Az Európai Unió
Tanácsa

Brüsszel, 2018. május 29.
(OR. en)

9350/18

Intézményközi referenciaszám:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

FELJEGYZÉS

Küldi:	az elnökség
Címzett:	a Tanács
Előző dok. sz.:	8834/18
Biz. dok. sz.:	12183/17
Tárgy:	Javaslat – AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály”) – Általános megközelítés

I. BEVEZETÉS

1. A Bizottság 2017. szeptember 13-án a digitális egységes piaci stratégiájával összefüggésben elfogadta és továbbította a Tanácsnak és az Európai Parlamentnek a fenti, jogalapként az EUMSZ 114. cikkére épülő javaslatot[1]. A javaslat az ún. „kiberbiztonsági csomag" részét képezi, és mint ilyennek, a célja a magas szintű kiberbiztonság, kiberreziliencia és bizalom megteremtése az Unióban, a belső piac megfelelő működésének a biztosítása céljából.

2. A javasolt rendelet rögzíti az ENISA – az Európai Uniós Kiberbiztonsági Ügynökség – céljait, feladatait és szervezeti felépítésének különböző szempontjait, valamint megteremti az európai kiberbiztonsági tanúsítási rendszerek létrehozásának keretrendszerét az ikt-termékek és -szolgáltatások megfelelő szintű kiberbiztonságának a biztosítása érdekében. A Bizottság javaslatát hatásvizsgálat kíséri, amely nyolc különböző szakpolitikai opciót vizsgál meg az ENISA és az ikt területére vonatkozó kiberbiztonsági tanúsítás felülvizsgálatával kapcsolatban.

3. A javasolt rendelet az alábbi két nagyobb tematikus ágra osztható:

   - egyrészt állandó megbízást biztosít az Ügynökség számára, amelynek hatálya tekintetében az szabja meg a kereteket, hogy milyen szükségleteket kell kielégíteni az új szakpolitikai prioritások és eszközök értelmében, valamint megújított feladat- és funkciómeghatározást is tartalmaz az Ügynökség számára annak érdekében, hogy hatékonyan és eredményesen tudja támogatni a tagállamoknak, az uniós intézményeknek és az egyéb érdekelteknek a biztonságos kibertér kialakítására irányuló erőfeszítéseit;

   - másrészt új európai kiberbiztonsági tanúsítási keretrendszert hoz létre az ikt-termékeket és -szolgáltatásokat illetően, valamint meghatározza az európai kiberbiztonsági tanúsítási rendszerekre vonatkozó szabályokat, melyek alapján biztosított lesz az e rendszerek keretében kiállított tanúsítványok összes tagállamban való érvényessége és elismerése, megoldást kínálva a piacok jelenlegi fragmentáltságára.

[1] 12183/17; 12183/1/17 REV 1; 12183/2/17 REV 2.

4. Az Európai Tanács 2017. októberben felhívta a figyelmet arra[2], hogy a Bizottság kiberbiztonsággal kapcsolatos javaslatait összefüggően kell kidolgozni, megfelelő időben elő kell terjeszteni, és azután késedelem nélkül meg kell vizsgálni a Tanács által kidolgozandó cselekvési terv alapján.

5. Az Általános Ügyek Tanácsa 2017. december 12-én elfogadta az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, az Európai Parlamenthez és a Tanácshoz intézett közös közleményről[3] szóló tanácsi következtetések[4] végrehajtásáról szóló cselekvési tervet[5]. A cselekvési terv a Tanács azon célkitűzését tükrözte, hogy 2018. júniusig létrejöjjön a javaslatra vonatkozó általános megközelítés.

6. Az Európai Parlament Angelika NIEBLER-t (ITRE, EPP) jelölte ki felelős előadóként. Az ITRE bizottság 2018. június 19-én szavaz a jelentéséről.

7. Az Európai Gazdasági és Szociális Bizottság 2018. február 14-én fogadta el véleményét.

II. A TANÁCSBAN FOLYÓ MUNKA

8. A Bizottság 2017. szeptember 26-án nyújtotta be a javaslatot és a hatásvizsgálatot a kiberkérdésekkel foglalkozó horizontális munkacsoportnak (a továbbiakban: a munkacsoport). A munkacsoport 2017. október 20-án tárgyalt a hatásvizsgálatról. Az ezt követően tartott megbeszélések középpontjában az Ügynökség operatív kapacitása és az illetékes nemzeti hatóságokkal való interakciók hatóköre állt, valamint az, hogy milyen hatást gyakorol majd a tanúsítási keretrendszer a piacra és a vállalkozások versenyképességére. Általánosságban mind a hatásvizsgálat, mind a javaslat kedvező fogadtatásra talált a delegációk körében.

