynökség, legkésőbb hat hónappal működésének megkezdése után csatlakozik az Európai Csalás Elleni Hivatal (OLAF) belső vizsgálatairól szóló, 1999. május 25-i intézményközi megállapodáshoz, és a megállapodás mellékletében szereplő minta alapján elfogadja az Ügynökség személyzetének valamennyi tagjára alkalmazandó megfelelő rendelkezéseket.

<sup>39</sup>

[Az Európai Parlament és a Tanács 883/2013/EU, Euratom rendelete \(2013. szeptember 11.\) az Európai Csalás Elleni Hivatal \(OLAF\) által lefolytatott vizsgálatokról, valamint az 1073/1999/EK európai parlamenti és tanácsi rendelet és az 1074/1999/Euratom tanácsi rendelet hatályon kívül helyezéséről \(HL L 248., 2013.9.18., 1. o.\).](#)

- (2) A Számvevőszék jogosult dokumentumalapú és helyszíni ellenőrzést végezni a támogatások összes kedvezményezettjénél, valamint az Ügynökségtől uniós forrásokban részesülő vállalkozóknál és alvállalkozóknál.
- (3) Az OLAF a 883/2013/EU, Euratom európai parlamenti és tanácsi rendeletben és az Európai Közösségek pénzügyi érdekeinek csalással és egyéb szabálytalanságokkal szembeni védelmében a Bizottság által végzett helyszíni ellenőrzésekről és vizsgálatokról szóló, 1996. november 11-i 2185/96/Euratom, EK tanácsi rendeletben<sup>40</sup> előírt rendelkezéseknek és eljárásoknak megfelelően vizsgálatokat, ezen belül helyszíni ellenőrzéseket és vizsgálatokat is végezhet annak megállapítására, hogy az Ügynökség által finanszírozott támogatással vagy szerződéssel összefüggésben történt-e az Unió pénzügyi érdekeit sértő csalás, korrupció vagy más jogellenes cselekmény.
- (4) Az (1), a (2) és a (3) bekezdés sérelme nélkül az Ügynökség által harmadik országokkal és nemzetközi szervezetekkel kötött együttműködési megállapodásoknak, továbbá az általa kötött szerződéseknek, támogatási megállapodásoknak és támogatási határozatoknak olyan rendelkezéseket kell tartalmazniuk, amelyek kifejezetten felhatalmazzák a Számvevőszéket és az OLAF-ot arra, hogy saját hatáskörüknek megfelelően lefolytassák az ilyen ellenőrzéseket és vizsgálatokat.

## **IV. FEJEZET**

### **AZ ÜGYNÖKSÉG SZEMÉLYZETE**

#### *31. cikk*

#### ***Általános rendelkezések***

Az Ügynökség személyzetére a személyzeti szabályzat, az egyéb alkalmazottakra vonatkozó alkalmazási feltételek, valamint az uniós intézmények közötti megállapodás útján elfogadott, a személyzeti szabályzat alkalmazására vonatkozó szabályok irányadók.

#### *32. cikk*

#### ***Kiváltságok és mentességek***

Az Ügynökségre és személyzetére az Európai Unióról szóló szerződéshez és az EUMSZ-hez csatolt, az Európai Unió kiváltságairól és mentességeiről szóló 7. jegyzőkönyv vonatkozik.

#### *33. cikk*

#### ***Ügyvezető igazgató***

- (1) Az Ügynökség az ügyvezető igazgatót az egyéb alkalmazottakra vonatkozó alkalmazási feltételek 2. cikkének a) pontja értelmében ideiglenes alkalmazottként foglalkoztatja.
- (2) Az ügyvezető igazgatót nyílt és átlátható kiválasztási eljárást követően az igazgatótanács nevezi ki a Bizottság által javasolt jelöltek listájáról.

<sup>40</sup>

[A Tanács 2185/96/Euratom, EK rendelete \(1996. november 11.\) az Európai Közösségek pénzügyi érdekeinek csalással és egyéb szabálytalanságokkal szembeni védelmében a Bizottság által végzett helyszíni ellenőrzésekről és vizsgálatokról](#) (HL L 292., 1996.11.15., 2. o.).

- (3) Az ügyvezető igazgató szerződésének megkötése céljából az Ügynökséget az igazgatótanács elnöke képviseli.
- (4) Kinevezése előtt az igazgatótanács által kiválasztott jelölt felkérést kap, hogy tegyen nyilatkozatot az Európai Parlament illetékes bizottsága előtt, és válaszoljon a képviselők kérdéseire.
- (5) Az ügyvezető igazgató hivatali ideje öt év. Ezen időszak lejártá előtt a Bizottság értékelést készít, amely figyelembe veszi az ügyvezető igazgató teljesítményét, valamint az Ügynökség jövőbeni feladatait és az előtte álló kihívásokat.
- (6) Az igazgatótanács az ügyvezető igazgató kinevezéséről, hivatali idejének meghosszabbításáról és felmentéséről a szavazásra jogosult tagok kétharmadának szavazatával dönt.
- (7) Az igazgatótanács az (5) bekezdésben említett értékelést figyelembe vevő bizottsági javaslat alapján eljárva az ügyvezető igazgató hivatali idejét egy alkalommal, legfeljebb öt évre meghosszabbíthatja.
- (8) Amennyiben az igazgatótanács meg kívánja hosszabbítani az ügyvezető igazgató hivatali idejét, erről tájékoztatja az Európai Parlamentet. Legfeljebb három hónappal hivatali idejének meghosszabbítása előtt az ügyvezető igazgató – amennyiben felkéri – az Európai Parlament illetékes bizottsága előtt nyilatkozatot tesz, és válaszol a képviselők kérdéseire.
- (9) Az az ügyvezető igazgató, akinek a hivatali ideje meghosszabbításra került, nem vehet részt az ugyanazon álláshelyre vonatkozó újabb kiválasztási eljárásokban.
- (10) Az ügyvezető igazgató kizárólag az igazgatótanács határozatával hívható vissza hivatalából, amely határozatot az igazgatótanács a Bizottság javaslata alapján hozott meg.

#### *34. cikk*

#### ***Kirendelt nemzeti szakértők és egyéb személyzet***

- (1) Az Ügynökség igénybe vehet kirendelt nemzeti szakértőket és egyéb, nem az Ügynökség alkalmazásában álló személyzetet. Rájuk a személyzeti szabályzat és az egyéb alkalmazottakra vonatkozó alkalmazási feltételek nem vonatkoznak.
- (2) Az igazgatótanács határozatot fogad el a nemzeti szakértők Ügynökséghez való kirendelésére vonatkozó szabályokról.

## **V. FEJEZET ÁLTALÁNOS RENDELKEZÉSEK**

#### *35. cikk*

#### ***Az Ügynökség jogállása***

- (1) Az Ügynökség az Unió szerve, és jogi személyiséggel rendelkezik.
- (2) Az Ügynökséget valamennyi tagállamban a nemzeti jog által a jogi személyeknek nyújtott legteljesebb jogképesség illeti meg. Az Ügynökség ingó- és ingatlanvagyonot szerezhet, illetve idegeníthet el, és/vagy per képességgel rendelkezik.
- (3) Az Ügynökséget az ügyvezető igazgató képviseli.

36. cikk

***Az Ügynökség felelőssége***

- (1) Az Ügynökség szerződéses felelősségére az adott szerződésre alkalmazandó jog irányadó.
- (2) Az Ügynökség által megkötött szerződések választottbíróági záradékai alapján a felmerülő jogvitákban az Európai Unió Bírósága rendelkezik hatáskörrel.
- (3) Szerződésen kívüli felelősség esetén az Ügynökség a tagállamok jogában közös általános jogelvekkel összhangban megtéríti az általa vagy alkalmazottai által feladataik ellátása során okozott károkat.
- (4) Az ilyen károk megtérítésére vonatkozó jogviták tekintetében az Európai Unió Bírósága rendelkezik hatáskörrel.
- (5) Az Ügynökség alkalmazottainak az Ügynökséggel szemben fennálló személyes felelősségét illetően az Ügynökség személyzetére e tekintetben irányadó feltételeket kell alkalmazni.

37. cikk

***Nyelvhasználat***

- (1) Az 1. tanácsi rendeletben<sup>41</sup> megállapított rendelkezések az Ügynökségre is vonatkoznak. A tagállamok és az általuk kijelölt egyéb szervek az Unió intézményeinek bármely hivatalos nyelvén fordulhatnak az Ügynökséghez, és jogosultak ugyanezen a nyelven választ kapni.
- (2) Az Ügynökség működéséhez szükséges fordítási szolgáltatásokat Az Európai Unió Szerveinek Fordítóközpontja biztosítja.

38. cikk

***A személyes adatok védelme***

- (1) A személyes adatok Ügynökség általi feldolgozására a 45/2001/EK európai parlamenti és tanácsi rendelet<sup>42</sup> vonatkozik.
- (2) A 45/2001/EK rendelet 24. cikkének (8) bekezdésében említett végrehajtási intézkedéseket az igazgatótanács fogadja el. Az igazgatótanács további intézkedéseket fogadhat el, amennyiben azok szükségesek a 45/2001/EK rendelet Ügynökség általi alkalmazásához.

39. cikk

***Együttműködés harmadik országokkal és nemzetközi szervezetekkel***

- (1) Amennyiben az e rendeletben meghatározott célkitűzések eléréséhez szükséges, az Ügynökség harmadik országok illetékes hatóságaival és/vagy nemzetközi

<sup>41</sup> [1. rendelet az Európai Atomenergia-közösség által használt nyelvek meghatározásáról](#) (HL 17., 1958.10.6., 401. o.).

<sup>42</sup> Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról (HL L 8., 2001.1.12., 1. o.).

szervezetekkel is együttműködhet. Ebből a célból az Ügynökség a Bizottság előzetes jóváhagyásával a harmadik országok hatóságaival és a nemzetközi szervezetekkel munkamegállapodásokat köthet. Ezek a megállapodások nem keletkeztethetnek jogi kötelezettséget az Unióval és tagállamaival szemben.

- (2) Az Ügynökség nyitott azon harmadik országok részvételére, amelyek ebből a célból megállapodást kötöttek az Unióval. Ezen megállapodások vonatkozó rendelkezései alapján részletes szabályokat kell hozni, meghatározván különösen annak természetét, mértékét és módját, ahogyan ezen országok részt vesznek az Ügynökség munkájában, beleértve azon rendelkezéseket is, amelyek az Ügynökség kezdeményezéseiben való részvételre, a pénzügyi hozzájárulásokra és a személyi állományra vonatkoznak. A személyzeti kérdéseket illetően ezeknek a szabályoknak minden esetben meg kell felelniük a személyzeti szabályzatnak.
- (3) Az igazgatótanács az Ügynökség hatáskörébe tartozó kérdések tekintetében stratégiát fogad el a harmadik országokkal és nemzetközi szervezetekkel fenntartott kapcsolatokra vonatkozóan. A Bizottság gondoskodik arról, hogy az Ügynökség a megbízatásával összhangban és a meglévő intézményi kereteken belül működjön, és az Ügynökség ügyvezető igazgatójával munkamegállapodást köt erre a célra.

#### 40. cikk

##### ***Biztonsági szabályok a minősített adatok és a nem minősített bizalmas adatok védelmére***

A Bizottsággal folytatott konzultáció alapján az Ügynökség saját biztonsági szabályokat fogad el az EU-minősített adatok és a nem minősített bizalmas adatok védelmére vonatkozó, az (EU, Euratom) 2015/443 és az (EU, Euratom) 2015/444 bizottsági határozatban megállapított bizottsági biztonsági szabályokban foglalt biztonsági elvek alkalmazása érdekében. E szabályok többek között az ilyen adatok cseréjére, feldolgozására és tárolására vonatkozó rendelkezésekre terjednek ki.

#### 41. cikk

##### ***Székhely-megállapodás és működési feltételek***

- (1) Az Ügynökségnek az adott tagállambeli elhelyezéséhez szükséges rendelkezéseket, a tagállam által rendelkezésre bocsátandó létesítményeket, továbbá az Ügynökség ügyvezető igazgatójára, az igazgatótanács tagjaira, valamint az Ügynökség személyi állományára és a családtagokra az adott tagállamban alkalmazandó konkrét szabályokat az Ügynökség és az annak otthont adó tagállam által – az igazgatótanács jóváhagyásának megszerzése után és legkésőbb [2 évvel e rendelet hatálybalépését követően] – megkötött székhely-megállapodás rögzíti.
- (2) Az Ügynökségnek otthont adó tagállam a lehető legjobb feltételeket biztosítja az Ügynökség megfelelő működéséhez, ideértve a székhely megközelíthetőségét, az alkalmazottak gyermekeinek biztosított megfelelő oktatási lehetőségeket, valamint a személyzetet kísérő gyermekek és házastársak munkaerőpiachoz, társadalombiztosításhoz és egészségügyi ellátáshoz való hozzáférését is.

#### 42. cikk

##### ***Adminisztratív ellenőrzés***

Az Ügynökség működése felett az EUMSZ 228. cikkének megfelelően az ombudsman gyakorol felügyeleti jogkört.

### III. CÍM

## KIBERBIZTONSÁGI TANÚSÍTÁSI KERETRENDSZER

#### 43. cikk

##### ***Európai kiberbiztonsági tanúsítási rendszerek***

Az európai kiberbiztonsági tanúsítási rendszer annak igazolására szolgál, hogy az ilyen rendszernek megfelelően tanúsított IKT-termékek és -szolgáltatások megfelelnek az azzal kapcsolatban meghatározott követelményeknek, hogy képesek egy adott biztonsági szinten ellenállni az olyan tevékenységekkel szemben, amelyek célja, hogy veszélyeztessék az e termékek, eljárások, szolgáltatások és rendszerek által tárolt vagy továbbított vagy feldolgozott adatok, illetve az említett termékek, eljárások, szolgáltatások és rendszerek által biztosított vagy elérhetővé tett funkciók vagy szolgáltatások hozzáférhetőségét, hitelességét, sértetlenségét és titkosságát.

#### 44. cikk

##### ***Az európai kiberbiztonsági tanúsítási rendszer kidolgozása és elfogadása***

- (1) Az ENISA a Bizottság felkérésére az e rendelet 45., 46. és 47. cikkében meghatározott követelményeknek megfelelő európai kiberbiztonsági tanúsítási rendszerre irányuló javaslatot dolgoz ki. A Bizottságnak a tagállamok vagy az 53. cikk alapján létrehozott európai kiberbiztonsági tanúsítási csoport (a továbbiakban: csoport) tehetnek javaslatot európai kiberbiztonsági tanúsítási rendszerre irányuló javaslat kidolgozására.
- (2) Az e cikk (1) bekezdésében említett rendszerekre irányuló javaslatok kidolgozása során az ENISA valamennyi érdekelt féllel konzultál, és szorosan együttműködik a csoporttal. A csoport biztosítja az ENISA számára a rendszerre irányuló javaslat kidolgozásához szükséges segítséget és szakértői tanácsadást, többek között azáltal, hogy szükség esetén véleményeket ad ki.
- (3) Az ENISA az e cikk (2) bekezdésével összhangban kidolgozott európai kiberbiztonsági tanúsítási rendszerre irányuló javaslatot benyújtja a Bizottságnak.
- (4) A Bizottság az ENISA által javasolt rendszer alapján az 55. cikk (1) bekezdésének megfelelően végrehajtási jogi aktusokat fogadhat el, amelyekben az IKT-termékekre és -szolgáltatásokra vonatkozó, az e rendelet 45., 46. és 47. cikkében foglalt követelményeknek megfelelő európai kiberbiztonsági tanúsítási rendszerekről rendelkezik.
- (5) Az ENISA külön honlapot tart fenn, amelyen tájékoztatást nyújt az európai kiberbiztonsági tanúsítási rendszerekről, és népszerűsíti azokat.

#### 45. cikk

##### ***Az európai kiberbiztonsági tanúsítási rendszerek biztonsági célkitűzései***

Az európai kiberbiztonsági tanúsítási rendszereket úgy kell kialakítani, hogy értelemszerűen figyelembe vegyék az alábbi biztonsági célkitűzéseket:



- a) a tárolt, továbbított vagy egyéb módon feldolgozott adatok védelme a véletlen vagy illetéktelen tárolással, feldolgozással, hozzáféréssel és nyilvánosságra hozatallal szemben;
- b) a tárolt, továbbított vagy egyéb módon feldolgozott adatok védelme a véletlen vagy illetéktelen megsemmisítéssel, véletlen elvesztéssel és módosítással szemben;
- c) annak biztosítása, hogy az arra engedéllyel rendelkező személyek, programok vagy gépek kizárólag a hozzáférési jogaik tárgyát képező adatokhoz, szolgáltatásokhoz vagy funkciókhoz férhessenek hozzá;
- d) annak rögzítése, hogy ki mikor mely adatokat, funkciókat és szolgáltatásokat továbbította;
- e) annak lehetővé tétele, hogy ellenőrizni lehessen, ki mikor mely adatokhoz, szolgáltatásokhoz vagy funkciókhoz fért hozzá, illetve mely adatokat, szolgáltatásokat vagy funkciókat használta fel;
- f) fizikai vagy műszaki biztonsági esemény bekövetkeztekor az adatok, szolgáltatások és funkciók elérhetőségének, illetve az adatokhoz, a szolgáltatásokhoz és a funkciókhoz való hozzáférésnek mihamarabbi helyreállítása;
- g) annak biztosítása, hogy az IKT-termékek és -szolgáltatások szoftvere naprakész legyen, ne legyenek ismert sebezhetőségei, és szoftvereik frissítésére biztonságos mechanizmusok álljanak rendelkezésre.

#### *46. cikk*

##### ***Az európai kiberbiztonsági tanúsítási rendszerek biztonsági szintjei***

- (1) Az európai kiberbiztonsági tanúsítási rendszer az „alapvető”, „jelentős” és/vagy „magas” biztonsági szintek közül egy vagy több szintet határozhat meg az e rendszer keretében kibocsátott IKT-termékek és -szolgáltatások vonatkozásában.
- (2) Az alapvető, jelentős, illetve magas szintű biztonsági szinteknek értelemszerűen a következő kritériumoknak kell megfelelniük:
  - a) az „alapvető” biztonsági szint egy európai kiberbiztonsági tanúsítási rendszer keretében kibocsátott olyan tanúsítványra utal, amely – a megfelelő műszaki leírásokra, szabványokra és eljárásokra, többek között műszaki ellenőrzésekre hivatkozva, melyek célja a kiberbiztonsági események kockázatának csökkentése – az adott IKT-termék vagy -szolgáltatás állítólagos vagy igazolt kiberbiztonsági jellemzőinek korlátozott megbízhatóságot tulajdonít;
  - b) a „jelentős” biztonsági szint egy európai kiberbiztonsági tanúsítási rendszer keretében kibocsátott olyan tanúsítványra utal, amely – a megfelelő műszaki leírásokra, szabványokra és eljárásokra, többek között műszaki ellenőrzésekre hivatkozva, melyek célja a kiberbiztonsági események kockázatának jelentős csökkentése – az adott IKT-termék vagy -szolgáltatás állítólagos vagy igazolt kiberbiztonsági jellemzőinek jelentős mértékű megbízhatóságot tulajdonít;
  - c) a „magas” biztonsági szint egy európai kiberbiztonsági tanúsítási rendszer keretében kibocsátott olyan tanúsítványra utal, amely – a megfelelő műszaki leírásokra, szabványokra és eljárásokra, többek között műszaki ellenőrzésekre hivatkozva, melyek célja a kiberbiztonsági események megelőzése – az adott

IKT-termék vagy -szolgáltatás állítólagos vagy igazolt kiberbiztonsági jellemzőinek nagyobb mértékű megbízhatóságot tulajdonít, mint a „jelentős” biztonsági szintet igazoló tanúsítványok.

#### 47. cikk

##### ***Az európai kiberbiztonsági tanúsítási rendszerek elemei***

- (1) Az európai kiberbiztonsági tanúsítási rendszerek a következő elemeket tartalmazzák:
  - a) a tanúsítás tárgya és hatálya, ideértve az érintett IKT-termékek és -szolgáltatások típusát vagy kategóriáit;
  - b) azon kiberbiztonsági követelmények részletes leírása, amelyek alapján az adott IKT-termékeket és -szolgáltatásokat értékelik, például az uniós vagy nemzetközi szabványokra vagy műszaki előírásokra való hivatkozással;
  - c) adott esetben egy vagy több biztonsági szint;
  - d) konkrét értékelési kritériumok és módszerek, ideértve az értékelés típusait is, amelyeket a 45. cikkben említett konkrét célkitűzések elérésének bizonyítása érdekében alkalmaznak;
  - e) a kérelmező által a megfelelőségértékelő szervezetek részére benyújtandó, a tanúsításhoz szükséges információk;
  - f) amennyiben a rendszer jelölésekről vagy címkékről rendelkezik, e jelölések vagy címkék használati feltételei;
  - g) amennyiben a felügyelet is a rendszer része, a tanúsítványokban foglalt követelményeknek való megfelelés nyomon követésére vonatkozó szabályok, beleértve a meghatározott kiberbiztonsági követelményeknek való folyamatos megfelelés bizonyítására szolgáló mechanizmusokat;
  - h) a tanúsítás megadására és fenntartására, valamint hatályának kiterjesztésére és csökkentésére vonatkozó feltételek;
  - i) az arra vonatkozó szabályok, ha a tanúsított IKT-termékek és -szolgáltatások nem felelnek meg a tanúsítási követelményeknek;
  - j) az IKT-termékek és -szolgáltatások terén korábban nem észlelt kiberbiztonsági sebezhetőségek jelentésére és kezelésére vonatkozó szabályok;
  - k) a megfelelőségértékelő szervezetek nyilvántartásainak megőrzésére vonatkozó szabályok;
  - l) az azonos típusú vagy kategóriájú IKT-termékekre és -szolgáltatásokra kiterjedő nemzeti kiberbiztonsági tanúsítási rendszerek azonosítása;
  - m) a kiadott tanúsítvány tartalma.
- (2) A rendszerben előírt követelmények nem mondhatnak ellent a vonatkozó jogi előírásoknak, különösen a harmonizált uniós jogszabályokból eredő követelményeknek.
- (3) Amennyiben egy adott uniós jogi aktus úgy rendelkezik, az európai kiberbiztonsági tanúsítási rendszer keretében történő tanúsítással vélelmezhetővé válik az adott jogi aktus követelményeinek való megfelelés is.

- (4) Azokon a területeken, amelyeken nincsenek harmonizált uniós jogszabályok, a tagállamok rendelkezhetnek úgy jogszabályaikban, hogy az európai kiberbiztonsági tanúsítási rendszer bizonyos jogi követelményeknek való megfelelés vélelmezésére is használható.

#### *48. cikk*

##### ***Kiberbiztonsági tanúsítás***

- (1) A 44. cikk alapján elfogadott európai kiberbiztonsági tanúsítási rendszer keretében tanúsított IKT-termékekről és -szolgáltatásokról vélelmezni kell, hogy megfelelnek az e rendszer által támasztott követelményeknek.
- (2) Amennyiben az uniós jog másként nem rendelkezik, a tanúsítás önkéntes.
- (3) Az e cikk szerinti európai kiberbiztonsági tanúsítványt az 51. cikkben említett megfelelőségértékelő szervezetek adják ki a 44. cikk alapján elfogadott európai kiberbiztonsági tanúsítási rendszerben foglalt kritériumok alapján.
- (4) A (3) bekezdéstől eltérve, kellően indokolt esetekben egy adott európai kiberbiztonsági tanúsítási rendszer előírhatja, hogy e rendszer keretében csak közjogi szerv adhat ki európai kiberbiztonsági tanúsítványt. Ez a közjogi szerv a következők egyike:
- a) az 50. cikk (1) bekezdésében említett nemzeti tanúsításfelügyeleti hatóság;
  - b) az 51. cikk (1) bekezdése szerinti megfelelőségértékelő szervezetként akkreditált testület, vagy
  - c) valamely érintett tagállam törvényei, jogszabályai vagy más hivatalos közigazgatási eljárásai alapján létrehozott testület, amely megfelel az ISO/IEC 17065: 2012 szabvány termékek, eljárások és szolgáltatások tanúsítását végző szervezetekre vonatkozó követelményeinek.
- (5) Az IKT-termékeiket vagy -szolgáltatásaikat tanúsításra benyújtó természetes vagy jogi személyek az 51. cikkben említett megfelelőségértékelő szervezet rendelkezésére bocsátják a tanúsítási eljárás lefolytatásához szükséges valamennyi információt.
- (6) A tanúsítványok legfeljebb hároméves időtartamra szólnak, és azonos feltételek mellett megújíthatók, feltéve, hogy a megfelelő követelmények továbbra is teljesülnek.
- (7) Az e cikk alapján kiadott európai kiberbiztonsági tanúsítványokat valamennyi tagállamban el kell ismerni.

#### *49. cikk*

##### ***Nemzeti kiberbiztonsági tanúsítási rendszerek és tanúsítványok***

- (1) A (3) bekezdés sérelme nélkül a nemzeti kiberbiztonsági tanúsítási rendszerek és az európai kiberbiztonsági tanúsítási rendszer hatálya alá tartozó IKT-termékekre és -szolgáltatásokra vonatkozó idevágó eljárások a 44. cikk (4) bekezdése alapján elfogadott végrehajtási jogi aktusban meghatározott időponttól kezdve nem keletkeztetnek joghatást. A hatályos nemzeti kiberbiztonsági tanúsítási rendszerek, valamint az európai kiberbiztonsági tanúsítási rendszer hatálya alá nem tartozó IKT-

termékekre és -szolgáltatásokra vonatkozó idevágó eljárások azonban továbbra is fennmaradnak.

- (2) A tagállamok a valamely hatályos európai kiberbiztonsági tanúsítási rendszer hatálya alá tartozó IKT-termékekre és -szolgáltatásokra vonatkozóan nem vezethetnek be új nemzeti kiberbiztonsági tanúsítási rendszereket.
- (3) A nemzeti kiberbiztonsági tanúsítási rendszerek alapján kiadott meglévő tanúsítványok lejáratuk napjáig érvényben maradnak.

#### 50. cikk

#### **Nemzeti tanúsításfelügyeleti hatóságok**

- (1) Minden tagállam kijelöl egy nemzeti tanúsításfelügyeleti hatóságot.
- (2) Minden tagállam közli a Bizottsággal, hogy mely hatóságot jelölte ki.
- (3) Minden nemzeti tanúsításfelügyeleti hatóságnak – szervezetét, a finanszírozási határozatokat, jogi felépítését és a döntéshozatalt illetően – függetlennek kell lennie az általa felügyelt szervezetektől.
- (4) A tagállamok biztosítják, hogy a nemzeti tanúsításfelügyeleti hatóságok rendelkezzenek a hatáskörük gyakorlásához, valamint a rájuk bízott feladatok hatékony és eredményes elvégzéséhez szükséges forrásokkal.
- (5) A rendelet hatékony végrehajtása érdekében helyénvaló, hogy ezek a hatóságok – aktív, hatékony, eredményes és biztonságos módon – részt vegyenek az 53. cikk alapján létrehozott európai kiberbiztonsági tanúsítási csoportban.
- (6) A nemzeti tanúsításfelügyeleti hatóságok:
  - a) figyelemmel kísérik és biztosítják az e címben meghatározott rendelkezések nemzeti szintű alkalmazását, valamint felügyelik, hogy az adott tagállam területén létrehozott megfelelőségértékelő szervezetek által kiállított tanúsítványok megfelelnek-e az e címben és a megfelelő európai kiberbiztonsági tanúsítási rendszerben meghatározott követelményeknek;
  - b) figyelemmel kísérik és felügyelik a megfelelőségértékelő szervezetek tevékenységeit e rendelet alkalmazásában, többek között a megfelelőségértékelő szervezetek bejelentésével és az e rendelet 52. cikkében meghatározott idevágó feladatokkal kapcsolatban;
  - c) kezelik a természetes vagy jogi személyek által az adott tagállam területén létrehozott megfelelőségértékelő szervezetek által kiadott tanúsítványokkal kapcsolatban benyújtott panaszokat, megfelelő mértékben kivizsgálják a panasz tárgyát, és észszerű időn belül tájékoztatják a panaszost a vizsgálat előrehaladásáról és eredményéről;
  - d) együttműködnek a többi nemzeti tanúsításfelügyeleti hatósággal és más hatóságokkal, többek között azáltal, hogy megosztják az azzal kapcsolatos információkat, ha bizonyos IKT-termékek és -szolgáltatások nem felelnek meg e rendelet vagy egyes európai kiberbiztonsági tanúsítási rendszerek követelményeinek;
  - e) figyelemmel kísérik a kiberbiztonsági tanúsítás terén zajló releváns fejleményeket.

- (7) Minden nemzeti tanúsításfelügyeleti hatóság legalább a következő hatáskörökkel rendelkezik:
- a) felszólíthatja a megfelelőségértékelő szervezeteket és az európai kiberbiztonsági tanúsítványok jogosultjait, hogy bocsássák rendelkezésére a feladata ellátásához szükséges információkat;
  - b) a III. cím rendelkezéseinek való megfelelés ellenőrzése céljából vizsgálatokat végezhet a megfelelőségértékelő szervezeteknél és az európai kiberbiztonsági tanúsítványok jogosultjainál tett ellenőrzések formájában;
  - c) a nemzeti joggal összhangban meghozhatja a megfelelő intézkedéseket annak biztosítása érdekében, hogy a megfelelőségértékelő szervezetek, illetve a tanúsítványok jogosultjai megfeleljenek e rendeletnek, illetve az adott európai kiberbiztonsági tanúsítási rendszernek;
  - d) a megfelelőségértékelő szervezetek és az európai kiberbiztonsági tanúsítványok jogosultjainak bármely helyiségébe beléphet az uniós vagy tagállami eljárásjoggal összhangban folytatott vizsgálatok elvégzése céljából;
  - e) a nemzeti joggal összhangban visszavonhatja az e rendeletnek vagy az adott európai kiberbiztonsági tanúsítási rendszernek meg nem felelő tanúsítványokat;
  - f) az 54. cikknek megfelelően szankciókat rendelhet el a nemzeti joggal összhangban, valamint előírhatja az e rendeletben meghatározott kötelezettségek megszegésének azonnali megszüntetését.
- (8) A nemzeti tanúsításfelügyeleti hatóságok együttműködnek egymással és a Bizottsággal, azaz megosztják egymással az IKT-termékek és -szolgáltatások kiberbiztonságának tanúsításával és az idevágó technikai kérdésekkel kapcsolatos információkat, tapasztalataikat és az e téren bevált módszereket.

#### *51. cikk*

##### ***Megfelelőségértékelő szervezetek***

- (1) A 765/2008/EK rendelet alapján kijelölt nemzeti akkreditáló testület csak abban az esetben akkreditálja a megfelelőségértékelő szervezeteket, ha azok megfelelnek az e rendelet mellékletében meghatározott követelményeknek.
- (2) Az akkreditáció legfeljebb öt évre szól, és azonos feltételek mellett megújítható, feltéve, hogy az adott megfelelőségértékelő szervezet teljesíti az e cikkben meghatározott követelményeket. Az akkreditáló testületek visszavonják a megfelelőségértékelő szervezet e cikk (1) bekezdése szerinti akkreditációját, amennyiben az akkreditáció feltételei nem, vagy már nem teljesülnek, vagy ha a megfelelőségértékelő szervezet által hozott intézkedések megsértik ezt a rendeletet.

#### *52. cikk*

##### ***Bejelentés***

- (1) A nemzeti tanúsításfelügyeleti hatóságok a 44. cikk alapján elfogadott minden egyes európai kiberbiztonsági tanúsítási rendszer vonatkozásában bejelentik a Bizottságnak, hogy mely megfelelőségértékelő szervezeteket akkreditálták a 46. cikkben említett, meghatározott biztonsági szintű tanúsítványok kiadására,

valamint indokolatlan késedelem nélkül azt is, ha e szervezetekkel kapcsolatban bármilyen változás következik be.

- (2) Egy évvel az adott európai kiberbiztonsági tanúsítási rendszer hatálybalépését követően a Bizottság közzéteszi a bejelentett megfelelőségértékelő szervezetek jegyzékét a *Hivatalos Lapban*.
- (3) Amennyiben a (2) bekezdésben említett határidő lejártá után érkezik bejelentés, a Bizottság a (2) bekezdésben említett jegyzék módosításait a bejelentés kézhezvételétől számított két hónapon belül közzéteszi az *Európai Unió Hivatalos Lapjában*.
- (4) A nemzeti tanúsításfelügyeleti hatóságok kérelmet nyújthatnak be a Bizottsághoz az érintett nemzeti tanúsításfelügyeleti hatóság által bejelentett megfelelőségértékelő szervezetnek az e cikk (2) bekezdésében említett jegyzékből való törlésére. A Bizottság a nemzeti tanúsításfelügyeleti hatóság kérelmének kézhezvételétől számított egy hónapon belül közzéteszi a jegyzék megfelelő módosításait az *Európai Unió Hivatalos Lapjában*.
- (5) A Bizottság végrehajtási jogi aktusok útján meghatározhatja az e cikk (1) bekezdésében említett bejelentésekre vonatkozó feltételeket, formátumokat és eljárásokat. E végrehajtási jogi aktusokat az 55. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

### 53. cikk

#### ***Európai kiberbiztonsági tanúsítási csoport***

- (1) Létre kell hozni az európai kiberbiztonsági tanúsítási csoportot (a továbbiakban: csoport).
- (2) A csoport nemzeti tanúsításfelügyeleti hatóságokból áll. A hatóságokat a nemzeti tanúsításfelügyeleti hatóságok vezetői vagy más magas rangú képviselői képviselik.
- (3) A csoport a következő feladatokat látja el:
  - a) tanácsot ad és segítséget nyújt a Bizottságnak az e cím rendelkezéseinek következetes végrehajtására és alkalmazására irányuló munkájával kapcsolatban, különös tekintettel a kiberbiztonsági tanúsítási politikával kapcsolatos kérdésekre, a szakpolitikai megközelítések összehangolására, valamint az európai kiberbiztonsági tanúsítási rendszerek kidolgozására;
  - b) segítséget nyújt és tanácsot ad az ENISA-nak, valamint együttműködik vele a rendszerre irányuló javaslat e rendelet 44. cikkének megfelelően történő kidolgozásával kapcsolatban;
  - c) javaslatot tesz a Bizottságnak, hogy kérje fel az Ügynökséget, hogy e rendelet 44. cikkének megfelelően dolgozzon ki európai kiberbiztonsági tanúsítási rendszerre irányuló javaslatot;
  - d) a Bizottságnak címzett véleményeket fogad el a meglévő európai kiberbiztonsági tanúsítási rendszerek fenntartásával és felülvizsgálatával kapcsolatban;
  - e) tanulmányozza a kiberbiztonsági tanúsítás terén zajló releváns fejleményeket, és megosztja a kiberbiztonsági tanúsítási rendszerekkel kapcsolatban bevált módszereket;

- f) az információk megosztásával előmozdítja a nemzeti tanúsításfelügyeleti hatóságok közötti, e cím rendelkezései szerinti együttműködést, különösen a kiberbiztonsági tanúsítással kapcsolatos valamennyi kérdésre vonatkozó hatékony információcserére szolgáló módszerek kialakítása révén.
- (4) A csoportban a Bizottság látja el az elnökséget, és a 8. cikk a) pontjának megfelelően az ENISA segítségével biztosítja a titkárságot.

#### *54. cikk*

#### **Szankciók**

A tagállamok megállapítják az e címbe foglalt rendelkezések és az európai kiberbiztonsági tanúsítási rendszerek megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és minden szükséges intézkedést meghoznak e szabályok alkalmazása érdekében. Az előírt szankcióknak hatékonyak, arányosak és visszatartó erejűnek kell lenniük. A tagállamok [...-ig/haladéktalanul] értesítik a Bizottságot e szabályokról és intézkedésekről, és bejelentik az ezeket érintő esetleges későbbi módosításokat.

## IV. CÍM

# ZÁRÓ RENDELKEZÉSEK

### 55. cikk

#### **Bizottsági eljárásrend**

- (1) A Bizottság munkáját egy bizottság segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottság.
- (2) Az e bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 4. cikkét kell alkalmazni.

### 56. cikk

#### **Értékelés és felülvizsgálat**

- (1) A Bizottság legkésőbb öt évvel az 58. cikkben említett időpontot követően, majd azt követően ötévenként értékeli az Ügynökség és munkamódszereinek hatását, eredményességét és hatékonyságát, valamint azt is, hogy szükséges-e módosítani az Ügynökség megbízatását, és ha igen, e módosítás milyen pénzügyi vonzatokkal járna. Az értékelésben figyelembe kell venni minden olyan visszajelzést is, amelyet az Ügynökség a tevékenységével kapcsolatban kapott. Amennyiben a Bizottság megítélése szerint az Ügynökség fenntartása a kitűzött célokra, megbízatásra és feladatokra tekintettel a továbbiakban nem indokolt, javasolhatja, hogy módosítsák e rendeletet az Ügynökségre vonatkozó rendelkezések tekintetében.
- (2) Az értékelésben ki kell térni arra is, hogy a III. címben foglalt rendelkezéseknek milyen a hatása, eredményessége és hatékonysága az IKT-termékek és -szolgáltatások Unión belüli megfelelő szintű kiberbiztonságának biztosítására és a belső piac működésének javítására vonatkozó célkitűzések tekintetében.
- (3) A Bizottság az értékelő jelentést és az azzal kapcsolatos következtetéseit megküldi az Európai Parlamentnek és a Tanácsnak, valamint az igazgatótanácsnak. Az értékelő jelentés megállapításait közzé kell tenni.

### 57. cikk

#### **Hatályon kívül helyezés és jogutódlás**

- (1) Az 526/2013/EK rendelet [...] -val/vel hatályát veszti.
- (2) Az 526/2013/EK rendeletre és az ENISA-ra való hivatkozásokat erre a rendeletre, illetve az Ügynökségre való hivatkozásként kell értelmezni.
- (3) Az Ügynökség mindennemű tulajdonviszony, megállapodás, jogi kötelezettség, munkaszerződés, pénzügyi kötelezettségvállalás és felelősség vonatkozásában az 526/2013/EK rendelettel létrehozott ügynökség jogutódja. Az igazgatótanács és a felügyelőtestület által hozott valamennyi határozat érvényben marad, feltéve, hogy azok nem ütköznek e rendelet rendelkezéseivel.
- (4) Az Ügynökség [...] -tól/től kezdődően határozatlan időtartamra jön létre.



- (5) Az 526/2013/EK rendelet 24. cikkének (4) bekezdése alapján kinevezett ügyvezető igazgató hivatali idejének fennmaradó részére az Ügynökség ügyvezető igazgatója marad.
- (6) Az igazgatótanács 526/2013/EK rendelet 6. cikke alapján kinevezett tagjai és póttagjai hivatali idejük fennmaradó részére az Ügynökség igazgatótanácsának tagjai és póttagjai maradnak.

*58. cikk*

- (1) Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.
- (2) Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, -án/-én.

*az Európai Parlament részéről*  
*az elnök*

*a Tanács részéről*  
*az elnök*

## PÉNZÜGYI KIMUTATÁS

### 1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

#### 1.1. A javaslat/kezdemenyezés címe

Javaslat – az Európai Parlament és a Tanács rendelete az ENISA-ról, az „Európai Unió kiberbiztonsági ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről és az információs és kommunikációs technológiák biztonsági tanúsításáról (kiberbiztonsági jogszabály/rendelet)

#### 1.2. Érintett szakpolitikai terület(ek)

Szakpolitikai terület: 09 – Tartalmak, technológiák és kommunikációs hálózatok  
Tevékenység: 09.02 digitális egységes piac

#### 1.3. A javaslat/kezdemenyezés típusa

- ☒ A javaslat/kezdemenyezés új intézkedésre irányul (III. cím – Tanúsítás)
- ☐ A javaslat/kezdemenyezés **kísérleti projektet / előkészítő intézkedést követő új intézkedésre** irányul<sup>43</sup>
- ☒ A javaslat/kezdemenyezés jelenlegi intézkedés meghosszabbítására irányul (II. cím – az ENISA megbízatása)
- ☐ A javaslat/kezdemenyezés új intézkedésnek megfelelően módosított intézkedésre irányul

#### 1.4. Célkitűzés(ek)

##### 1.4.1. A javaslat/kezdemenyezés által érintett többéves bizottsági stratégiai célkitűzés(ek)

1. Az ellenálló képesség növelése a tagállamoknál, a vállalkozásoknál és az Unió egészében
2. Az IKT-termékek és -szolgáltatások uniós belső piaca megfelelő működésének biztosítása
3. Az IKT területén működő uniós vállalatok nemzetközi versenyképességének növelése
4. A tagállamok kiberbiztonságot igénylő törvényi, rendeleti és közigazgatási rendelkezéseinek közelítése

##### 1.4.2. Konkrét célkitűzés(ek)

Az általános célokat szem előtt tartva, a felülvizsgált kiberbiztonsági stratégiával tágabb összefüggésben az eszköz – az ENISA hatályának és megbízatásának meghatározása és az IKT-termékekre és -szolgáltatásokra vonatkozó európai tanúsítási keretrendszer létrehozása révén – a következő egyedi célkitűzéseket igyekszik teljesíteni:

1. A tagállamok és vállalkozások képességeinek és felkészültségének javítása.
2. A tagállamok, uniós intézmények, hivatalok és szervek közötti együttműködés és koordináció javítása.
3. A tagállami fellépések kiegészítését szolgáló uniós szintű képességek növelése, különösen a határon átnyúló kiberválságok esetében.

<sup>43</sup>

A költségvetési rendelet 54. cikke (2) bekezdésének a) vagy b) pontja szerint.

4. A magánfelhasználók és a vállalkozások tudatosságának növelése a kiberbiztonsággal kapcsolatos kérdésekben.
5. A digitális egységes piac és digitális innováció iránti bizalom megerősítése az IKT-termékek és -szolgáltatások **kiberbiztonsági szintje** általános **átláthatóságának**<sup>44</sup> növelésével.

**Az ENISA a következők útján járul hozzá a fenti célkitűzésekhez:**

Megerősített döntéshozatali támogatás – iránymutatás és tanácsadás nyújtása a Bizottság és a tagállamok számára egy holisztikus normatív keretrendszer naprakésszé tétele és kidolgozása érdekében a kiberbiztonság területén, valamint olyan ágazatspecifikus politikai és jogalkotási kezdeményezések terén, amelyek kiberbiztonsági szempontból érintettek; szakértelem és támogatás nyújtása révén hozzájárulás az együttműködési csoport munkájához (az (EU) 2016/1148 irányelv 11. cikke); szakpolitika kidolgozása és végrehajtása az elektronikus azonosítás és a bizalmi szolgáltatások terén; a bevált módszerek megosztásának ösztönzése az illetékes hatóságok szintjén.

**A kapacitásépítés fokozott támogatása** – a tagállamok, az uniós intézmények, szervek és hivatalok támogatása a kiberbiztonsági problémák és események megelőzésének, észlelésének, elemzésének, valamint az azokra való reagálási kapacitásnak a fejlesztése és javítása érdekében; igény szerint a tagállamok támogatása a nemzeti CSIRT-ek és nemzeti kiberbiztonsági stratégiák kidolgozásában; uniós intézmények támogatása az uniós kiberbiztonsági stratégiák kidolgozásában és felülvizsgálatában; kiberbiztonsági képzések biztosítása; a tagállamok támogatása az együttműködési csoport révén a bevált módszerek cseréjében; ágazati információmegosztási és elemző központok (ISAC-ok) létrehozásának elősegítése.

Operatív együttműködés és válságkezelési támogatás – az illetékes állami szervek és érdekelt felek közötti együttműködés támogatása a kiberbiztonsággal, számítástechnikai bűnözéssel, valamint a magánélet és a személyes adatok védelmével foglalkozó uniós intézményekkel, szervekkel és hivatalokkal folytatott rendszeres együttműködés kialakítása révén; a CSIRT-hálózatok titkárságának biztosítása (az (EU) 2016/1148 irányelv 12. cikkének (2) bekezdése), valamint hozzájárulás a hálózaton belüli operatív együttműködéshez a tagállamok – igény szerinti – a CERT-EU-val közösen történő támogatásával; rendszeres kiberbiztonsági gyakorlatok szervezése; hozzájárulás közös reagálás kialakításához a nagy léptékű, határokon átnyúló kiberbiztonsági események és válságok kezelésére; a CSIRT-hálózattal együttműködve a jelentős biztonsági események utólagos technikai vizsgálata és nyomkövetési ajánlások kiadása.

Piaci feladatok (szabványosítás, tanúsítás) – több, a kifejezetten a belső piacot támogató feladatkörök betöltése: kiberbiztonsági piaci megfigyelőközpontként a kiberbiztonsági piac releváns tendenciáinak elemzése a kereslet és kínálat megfelelőbb kielégítése érdekében; az IKT-termékek és -szolgáltatások kiberbiztonsági tanúsításával kapcsolatos uniós politika kidolgozásának és végrehajtásának támogatása és ösztönzése az ilyen termékek és szolgáltatások európai kiberbiztonsági tanúsítási rendszereire irányuló javaslatok kidolgozásával, biztosítva az Unió kiberbiztonsági tanúsítási csoportjának titkárságát, amely iránymutatásokat és bevált gyakorlatokat biztosít az IKT-termékek és -szolgáltatások biztonsági követelményei terén a nemzeti tanúsításfelügyeleti hatóságokkal és az iparral együttműködve. Fokozott támogatás ismeretbővítés, tájékoztatás

<sup>44</sup>

A kiberbiztonsági szint átláthatósága azt jelenti, hogy a felhasználók elegendő információhoz jutnak a kiberbiztonsági tulajdonságokra vonatkozóan, amelynek révén objektív módon képesek meghatározni egy adott IKT-termék, -szolgáltatás vagy -folyamat biztonsági szintjét.

és tudatosságnövelés céljából – segítségnyújtás és tanácsadás a Bizottság és a tagállamok részére annak érdekében, hogy az Európai Unió teljes területén magas szintű tudás legyen mozgósítható a hálózat- és információbiztonsággal összefüggő kérdésekben, valamint ennek alkalmazása az ipari érdekeltekre. Ez magában foglalja továbbá a nyilvánosság tájékoztatását a hálózati és információs rendszerek biztonságával [illetve a kiberbiztonsággal] kapcsolatos tudnivalók összegyűjtésével, rendszerezésével és erre a célra létrehozott portálon való közzétételével. A tevékenység egy másik fontos eleme olyan tudatosságnövelő tevékenységek és átfogó kampányok szervezése a nyilvánosság számára, amelyek a kiberbiztonsági kockázatokkal foglalkoznak.

Fokozottabb kutatási és innovációs támogatás – tanácsadás a kiberbiztonságot érintő kutatási igényekkel és a prioritások meghatározásával kapcsolatban.

Nemzetközi együttműködési támogatás – az Unió azon erőfeszítéseinek támogatása, amelyek célja a harmadik országokkal és nemzetközi szervezetekkel való együttműködés a nemzetközi kiberbiztonsági együttműködés előmozdítása érdekében.

### **TANÚSÍTÁS**

**A tanúsítási keret hozzá fog járulni a célkitűzések eléréséhez azáltal,** hogy növeli az IKT-termékek és -szolgáltatások kiberbiztonsági szintjének általános átláthatóságát<sup>45</sup>, és ilyen módon erősíti a digitális egységes piac és a digitális innováció iránti bizalmat. Ez továbbá az uniós tanúsítási rendszerek és a kapcsolódó biztonsági követelmények és értékelési kritériumok tagállamok és ágazatok közötti összehangolatlanságának elkerüléséhez is hozzá fog járulni.

#### **1.4.3. Várható eredmény(ek) és hatás(ok)**

*Tüntesse fel, milyen hatásokat gyakorolhat a javaslat/kezdemenyezés a kedvezményezettek/célcsoportokra.*

A megerősített ENISA (a képességek, a megelőzés, az együttműködés és a tudatosság uniós szintű támogatásával, és ezért az Unió kibertámadásokkal szembeni teljes körű ellenálló képességének növelésére való alkalmasságával), valamint az IKT-termékek és -szolgáltatások uniós tanúsítási keretrendszerének támogatása várhatóan a következő hatásokkal jár majd (a teljesség igénye nélkül):

#### **Összhatás:**

– Összességében pozitív hatás a belső piacra nézve a piac széttagoltsága csökkenésének és a digitális technológiákba vetett bizalomnak köszönhetően, amit a jobb együttműködés, az EU kiberbiztonsági politikáinak összehangoltabb megközelítései és az uniós szintű képességek növekedése révén érnek el. Mindennek pozitív gazdasági hatással kell járnia azáltal, hogy hozzájárul a kiberbiztonsági/kiberbűnözési események költségeinek csökkentéséhez, amelyeknél a becsült gazdasági hatás az Unió GDP-jének 0,41 %-át teszi ki (azaz mintegy 55 milliárd EUR-t).

#### **Konkrét eredmények:**

***Javulás a tagállamok és vállalkozások kiberbiztonsági képességeit és felkészültségét illetően***

<sup>45</sup>

A kiberbiztonsági szint átláthatósága azt jelenti, hogy a felhasználók elegendő információhoz jutnak a kiberbiztonsági tulajdonságokra vonatkozóan, amelynek révén objektív módon képesek meghatározni egy adott IKT-termék, -szolgáltatás vagy -folyamat biztonsági szintjét.

– Javulás a tagállamok kiberbiztonsági képességeit és felkészültségét illetően (a kiberfenyegetésekre és kiberbiztonsági eseményekre vonatkozó hosszú távú stratégiai elemzésnek, az iránymutatásnak és jelentéseknek, a szakértelem és a bevált gyakorlatok átadásának, a képzés és az oktatási anyagok hozzáférhetővé tételének, és a CyberEurope megerősített gyakorlatának köszönhetően).

– Javulás a magánszereplők képességeit illetően a különböző ágazatokban létrejött információmegosztási és elemző központok (ISAC-ok) révén.

– Javulás az uniós és tagállami kiberbiztonsági felkészültség terén, a CyberEurope gyakorlatainak részeként tesztelt, nagy léptékű, határokon átnyúló kiberbiztonsági események szintjén kipróbált és közösen elfogadott tervek rendelkezésre állásának köszönhetően.

***Javulás a tagállamok, uniós intézmények, hivatalok és szervek közötti együttműködés és koordináció területén***

– Hatékonyabb együttműködés az állami és magánszektor szintjén és a két szektor között.

– Nagyobb összhang a kiberbiztonsági irányelv végrehajtási megközelítései terén a tagállamok és ágazatok között.

– Fokozottabb együttműködés a tanúsítás területén az európai kiberbiztonsági tanúsítási rendszerek fejlesztését és egy közös kiberbiztonsági szakpolitika kialakítását ösztönző intézményi keretnek köszönhetően.

***Javulás a tagállamok fellépését kiegészítő uniós szintű képességek területén***

– Hatékonyabb „uniós műveleti kapacitás”, amely kiegészíti a tagállamok fellépését, és igény szerint, valamint korlátozott számú és előre meghatározott szolgáltatások tekintetében támogatást nyújt a számukra; mindezek várhatóan mind tagállami, mind uniós szinten kedvező hatással lesznek a biztonsági események megelőzésének, észlelésének sikerességére és az ilyen eseményekre való reakció eredményességére.

***Javulás a magánfelhasználók és a vállalkozások kiberbiztonsággal kapcsolatos tudatosságának növelése terén***

– Javulás a magánfelhasználók és a vállalkozások kiberbiztonsággal kapcsolatos általános tudatosságának növelése terén.

– Az IKT-termékekkel és -szolgáltatásokkal kapcsolatos tájékozott vásárlási döntések megalapozottabbá válása a kiberbiztonsági tanúsításnak köszönhetően.

***A digitális egységes piac és digitális innováció iránti megerősített bizalom az IKT-termékek és -szolgáltatások kiberbiztonsági szintjének fokozottabb átláthatósága révén***

– Az IKT-termékek és -szolgáltatások kiberbiztonsági szintjének fokozottabb átláthatósága<sup>46</sup> az uniós keret részeként megvalósuló egyszerűbb biztonsági tanúsítási eljárásoknak köszönhetően.

– Javulás az IKT-termékek és -szolgáltatások biztonsági tulajdonságainak biztosítása terén.

– Egyszerűsített eljárásokkal, a költségek csökkentésével és a piaci széttagoltság által nem gátolt uniós szintű üzleti lehetőségekkel ösztönzött biztonsági tanúsítás fokozottabb használata

<sup>46</sup>

A kiberbiztonsági szint átláthatósága azt jelenti, hogy a felhasználók elegendő információhoz jutnak a kiberbiztonsági tulajdonságokra vonatkozóan, amelynek révén objektív módon képesek meghatározni egy adott IKT-termék, -szolgáltatás vagy -folyamat biztonsági szintjét.

– Versenyképesebb uniós kiberbiztonsági piac az alacsonyabb költségeknek és a kkv-kat érintő kisebb adminisztratív terheknek köszönhetően, valamint a több nemzeti tanúsítási rendszer miatt esetlegesen előálló piacra lépési korlátok megszüntetése.

#### **Egyéb**

- Egyik célkitűzés esetében sem várható jelentős környezeti hatás.
- Az Unió intézményeinek, hivatalainak és szerveinek tevékenységei közötti fokozottabb együttműködés és koordináció révén hatékonyságnövekedés az Unió költségvetését illetően.

#### **1.4.4. Eredmény- és hatásmutatók**

*Tüntesse fel a javaslat/kezdemenyezés megvalósításának nyomon követését lehetővé tevő mutatókat.*

a)

##### **Célkitűzés: A tagállamok és vállalkozások képességeinek és felkészültségének javítása:**

- Az ENISA által szervezett képzések száma
- Az ENISA által nyújtott közvetlen segítség földrajzi lefedettsége (az országok és területek száma)
- A tagállamok által a CSIRT kifarrottsága és a kiberbiztonsággal kapcsolatos szabályozási intézkedések felügyelete terén elért készenléti szint
- Az ENISA által biztosított, a kritikus infrastruktúrákra vonatkozó uniós szintű bevált gyakorlatok száma
- Az ENISA által biztosított, a kkv-kra vonatkozó uniós szintű bevált gyakorlatok száma
- A kiberfenyegetések és kiberbiztonsági események éves stratégiai elemzésének közzététele az új tendenciák ENISA általi azonosítása céljából
- Az ENISA rendszeres hozzájárulása az európai szabványügyi szervezetek (ESO) kiberbiztonsági munkacsoportjainak munkájához.

##### **Célkitűzés: A tagállamok, uniós intézmények, hivatalok és szervek közötti együttműködés és koordináció javítása:**

- Azon tagállamok száma, amelyek a szakpolitikai döntés-előkészítés során felhasználták az ENISA ajánlásait és véleményét
- Azon uniós intézmények, hivatalok és szervek száma, amelyek a szakpolitikai döntés-előkészítés során felhasználták az ENISA ajánlásait és véleményét
- A CSIRT-hálózat munkaprogramjának rendszeres végrehajtása és a hálózat informatikai infrastruktúrájának és kommunikációs csatornáinak megfelelő működtetése
- Az együttműködési csoport számára elérhető és az általa felhasznált technikai jelentések száma
- Összehangolt megközelítés a kiberbiztonsági irányelv végrehajtása terén a tagállamok és ágazatok szintjén
- Az ENISA által végrehajtott jogszabályi megfelelésértékelések száma

- A különböző ágazatokban működő, különösen a kritikus infrastruktúrákkal foglalkozó ISAC-ok száma
- Az uniós intézményektől, hivataloktól és szervektől származó kiberbiztonsági tudnivalók terjesztésére szolgáló információs platform létrehozása és rendszeres működtetése
- Rendszeres hozzájárulás az Unió kutatási és innovációs munkaprogramjainak előkészítéséhez
- Együttműködési megállapodás az ENISA, az EC3 és a CERT-EU között
- A keretrendszer részét képező és annak részeként létrehozott tanúsítási rendszerek száma

**Célkitűzés: A tagállami fellépések kiegészítését szolgáló uniós szintű képességek növelése, különösen a határon átnyúló kiberválságok esetében:**

- A kiberfenyegetések és kiberbiztonsági események éves stratégiai elemzésének közzététele az új tendenciák ENISA általi azonosítása céljából
- A kiberbiztonsági irányelvvel összhangban bejelentett biztonsági események összesített információinak az ENISA általi közzététele
- Az Ügynökség által koordinált páneurópai gyakorlatok, valamint az érintett tagállamok és szervezetek száma
- A tagállamok által az ENISA-hoz bejelentett és az Ügynökség által teljesített veszélyhelyzet-reagálási kérések száma
- A sebezhetőségek, informatikai hibák és biztonsági események ENISA által a CERT-EU-val együttműködve végzett elemzésének száma
- Az Unió egészére kiterjedő helyzetjelentések rendelkezésre bocsátása az ENISA számára a tagállamok és egyéb jogalanyok által a nagy léptékű, határokon átnyúló kiberbiztonsági eseményeket érintően átadott információk alapján.

**Célkitűzés: A magánfelhasználók és a vállalkozások tudatosságának növelése kiberbiztonsági kérdésekkel kapcsolatban.**

- Rendszeres uniós szintű és a nemzeti tudatosságnövelő kampányok szervezése, valamint a témák rendszeres frissítése a felmerülő tanulási igényeknek megfelelően
- A kiberbiztonsággal kapcsolatos tudatosság növelése az Unió polgárai körében
- Rendszeres kvízek lebonyolítása a kiberbiztonsággal kapcsolatos tudatosság mérésére, és a helyes válaszok arányának idővel történő növekedése
- A munkavállalóknak és szervezeteknek szánt, a kiberbiztonsággal és kiberhigiéniával kapcsolatos bevált gyakorlatok rendszeres közzététele.

**Célkitűzés: A digitális egységes piac és digitális innováció iránti bizalom megerősítése az IKT-termékek és -szolgáltatások kiberbiztonsági szintje<sup>47</sup> általános átláthatóságának növelésével.**

<sup>47</sup>

A kiberbiztonsági szint átláthatósága azt jelenti, hogy a felhasználók elegendő információhoz jutnak a kiberbiztonsági tulajdonságokra vonatkozóan, amelynek révén objektív módon képesek meghatározni egy adott IKT-termék, -szolgáltatás vagy -folyamat biztonsági szintjét.

- Az uniós keretrendszerhez csatlakozó rendszerek száma
- Az IKT-biztonsági tanúsítvány megszerzésével járó költség csökkentése
- Az IKT-tanúsításra szakosodott megfelelőségértékelő szervezetek száma tagállami szinten
- Az európai kiberbiztonsági tanúsítási csoport létrehozása és üléseinek rendszeres megszervezése
- A tanúsításra vonatkozó iránymutatások a meglévő uniós keretrendszerrel összhangban
- Az eredmények rendszeres közzététele az uniós kiberbiztonsági piac főbb tendenciáinak elemzéséről
- Az európai kiberbiztonsági tanúsítási keretrendszernek megfelelően tanúsított IKT-termékek és -szolgáltatások száma
- Olyan végfelhasználók egyre növekvő száma, akik tisztában vannak az IKT-termékek és -szolgáltatások biztonsági jellemzőivel

b)

#### 1.4.5. Rövid vagy hosszú távon kielégítendő szükséglet(ek)

Figyelembe véve a szabályozási követelményeket és a kiberbiztonsági fenyegetések gyorsan változó jellegét, az ENISA megbízatását felül kell vizsgálni, hogy új feladatokat és funkciókat határozzanak meg a számára azért, hogy hatékonyan és eredményesen támogassa a tagállamok, az uniós intézmények és az érdekeltek biztonságos uniós kibertér kialakítására irányuló erőfeszítéseit. A megbízatás javasolt hatálya pontosan körül van határolva – megerősíti azokat a területeket, ahol az Ügynökség egyértelműen hozzáadott értéket mutat, illetve olyan új területekkel egészül ki, ahol az új szakpolitikai prioritások és eszközök – mindenekelőtt a kiberbiztonsági irányelv, az uniós kiberbiztonsági stratégia felülvizsgálata, a kiberválsággal összefüggő együttműködésről szóló, készülő uniós kiberbiztonsági tervezet és az IKT biztonsági tanúsítás – vonatkozásában támogatásra van szükség. Az új, javasolt megbízatás erőteljesebb és központibb szerepet kíván biztosítani az Ügynökség számára mindenekelőtt azzal, hogy az Ügynökség a tagállamokat is aktívabban támogatja bizonyos fenyegetések elhárításában (operatív kapacitás), illetve hogy szakértői központtá válva támogatja a tagállamokat és a Bizottságot a kiberbiztonsági tanúsítás területén.

Ugyanakkor a javaslat létrehozza az európai kiberbiztonsági tanúsítási keretrendszert (a továbbiakban: keretrendszer) az IKT-termékekre és -szolgáltatásokra vonatkozóan, és meghatározza az ENISA alapvető funkcióit és feladatait a kiberbiztonsági tanúsítás területén. A keretrendszer olyan közös rendelkezéseket és eljárásokat ír elő, amelyek lehetővé teszik az adott IKT-termékekre/-szolgáltatásokra, illetve a kiberbiztonsági kockázatokra irányuló uniós szintű kiberbiztonsági tanúsítási rendszerek létrehozását. Az európai kiberbiztonsági tanúsítási rendszerek keretrendszerrel összhangban történő létrehozása lehetővé teszi majd egyfelől, hogy az ilyen rendszerek részeként kiállított tanúsítványok minden tagállamban érvényesek legyenek, illetve minden tagállam elismerje őket, másfelől, hogy kezelje a piac jelenlegi széttagoltságát.

#### 1.4.6. Az uniós részvételből adódó többletérték

A kiberbiztonság valóban globális kérdés, amely természeténél fogva határokon átívelő terület, és egyre több ágazatot érint a hálózatok és az információs rendszerek közötti



kölcsönös függések miatt. A kiberbiztonsági események száma, összetettsége és mérete, valamint a gazdaságra és társadalomra gyakorolt hatása idővel egyre nagyobb lesz, és a technológia fejlődésével, például a dolgok internetének terjedésével párhuzamosan pedig még tovább nő. Ez azt jelenti, hogy a tagállamok, az uniós intézmények és a magánszereplők részéről nem várható a jövőre nézve, hogy csökkenjen az igény a kiberbiztonsági fenyegetésekkel szembeni fokozott közös erőfeszítések iránt.

2004-es megalakulása óta az ENISA célja, hogy előmozdítsa a tagállamok és a hálózat- és információbiztonság terén érintettek közötti együttműködést, egyebek mellett a köz- és a magánszféra közötti együttműködés támogatása révén. Az együttműködés támogatásának részeként az Ügynökség technikai munkát is végzett annak érdekében, hogy felvázolja az Unió fenyegetettségi térképét, szakértői csoportot hozzon létre, valamint páneurópai kiberbiztonsági események és válságok kezelésére szolgáló gyakorlatokat szervezzen az állami és magánszektor számára (különösen a „Cyber Europe”-ot). A kiberbiztonsági irányelv további feladatokat ruházott az ENISA-ra, köztük a tagállamok közötti operatív együttműködést elősegítő CSIRT-hálózat titkársági szerepét.

A 2016. évi tanácsi következtetések<sup>48</sup> elismerték az uniós szintű fellépés hozzáadott értékét, különösen a tagállamok, de a hálózat- és információbiztonsági közösségek közötti együttműködés fokozását illetően is, és ahogy az az ENISA 2017. évi értékeléséből is világosan kitűnik, az Ügynökség hozzáadott értéke elsősorban abban rejlik, hogy képes megerősíteni az érdekelték közötti együttműködést. Uniós szinten az ENISA az egyetlen olyan szereplő, amelyik ilyen sokféle érdekelt együttműködését támogatja a hálózat- és információbiztonság területén.

Az ENISA nemcsak a kiberbiztonsági közösségek és érdekelték összehozása, de a tanúsítás terén is hozzáadott értékkel bír. A kiberbűnözés és a biztonsági fenyegetések megjelenése olyan nemzeti kezdeményezéseket eredményezett, amelyek magas szintű kiberbiztonsági és tanúsítási követelményeket határoznak meg a hagyományos infrastruktúrában használt IKT-összetevők számára. Noha fontosak ezek a kezdeményezések, az egységes piac szétagoltságát eredményezhetik, és akadályokat gördíthetnek az átjárhatóság elé. Előfordulhat, hogy az IKT-gyártóknak több tanúsítási eljárás is át kell menniük ahhoz, hogy több tagállam piacán értékesíthessék termékeiket. Nem valószínű, hogy a jelenlegi tanúsítási rendszerek eredménytelensége/sikertelensége uniós beavatkozás hiányában orvosolható. Nagyon valószínű, hogy intézkedés hiányában a piac szétagoltsága tovább nő rövid és középtávon (az elkövetkező 5–10 évben), ha új tanúsítási rendszerek látnak napvilágot. A koordináció és az átjárhatóság hiánya az ilyen rendszerek között olyan tényező, amely csökkenti a digitális egységes piac létrejöttének esélyeit. Éppen ezért jelent hozzáadott értéket egy olyan európai kiberbiztonsági tanúsítási keretrendszer létrehozása az IKT-termékek és -szolgáltatások vonatkozásában, amely megfelelő feltételeket biztosít a különböző tagállamokban egyidejűleg meglévő többféle tanúsítási rendszerrel járó problémák hatékony kezeléséhez, miközben csökkenti a költségeket és ennél fogva kereskedelmi és versenyképességi szempontból összességében Uniós-szerte vonzóbbá teszi a tanúsítást.

#### 1.4.7. Hasonló korábbi tapasztalatok tanulsága

Az ENISA jogalapjának megfelelően a Bizottság elvégezte az Ügynökség értékelését, amely független tanulmányt, valamint nyilvános konzultációt is magában foglal. Az

<sup>48</sup> A Tanács következtetései Európa kibertámadásokkal szembeni ellenálló képességének erősítéséről, valamint a versenyképes és innovatív kiberbiztonsági ágazat támogatásáról – 2016. november 15.

értékelés arra a következtetésre jutott, hogy az ENISA célkitűzései ma is időszerűek. Figyelembe véve a technológiai fejlődést, a kialakuló fenyegetéseket és azt, hogy megnövekedett az igény a hálózat- és információbiztonság iránt az Unióban, szükség van technikai szakértelemre az újabbnál újabb hálózat- és információbiztonsági kérdések kezeléséhez. A tagállamokban kapacitásokat kell kialakítani a fenyegetések megértése és az azokra való reagálás érdekében, a tematikus területek és intézmények érdekeltjeinek pedig együtt kell működniük.

Az Ügynökség sikeres munkát végez a megnövekedett hálózat- és információbiztonság terén Európa-szerte azáltal, hogy kapacitást épít az Unió 28 tagállamában, miközben megerősíti az együttműködést a tagállamok és a hálózat- és információbiztonság területén érdekelték között; emellett szakértelmével, közösségépítő erejével és a szakpolitika támogatásával is kitűnik.

Noha az ENISA – legalábbis bizonyos mértékig – hatást ért el a hálózat- és információbiztonság tágabb területén, összességében nem tudott erős márkanévet kialakítani és elegendő ismertséget szerezni ahhoz, hogy Európa szakértői központjaként ismerjék el. Ennek oka, hogy az ENISA megbízatása széles körű, amihez nem társult arányaiban elegendő erőforrás. Ezen túlmenően továbbra is az ENISA az egyetlen határozott idejű megbízatással rendelkező uniós ügynökség, ami korlátozza abban, hogy hosszú távú jövőképet fogalmazzon meg és fenntartható módon támogassa érdekeltjeit. Ez szintén ellentétes a kiberbiztonsági irányelv rendelkezéseivel, amelyek határozatlan időre szóló feladatokat ruháznak az ENISA-ra.

Jelenleg nincs olyan európai keretrendszer, amely az IKT-termékekre és -szolgáltatásokra vonatkozó kiberbiztonsági tanúsítást szabályozná. Mindazonáltal a kiberbűnözés és a biztonsági fenyegetések növekedése nemzeti kezdeményezések megjelenését eredményezte, ami az egységes piac szétagoltságának veszélyét rejti magában.

#### 1.4.8. Egyéb releváns eszközökkel való összeegyeztethetőség és lehetséges szinergia

A kezdeményezés és a meglévő politikák között igen nagy a koherencia, különösen, ami a belső piacot illeti. Valóban, a kezdeményezés a kiberbiztonság átfogó megközelítésével összhangban, a digitális egységes piaci stratégia felülvizsgálatának megfelelően született, hogy kiegészítsen egy átfogó intézkedéscsomagot, amely magában foglalja az uniós kiberbiztonsági stratégia felülvizsgálatát, a kiberválsággal összefüggő együttműködés tervezetét és a kiberbűnözés elleni küzdelemre irányuló kezdeményezéseket. Ez összhangban lenne a meglévő kiberbiztonsági jogszabályok rendelkezéseivel, különösen a kiberbiztonsági irányelvvel, és ezekre építene, hogy a képességek, az együttműködés, a kockázatkezelés és a kiberbiztonsági ismeretek megerősítése révén a kezdeményezés tovább növelje az Unió kibertámadásokkal szembeni ellenálló képességét.

A javasolt tanúsítási intézkedéseknek kezelniük kell a meglévő és új nemzeti tanúsítási rendszerek miatt esetleg kialakuló szétagoltságot, hozzájárulva ezáltal a digitális egységes piac fejlődéséhez. A kezdeményezés ezen túlmenően támogatja és kiegészíti a kiberbiztonsági irányelv végrehajtását olyan módon, hogy az irányelv hatálya alá tartozó vállalatokat eszközzel látja el annak igazolására, hogy az Unió egészében megfelelnek a hálózat és információbiztonsági előírásoknak.

Az európai kiberbiztonsági tanúsítási keret a javasolt formában nem érinti az általános adatvédelmi rendeletet<sup>49</sup> és különösen annak tanúsításról szóló rendelkezéseit<sup>50</sup>, mivel azok a személyes adatok feldolgozásával kapcsolatos biztonsági kérdésekkel foglalkoznak. Végül, de nem utolsósorban, a leendő európai keretrendszerben javasolt rendszereknek – lehetőség szerint – nemzetközi szabványokra kell épülniük, hogy ne gördítsenek akadályokat a kereskedelem útjába, és biztosítsák a nemzetközi kezdeményezésekkel való koherenciát.

---

<sup>49</sup> Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).

<sup>50</sup> Lásd a tanúsításról szóló 42. és a tanúsító szervezetekről szóló 43. cikket, valamint a feladatokról szóló 57., a független felügyeleti hatóságok hatásköreiről szóló 58. és az Európai Adatvédelmi Testület feladatairól szóló 70. cikket.

### 1.5. Az intézkedés és a pénzügyi hatás időtartama

- ☐ A javaslat/kezdeményezés határozott időtartamra vonatkozik
  - ☐ A javaslat/kezdeményezés időtartama: ÉÉÉÉ [HH/NN]-tól/-től ÉÉÉÉ [HH/NN]-ig
  - ☐ Pénzügyi hatás: ÉÉÉÉ-től/-től ÉÉÉÉ-ig
- ☒ A javaslat/kezdeményezés határozatlan időtartamra vonatkozik
  - Beindítási időszak: 2019-től 2020-ig,
  - azt követően: rendes ütem.

### 1.6. Tervezett irányítási módszer(ek)<sup>51</sup>

- ☒ Bizottság általi közvetlen irányítás (III. cím – Tanúsítás)
  - ☐ végrehajtó ügynökségek
- ☐ Megosztott irányítás a tagállamokkal
- ☒ Közvetett irányítás a költségvetés végrehajtásával kapcsolatos feladatoknak a következőkre történő átruházásával:
  - ☐ nemzetközi szervezetek és ügynökségek (nevezze meg)
  - ☐ az EBB és az Európai Beruházási Alap
  - ☒ a 208. és 209. cikkben említett szervek (II. cím – ENISA)
  - ☐ közjogi szervek
  - ☐ magánjog alapján működő, közfeladatot ellátó szervek, olyan mértékben, amennyiben megfelelő pénzügyi garanciákat nyújtanak
  - ☐ a valamely tagállam magánjoga alapján működő, köz- és magánszféra közötti partnerség végrehajtásával megbízott és megfelelő pénzügyi garanciákat nyújtó szervek
  - ☐ az EUSZ V. címének értelmében a KKBP terén konkrét fellépések végrehajtásával megbízott, és a vonatkozó alap-jogiaktusban meghatározott személyek.

#### Megjegyzések

A rendelet hatálya a következőkre terjed ki:

- a rendeletjavaslat II. címe felülvizsgálja az Európai Unió Hálózat- és Információbiztonsági Ügynökség (ENISA) megbízatását, miközben fontos szerepet ad neki a tanúsítás terén,
- a III. cím pedig keretrendszert hoz létre az IKT-termékek és -szolgáltatások európai kiberbiztonsági tanúsítási rendszereinek létrehozására vonatkozóan, amiben az ENISA meghatározó szerepet játszik.

<sup>51</sup>

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

## 2. IRÁNYÍTÁSI INTÉZKEDÉSEK

### 2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

*Gyakoriság és feltételek*

A nyomon követés a jogi eszköz elfogadását követően azonnal megkezdődik, és annak alkalmazására fog összpontosítani. A Bizottság az ENISA-val, a tagállamok képviselőivel (pl. szakértői csoportokkal) és az érdekelttel közös találkozókat fog szervezni, mindenekelőtt azért, hogy megkönnyítse a tanúsításra vonatkozó szabályok végrehajtását, például az igazgatótanács létrehozását.

Az első értékelésnek a jogi eszköz hatálybalépését követő öt év elteltével kell lezajlania, feltéve, hogy elegendő adat áll rendelkezésre. A Bizottság független értékelésének alapjául szolgáló explicit értékelési és felülvizsgálati záradék [XXX. cikk] a jogi eszköz része. A Bizottság ezt követően jelentést készít az Európai Parlamentnek és a Tanácsnak az értékeléséről, amelyet adott esetben egy felülvizsgálatra irányuló javaslat kísér, a rendelet hatásának és hozzáadott értékének a mérése céljából. Minden további felülvizsgálatot ötévente kell elvégezni. Az értékelés során a minőségi jogalkotást ösztönző bizottsági módszert fogják alkalmazni. Ezeket az értékeléseket célzott szakértői megbeszélések, tanulmányok és az érdekelttek részvételével zajló, átfogó konzultációk segítségével folytatják le.

Az ENISA ügyvezető igazgatójának két évente utólagos értékelést kell benyújtani az ENISA tevékenységeiről az igazgatótanács számára. Az Ügynökségnek továbbá nyomonkövetési cselekvési tervet kell készítenie a visszamenőleges értékelések következtetéseiről, és két évente jelentést kell benyújtania a Bizottságnak az elért eredményekről. Az igazgatótanács feladata, hogy figyelemmel kísérje az ilyen következtetések megfelelő nyomon követését.

Az Ügynökség tevékenységei során felmerülő hivatali visszasságok eseteit az európai ombudsman vizsgálja a Szerződés 228. cikkével összhangban.

A tervezett ellenőrzés adatai többnyire az ENISA-tól, az európai kiberbiztonsági tanúsítási csoporttól, az együttműködési csoporttól, a CSIRT-hálózattól és a tagállamok hatóságaitól származnak. Az ENISA, az európai kiberbiztonsági tanúsítási csoport, az együttműködési csoport és a CSIRT-hálózat jelentéseiből (az éves tevékenységi jelentéseket is ideértve) származó adatok mellett szükség szerint egyedi adatgyűjtési eszközöket is használnak majd (például nemzeti hatóságoknak szóló felméréseket, az Eurobarométer felméréseit, a kiberbiztonsági havi kampányok jelentéseit és a páneurópai gyakorlatokat).

## 2.2. Irányítási és kontrollrendszer

### 2.2.1. Felismert kockázat(ok)

A felismert kockázatok száma korlátozott: az uniós ügynökség már működik, megbízatásának javasolt alkalmazási körét pontosan körülhatárolják; ez megerősíti azokat a területeket, ahol az Ügynökség egyértelműen hozzáadott értéket mutat, illetve olyan új területekkel egészül ki, ahol az új szakpolitikai prioritások és eszközök – mindenekelőtt a kiberbiztonsági irányelv, az uniós kiberbiztonsági stratégia felülvizsgálata, a kiberválsággal összefüggő együttműködésről szóló készülő uniós kiberbiztonsági tervezet és az informatikai biztonsági tanúsítás – vonatkozásában támogatásra van szükség.

A javaslat ezért az Ügynökség feladatait részletezi, és hatékonyságnövekedést eredményez. Az operatív hatáskörök és feladatok bővülése nem jelent valós kockázatot, mivel igény szerint a tagállamok fellépését egészítené ki és támogatná korlátozott és előre meghatározott szolgáltatások vonatkozásában.

Ezen túlmenően az Ügynökség javasolt modellje – a közös megközelítésnek megfelelően – biztosítja, hogy megfelelő ellenőrzési módszereket alkalmazzanak annak megállapítására, hogy az ENISA eleget tesz-e célkitűzései teljesítésének. A javasolt változtatások operatív és pénzügyi kockázata csekélynek tűnik.

Ugyanakkor megfelelő pénzügyi forrásokat kell biztosítani annak érdekében, hogy az ENISA teljesíteni tudja az új megbízatásából fakadó feladatokat, a tanúsítás területén is.

#### 2.2.2. *Tervezett ellenőrzési mód(ok)*

Az Ügynökség beszámolóit a Számvevőszéknek kell jóváhagyásra benyújtani, és az előirányzott mentesítési eljárásnak és auditoknak kell alávetni.

Emellett az Ügynökség működését a Szerződés 228. cikkének rendelkezéseivel összhangban az ombudsman felügyeli.

Lásd még a fenti 2.1. és 2.2.1. pontot.

### 2.3. **A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések**

*Tüntesse fel a meglévő vagy tervezett megelőző és védintézkedéseket.*

Az ENISA megelőzési és védelmi intézkedései az alábbi esetekben kifejezetten alkalmazandók:

– A megrendelt szolgáltatásokat és felméréseket az Ügynökség személyi állománya a kifizetés előtt a szerződéses kötelezettségek, a gazdaságossági elvek, valamint a helyes pénzügyi és vezetési gyakorlat figyelembevételével ellenőrzi. Az Ügynökség és a kifizetések kedvezményezettjei között létrejövő mindennemű megállapodás és szerződés – felügyelet, jelentéstételi kötelezettség stb. formájában – tartalmazni fog csalás elleni rendelkezéseket.

– A csalások, korrupció és egyéb jogellenes tevékenységek elleni küzdelem érdekében az Európai Csalás Elleni Hivatal (OLAF) által lefolytatott vizsgálatokról szóló, 1999. május 25-i 883/2013/EU, Euratom európai parlamenti és tanácsi rendelet előírásait kell alkalmazni minden korlátozás nélkül.

– Az Ügynökség e rendelet hatálybalépésétől számított hat hónapon belül csatlakozik az Európai Parlament, az Európai Unió Tanácsa és az Európai Közösségek Bizottsága között az Európai Csaláselleni Hivatal (OLAF) belső vizsgálatairól szóló, 1999. május 25-i intézményközi megállapodáshoz, és haladéktalanul meghozza az Ügynökség valamennyi alkalmazottjára alkalmazandó megfelelő rendelkezéseket.

### 3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

#### 3.1. A többéves pénzügyi keret mely fejezetét/fejezeteit és a költségvetés mely kiadási tételét/tételeit érintik a kiadások?

- Jelenlegi költségvetési tételek

A többéves pénzügyi keret fejezetei, azon belül pedig a költségvetési tételek sorrendjében.

| A többéves pénzügyi keret fejezete                        | Költségvetési tétel                                                                                                                                                                          | Kiadási típusa                | Hozzájárulás                   |                                     |                      |                                                                          |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|--------------------------------|-------------------------------------|----------------------|--------------------------------------------------------------------------|
|                                                           |                                                                                                                                                                                              | Diff./Nem diff. <sup>52</sup> | EFTA-országoktól <sup>53</sup> | tagjelölt országoktól <sup>54</sup> | harmadik országokból | a költségvetési rendelet 21. cikke (2) bekezdésének b) pontja értelmében |
| 1a. Versenyképesség a növekedésért és a foglalkoztatásért | 09.0203 Az ENISA, valamint az információs és kommunikációs technológiák biztonsági tanúsítása                                                                                                | diff.                         | IGEN                           | NEM                                 | NEM                  | NEM                                                                      |
| 5<br>Igazgatási kiadások:                                 | 09.0101 A „Tartalmak, technológiák és kommunikációs hálózatok” területén aktív állományban lévő alkalmazottakkal kapcsolatos kiadások<br>09.0102 A „Tartalmak, technológiák és kommunikációs | Nem diff.                     | NEM                            | NEM                                 | NEM                  | NEM                                                                      |

<sup>52</sup> Diff. = Differenciált előirányzatok / Nem diff. = Nem differenciált előirányzatok.

<sup>53</sup> EFTA: Európai Szabadkereskedelmi Társulás.

<sup>54</sup> Tagjelölt országok és adott esetben a nyugat-balkáni potenciális tagjelölt országok.

|  |                                                                                  |  |  |  |  |  |
|--|----------------------------------------------------------------------------------|--|--|--|--|--|
|  | hálózatok” területén foglalkoztatott külső alkalmazottakkal kapcsolatos kiadások |  |  |  |  |  |
|  | 09.010211 Egyéb igazgatási kiadások                                              |  |  |  |  |  |

### 3.2. A kiadásokra gyakorolt becsült hatás

#### 3.2.1. A kiadásokra gyakorolt becsült hatás összegzése

millió EUR (három tizedesjegyig)

| A többéves pénzügyi keret fejezete                                                                                                                                                     |                                      | 1a   | Versenyképesség a növekedésért és a foglalkoztatásért |                        |        |        |        |          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|------|-------------------------------------------------------|------------------------|--------|--------|--------|----------|
| ENISA                                                                                                                                                                                  |                                      |      | Alap-helyzet<br>2017<br>(31/12/2016)                  | 2019<br>(2019.7.1-től) | 2020   | 2021   | 2022   | ÖSSZESEN |
| 1. cím: Személyzeti kiadások<br>(a személyzet felvételéhez, a képzésekhez, a szociális-egészségügyi infrastruktúrához és a külső szolgáltatásokhoz kapcsolódó kiadásokat is beleértve) | Kötelezettségvállalási előirányzatok | (1)  | 6,387                                                 | 9,899                  | 12,082 | 13,349 | 13,894 | 49,224   |
|                                                                                                                                                                                        | Kifizetési előirányzatok             | (2)  | 6,387                                                 | 9,899                  | 12,082 | 13,349 | 13,894 | 49,224   |
| 2. cím: Infrastrukturális és igazgatási kiadások                                                                                                                                       | Kötelezettségvállalási előirányzatok | (1a) | 1,770                                                 | 1,957                  | 2,232  | 2,461  | 2,565  | 9,215    |
|                                                                                                                                                                                        | Kifizetési előirányzatok             | (2a) | 1,770                                                 | 1,957                  | 2,232  | 2,461  | 2,565  | 9,215    |
| 3. cím: Operatív kiadások                                                                                                                                                              | Kötelezettségvállalási előirányzatok | (3a) | 3,086                                                 | 4,694                  | 6,332  | 6,438  | 6,564  | 24,028   |
|                                                                                                                                                                                        | Kifizetési előirányzatok             | (3b) | 3,086                                                 | 4,694                  | 6,332  | 6,438  | 6,564  | 24,028   |



|                                            |                                      |                  |        |  |        |        |        |        |        |
|--------------------------------------------|--------------------------------------|------------------|--------|--|--------|--------|--------|--------|--------|
| Előirányzatok ÖSSZESEN<br>az ENISA számára | Kötelezettségvállalási előirányzatok | =1+1<br>a+3a     | 11,244 |  | 16,550 | 20,646 | 22,248 | 23,023 | 82,467 |
|                                            | Kifizetési előirányzatok             | =2+2<br>a<br>+3b | 11,244 |  | 16,550 | 20,646 | 22,248 | 23,023 | 82,467 |

|                                       |   |                       |
|---------------------------------------|---|-----------------------|
| A többéves pénzügyi keret<br>fejezete | 5 | „Igazgatási kiadások” |
|---------------------------------------|---|-----------------------|

millió EUR (három tizedesjegyig)

|                                                                                    |               | 2019<br>(2019.7.1-től) | 2020  | 2021  | 2022  | ÖSSZESEN |
|------------------------------------------------------------------------------------|---------------|------------------------|-------|-------|-------|----------|
| FŐIGAZGATÓSÁG: A Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága |               |                        |       |       |       |          |
| • Humán erőforrás                                                                  |               | 0,216                  | 0,846 | 0,846 | 0,846 | 2,754    |
| • Egyéb igazgatási kiadások                                                        |               | 0,102                  | 0,235 | 0,238 | 0,242 | 0,817    |
| CNECT Főigazgatóság<br>ÖSSZESEN                                                    | Előirányzatok | 0,318                  | 1,081 | 1,084 | 1,088 | 3,571    |

A személyzeti költségeket a tervezett felvételi dátumnak megfelelően számították ki (a foglalkoztatás várhatóan 2019. július 1-jétől kezdődik).

A 2020 utáni forrásokkal kapcsolatos kilátások indikatívak, és nem érintik a 2020 utáni többéves pénzügyi keretre vonatkozó bizottsági javaslatokat

|                           |                                 |       |       |       |       |       |
|---------------------------|---------------------------------|-------|-------|-------|-------|-------|
| A többéves pénzügyi keret | (Összes kötelezettségvállalási) | 0,318 | 1,081 | 1,084 | 1,088 | 3,571 |
|---------------------------|---------------------------------|-------|-------|-------|-------|-------|

|                                                              |                                                 |  |  |  |  |  |
|--------------------------------------------------------------|-------------------------------------------------|--|--|--|--|--|
| <b>5. FEJEZETÉHEZ tartozó<br/>előirányzatok<br/>ÖSSZESEN</b> | előirányzat = Összes<br>kifizetési előirányzat) |  |  |  |  |  |
|--------------------------------------------------------------|-------------------------------------------------|--|--|--|--|--|

millió EUR (három tizedesjegyig)

|                                                                                              |                                         | <b>2019</b> | <b>2020</b> | <b>2021</b> | <b>2022</b> | <b>ÖSSZESEN</b> |
|----------------------------------------------------------------------------------------------|-----------------------------------------|-------------|-------------|-------------|-------------|-----------------|
| <b>A többéves pénzügyi keret<br/>1–5. FEJEZETÉHEZ tartozó<br/>előirányzatok<br/>ÖSSZESEN</b> | Kötelezettségvállalási<br>előirányzatok | 16,868      | 21,727      | 23,332      | 24,11       | <b>86,038</b>   |
|                                                                                              | Kifizetési előirányzatok                | 16,868      | 21,727      | 23,332      | 24,11       | <b>86,038</b>   |

### 3.2.2. Az ügynökség előirányzataira gyakorolt becsült hatás

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

Kötelezettségvállalási előirányzatok, millió EUR (három tizedesjegyig)

| Tüntesse fel a célkitűzéseket és a teljesítéseket <sup>55</sup><br>↓                                                                                                            | 2019  | 2020  | 2021  | 2022  | ÖSSZESEN |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|-------|-------|----------|
| A tagállamok és vállalkozások képességeinek és felkészültségének javítása                                                                                                       | 1,408 | 1,900 | 1,931 | 1,969 | 7,208    |
| A tagállamok, uniós intézmények, hivatalok és szervek közötti együttműködés és koordináció javítása.                                                                            | 0,939 | 1,266 | 1,288 | 1,313 | 4,806    |
| A tagállamok fellépését kiegészítő uniós szintű képességek javítása, különösen határokon átnyúló kiberválságok esetén.                                                          | 0,704 | 0,950 | 0,965 | 0,985 | 3,604    |
| A magánfelhasználók és a vállalkozások tudatosságának növelése a kiberbiztonsággal kapcsolatos kérdésekben.                                                                     | 0,704 | 0,950 | 0,965 | 0,985 | 3,604    |
| A digitális egységes piac és digitális innováció iránti bizalom megerősítése az IKT-termékek és -szolgáltatások kiberbiztonsági szintje általános átláthatóságának növelésével. | 0,939 | 1,266 | 1,288 | 1,313 | 4,806    |
| <b>ÖSSZKÖLTSÉG</b>                                                                                                                                                              | 4,694 | 6,332 | 6,437 | 6,565 | 24,028   |

<sup>55</sup> Ez a táblázat csak a 3. cím szerinti operatív kiadásokat ismerteti.

### 3.2.3. Az Ügynökség humánerőforrására gyakorolt becsült hatás

#### 3.2.3.1. Összegzés

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

millió EUR (három tizedesjegyre)

|                                         | Q3/4, 2019   | 2020          | 2021          | 2022          |
|-----------------------------------------|--------------|---------------|---------------|---------------|
| Ideiglenes tisztviselők (AD besorolás)  | 4,242        | 5,695         | 6,381         | 6,709         |
| Ideiglenes tisztviselők (AST besorolás) | 1,601        | 1,998         | 2,217         | 2,217         |
| Szerződéses alkalmazottak               | 2,041        | 2,041         | 2,041         | 2,041         |
| Kirendelt nemzeti szakértők             | 0,306        | 0,447         | 0,656         | 0,796         |
| <b>ÖSSZESEN</b>                         | <b>8,190</b> | <b>10,181</b> | <b>11,295</b> | <b>11,763</b> |

A személyzeti költségeket a tervezett felvételi dátumnak megfelelően számították ki (az ENISA esetében a személyzet teljes foglalkoztatása várhatóan 2019. január 1-jétől kezdődik). Az új alkalmazottak foglalkoztatása előreláthatólag 2019. július 1-től kezdődően fokozatosan történik, és a teljes foglalkoztatottság 2022-ben valósul meg. A 2020 utáni forrásokkal kapcsolatos kilátások indikatívak, és nem érintik a 2020 utáni többéves pénzügyi keretre vonatkozó bizottsági javaslatokat.

#### Alkalmazottakra gyakorolt becsült hatás (további teljes munkaidős egyenérték) – létszámterv

| Tisztviselői besorolások és fokozatok | 2017<br>Jelenlegi ENISA | Q3/Q4.2019 | 2020 | 2021 | 2022 |
|---------------------------------------|-------------------------|------------|------|------|------|
| AD16                                  |                         |            |      |      |      |
| AD15                                  | 1                       |            |      |      |      |
| AD14                                  |                         |            |      |      |      |
| AD13                                  |                         |            |      |      |      |
| AD12                                  | 3                       | 3          |      |      |      |
| AD11                                  |                         |            |      |      |      |
| AD10                                  | 5                       |            |      |      |      |
| AD9                                   | 10                      | 2          |      |      |      |
| AD8                                   | 15                      | 4          | 2    |      | 1    |
| AD7                                   |                         |            | 3    | 3    | 2    |
| AD6                                   |                         |            | 3    | 3    |      |
| AD5                                   |                         |            |      |      |      |

|                  |           |           |           |          |          |
|------------------|-----------|-----------|-----------|----------|----------|
| AD összesen      | 34        | 9         | 8         | 6        | 3        |
| AST11            |           |           |           |          |          |
| AST10            |           |           |           |          |          |
| AST9             |           |           |           |          |          |
| AST8             |           |           |           |          |          |
| AST7             | 2         | 1         | 1         | 1        |          |
| AST6             | 5         | 2         | 1         |          |          |
| AST5             | 5         |           |           |          |          |
| AST4             | 2         |           |           |          |          |
| AST3             |           |           |           |          |          |
| AST2             |           |           |           |          |          |
| AST1             |           |           |           |          |          |
| AST összesen     | 14        | 3         | 2         | 1        |          |
| AST/SC 6         |           |           |           |          |          |
| AST/SC 5         |           |           |           |          |          |
| AST/SC 4         |           |           |           |          |          |
| AST/SC 3         |           |           |           |          |          |
| AST/SC 2         |           |           |           |          |          |
| AST/SC 1         |           |           |           |          |          |
| AST/SC összesen  |           |           |           |          |          |
| <b>VÉGÖSSZEG</b> | <b>48</b> | <b>12</b> | <b>10</b> | <b>7</b> | <b>3</b> |

A kiegészítő AD/AST személyzet feladatai az eszköz 1.4.2. szakaszban leírt célkitűzéseinek teljesítése érdekében:

| <b>Feladatok</b>                                  | <b>AD</b> | <b>AST</b> | <b>SNE</b> | <b>Összesen</b> |
|---------------------------------------------------|-----------|------------|------------|-----------------|
| Politika és kapacitásépítés                       | 8         | 1          |            | 9               |
| Operatív együttműködés                            | 8         | 1          | 7          | 16              |
| Tanúsítás (piaci feladatok)                       | 9         | 3          | 2          | 14              |
| Ismeretbővítés, tájékoztatás és tudatosságnövelés | 1         | 1          |            | 2               |
| <b>ÖSSZESEN</b>                                   | <b>26</b> | <b>6</b>   | <b>9</b>   | <b>41</b>       |

Az elvégzendő feladatok leírása:

| <b>Feladatok</b>                                                                   | <b>További szükséges erőforrások</b>                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Az uniós szakpolitika kidolgozása és végrehajtása, valamint kapacitásépítés</b> | A feladatok között szerepelne az együttműködési csoport támogatása, a kiberbiztonsági irányelv egységes, határokon átnyúló végrehajtása, valamint rendszeres jelentések készítése az uniós jogi keretrendszer végrehajtásának állapotáról; emellett az ágazati kiberbiztonsági kezdeményezésekkel összefüggő tanácsadás és koordinálás is ide tartozna, többek között az |

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                | energiaügy, a közlekedés (pl. a légi/közúti/tengeri közlekedés és az összekapcsolt járművek), az egészségügy és a pénzügyek terén, valamint a különböző ágazatokat érintő információmegosztási és elemző központok (ISAC-ok) létrehozásának támogatása is.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Operatív együttműködés és válságkezelés</b> | <p><b>Feladatok:</b></p> <p>A CSIRT-hálózat titkársági feladatainak biztosítása azáltal, hogy az Ügynökség többek között biztosítja a hálózat informatikai infrastruktúrájának és kommunikációs csatornáinak megfelelő működését. Strukturált együttműködés biztosítása a CERT-EU, az EC3 és más érdekelt uniós szervekkel.</p> <p><b>Cyber Europe gyakorlatok</b><sup>56</sup> – a kétévenkénti megszervezésről az évente való megrendezésre való átállással összefüggő feladatok, és annak biztosítása, hogy ezek a gyakorlatok a biztonsági események teljes életciklusát vizsgálják.</p> <p>Technikai segítségnyújtás – a feladatok magukban foglalják a CERT-EU-val való szervezett együttműködést, hogy technikai segítség álljon rendelkezésre jelentős biztonsági események esetén, valamint az események elemzésének támogatására. Idetartozna a tagállamoknak a biztonsági események kezeléséhez, valamint a sebezhetőségek, informatikai hibák és biztonsági események elemzéséhez nyújtott segítség. Az egyes tagállamok közötti együttműködés megkönnyítése szintén a feladatok közé tartozna a vészhelyzetek elhárítására vonatkozóan, a tagállamok és más szervezetek által önkéntes alapon rendelkezésre bocsátott információk alapján készített nemzeti helyzetjelentések elemzése és összesítése révén.</p> <p>Tervezet a nagy léptékű, határokon átnyúló kiberbiztonsági eseményekre és válsághelyzetekre adható, uniós szinten összehangolt reagálásról – az Ügynökség hozzájárul majd ahhoz, hogy uniós és tagállami szinten összehangolt válasz szülessen a nagy</p> |

<sup>56</sup>

A Cyber Europe jelenleg a legnagyobb és legátfogóbb uniós kiberbiztonsági gyakorlat, amelyen több mint 700 kiberbiztonsági szakértő vesz részt az Unió mind a 28 tagállamából. A gyakorlatot két évente rendezik meg. Az ENISA és a 2013-as uniós kiberbiztonsági stratégia értékelése rávilágított arra, hogy sok érdekelt szerint a kiberfenyegetések gyors kialakulása miatt évente kellene megrendezni a Cyber Europe gyakorlatokat. Erre azonban az Ügynökség korlátozott erőforrásai miatt jelenleg nincs lehetőség.

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                          | <p>léptékű, határokon átnyúló kiberbiztonsági eseményekre vagy válságokra, többek között azáltal, hogy közreműködik az uniós szintű helyzetismeret megalapozásától az eseményekre vonatkozó együttműködési tervek teszteléséig terjedő feladatokban.</p> <p>A biztonsági események utólagos technikai vizsgálata – a CSIRT-hálózattal együttműködve a biztonsági események utólagos technikai vizsgálatának lebonyolítása vagy támogatása, amelynek célja, hogy a jövőbeli események hatékonyabb megelőzésére nyilvánosan hozzáférhető jelentések formájában ajánlások szülessenek, és sor kerüljön a képességek megerősítésére.</p>                                                                                                                                                                                 |
| <b>Piaci feladatok (szabványosítás, tanúsítás)</b>       | <p>A feladatok közé tartozna a tanúsítási keretrendszer részeként végzett munka aktív támogatása, az európai kiberbiztonsági tanúsítási rendszerekre irányuló javaslatok kidolgozásához szükséges technikai szakértelem biztosítását is ideértve. Szintén a feladatok közé tartozik majd a szabványosítást, tanúsítást és piaci megfigyelőközpontot érintő uniós szakpolitika kidolgozásának és végrehajtásának támogatása – ehhez szükség lesz az elektronikus termékek, hálózatok és szolgáltatásokra vonatkozó kockázatkezelési szabványok átvételének lehetővé tételére, valamint tanácsadásra a műszaki biztonsági követelményekről az alapvető és digitális szolgáltatásokat nyújtó szolgáltatók számára. Ezen túlmenően a kiberbiztonsági piac főbb tendenciáinak elemzése is az Ügynökség feladata lesz.</p> |
| <b>Tudás- és információmegosztás, tudatosságnövelés:</b> | <p>Annak érdekében, hogy könnyebben lehessen hozzáférni megfelelően strukturált információkhoz a kiberbiztonsági kockázatokra és a lehetséges ellenintézkedésekre vonatkozóan, a javaslat új feladatot határoz meg az Ügynökség számára, amelynek célja az Unió információs központjának kialakítása és fenntartása. Idetartozna egy, a nyilvánosság tájékoztatására szolgáló, a hálózati és információs rendszerek biztonságával, különösen a kiberbiztonsággal kapcsolatos tudnivalók összegyűjtésével, rendszerezésével foglalkozó portál, amely elsősorban az uniós intézmények, hivatalok és szervek által rendelkezésre bocsátott információkat tartalmazná. Szintén a feladatok</p>                                                                                                                           |

|  |                                                                                                                                |
|--|--------------------------------------------------------------------------------------------------------------------------------|
|  | közé tartozna az ENISA tájékoztatás terén végzett tevékenységeinek támogatása, hogy az Ügynökség fokozni tudja erőfeszítéseit. |
|--|--------------------------------------------------------------------------------------------------------------------------------|



3.2.3.2. A felügyeletet ellátó főigazgatóságnál felmerülő, becsült humánerőforrás-szükségletek

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

*A becsléseket egész számmal (vagy legfeljebb egy tizedesjeggyel) kell kifejezni*

|                                                                                    |                   | További személyzet |          |      |      |
|------------------------------------------------------------------------------------|-------------------|--------------------|----------|------|------|
|                                                                                    | Alaphelyzet, 2017 | Q3/4 2019          | 2020     | 2021 | 2020 |
| • A létszámtervben szereplő álláshelyek (tisztviselők és ideiglenes alkalmazottak) |                   |                    |          |      |      |
| 09 01 01 01 (a központban és a bizottsági képvisleteken)                           | 1                 | 2                  | 3        |      |      |
| • Külső munkatársak teljes munkaidős egyenértékben (FTE) kifejezve <sup>57</sup>   |                   |                    |          |      |      |
| 09 01 02 01 (AC, END, INT a teljes keretből)                                       | 1                 | 2                  |          |      |      |
| <b>ÖSSZESEN</b>                                                                    |                   | <b>4</b>           | <b>3</b> |      |      |

Az elvégzendő feladatok leírása:

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tisztviselők és ideiglenes alkalmazottak | <p>A Bizottság képviselte az Ügynökség igazgatótanácsában. A Bizottság véleményének kialakítása az ENISA egységes programozási dokumentumáról, és a dokumentum végrehajtásának nyomon követése. Az Ügynökség költségvetése elkészítésének felügyelete, és a költségvetés végrehajtásának figyelemmel kísérése. Az Ügynökség támogatása tevékenységeinek uniós politikákkal megfelelően történő kidolgozásában, a vonatkozó találkozókban való részvételt is ideértve.</p> <p>Az IKT-termékek és -szolgáltatások európai kiberbiztonsági tanúsítási rendszereit átfogó keretrendszer végrehajtásának felügyelete. Kapcsolat fenntartása a tagállamokkal és a többi érdekelt féllel a tanúsítással kapcsolatos törekvésekkel illetően. Együttműködés az ENISA-val a rendszerekre irányuló javaslatok tekintetében. Az európai kiberbiztonsági</p> |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

<sup>57</sup>

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

|                   |                                               |
|-------------------|-----------------------------------------------|
|                   | rendszerekre irányuló javaslatok kidolgozása. |
| Külső munkatársak | Lásd fent                                     |

### 3.2.4. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség

- ☐ A javaslat/kezdeményezés összeegyeztethető a jelenlegi többéves pénzügyi kerettel.
- ☒ A javaslat/kezdeményezés miatt szükséges a többéves pénzügyi keret vonatkozó fejezetének átprogramozása.

A javaslat a 09 02 03-es jogcímcsoport újraprogramozásával jár az ENISA megbízatásának felülvizsgálata miatt, amely új feladatokat ruház az Ügynökségre, többek között a kiberbiztonsági irányelv végrehajtására és az európai kiberbiztonsági tanúsítási keretrendszerre vonatkozóan. Megfelelő összegek:

| Pénzügyi év | Előirányzott | Kérelem |
|-------------|--------------|---------|
| 2019        | 10,739       | 16,550  |
| 2020        | 10,954       | 20,646  |
| 2021        | N.A.         | 22,248* |
| 2022        | N.A.         | 23,023* |

\* Becsült érték. A 2020 utáni időszakra vonatkozó EU-finanszírozás összegének meghatározására a 2020 utánra tervezett összes javaslat figyelembevételével, a Bizottság szintjén folytatandó egyeztetések keretében fog sor kerülni. Ez azt jelenti, hogy a következő többéves pénzügyi keretre vonatkozó javaslatának előterjesztése után a Bizottság – a hatásvizsgálat megállapításainak figyelembevételével – elő fogja terjeszteni e pénzügyi kimutatás módosítását is<sup>58</sup>.

- ☐ A javaslat/kezdeményezés miatt szükség van a rugalmassági eszköz alkalmazására vagy a többéves pénzügyi keret felülvizsgálatára<sup>59</sup>.

### 3.2.5. Harmadik felek részvétele a finanszírozásban

- ☐ A javaslat/kezdeményezés nem irányoz elő harmadik felek általi társfinanszírozást.
- ☒ A javaslat/kezdeményezés az alábbi becsült társfinanszírozást irányozza elő:

<sup>58</sup> A hatásvizsgálatot tartalmazó oldalra mutató hivatkozás.

<sup>59</sup> Lásd a 2014–2020-as időszakra vonatkozó többéves pénzügyi keretről szóló 1311/2013/EU, Euratom tanácsi rendelet 11. és 17. cikkét.

|      | Pénzügyi év<br>2019  | Pénzügyi év<br>2020 | Pénzügyi év<br>2021 | Pénzügyi év<br>2022 |
|------|----------------------|---------------------|---------------------|---------------------|
| EFTA | p.m. <sup>60</sup> . | p.m.                | p.m.                | p.m.                |

### 3.3. A bevételre gyakorolt becsült hatás

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

<sup>60</sup>

A következő évekre előírányzott pontos összeg akkor lesz ismert, ha rögzítik az EFTA arányossági tényezőjét az adott évekre vonatkozóan.