---

2 EUCO 14/17, 11. pont.
3 12211/17.
4 14435/17.
5 15748/17.

9. Magának a javaslatnak a munkacsoport keretében való megvitatása 2017. novemberben kezdődött el az észt elnökség ideje alatt, majd folytatódott a bolgár elnökség alatt is. Összesen 12 ülésre került sor a javaslat megtárgyalása céljából, és ezek során nyolc módosított szövegváltozat született azzal a céllal, hogy végül a TTE Tanács (Távközlés) 2018. június 8-i ülésén sor kerüljön az általános megközelítés elfogadására.

10. A munkacsoport 2018. május 14–15-i ülésén folytatott megbeszélés eredményét és az elnökség módosított kompromisszumos szövegét e feljegyzés melléklete tartalmazza. A preambulumbekezdések immár igazodnak a rendelkező rész változásaihoz. A bizottsági javaslathoz képest végrehajtott változtatásokat **félkövér** betűtípus, illetve [...] jelöli. A legutóbbi munkacsoporti dokumentumhoz (8834/18) képest történt változatásokat **félkövér aláhúzott** betűtípus, a törléseket pedig **[...]** jelöli.

III. KONKLÚZIÓ

11. Az elnökségnek a mellékletben foglalt kompromisszumos szövege az elnökség és a tagállamok azon erőfeszítését tükrözi, hogy megteremtsék a megfelelő egyensúlyt a szövegben.

12. Az Állandó Képviselők Bizottsága 2018. május 25-én – a 19. cikk (5) bekezdésének és a 48. cikk (5) bekezdésének a mellékletben látható módosításaival – megállapodásra jutott az elnökségi kompromisszumos szövegről.

13. Ennek megfelelően felkérjük a Tanácsot, hogy 2018. június 8-i ülésén fogadjon el általános megközelítést, és bízza meg az elnökséget azzal, hogy kezdje meg a tárgyalásokat az Európai Parlament és az Európai Bizottság képviselőivel.

MELLÉKLET

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

az ENISA-ról, az „*Európai Uniós 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 tervezetének a nemzeti parlamentek részére való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére[6],

tekintettel a Régiók Bizottságának véleményére[7],

rendes jogalkotási eljárás keretében,

[6] HL C […]., […]., […]. o.
[7] HL C […]., […]., […]. o.

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 a társadalmi tevékenységeket támogató összetett rendszerek alapját képezik, biztosítják a gazdaság olajozott működését olyan meghatározó ágazatokban, mint az egészségügy, az energiaügy, a pénzügy és a közlekedés, valamint mindenekelőtt elősegítik a belső piac működését.

(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 az összekapcsoltság, és a dolgok internetének terjedésével 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 nem rendelkeznek megfelelő biztonsági és rezilienciaszinttel, kiberbiztonsági szempontból nem teljesen megbízhatók. A tanúsítás korlátozott alkalmazása 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.

(3) Minél nagyobb méreteket ölt a digitalizáció és az összekapcsoltság, 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 szükséges intézkedést meg kell hozni azért, hogy a hálózati és információs rendszerek, a távközlési hálózatok, valamint a magánszemélyek, a közigazgatási szervek és a (kkv-ktől a kritikus infrastruktúrák üzemeltetőiig terjedő) vállalkozások 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 válaszintézkedései, akárcsak a bűnüldözési hatáskörök, túlnyomórészt nemzeti szintűek. A nagy kiterjedésű kiberbiztonsági események az egész EU-ban megzavarhatják az alapvető 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 szakpolitikai döntéshozók, a gazdasági élet szereplői és a felhasználók számára egyaránt fontos, hogy megbízható uniós adatok alapján rendszeres értékelés készüljön az EU kiberbiztonságának és kiberrezilienciájának 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 olyan átfogó intézkedéscsomagra van szükség, amely a korábbi uniós fellépésekre épül, és amely előmozdítja az egymást kölcsönösen erősítő célkitűzéseket. Ide tartozik 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, ügynökségek 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, nagy kiterjedésű 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[8], 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 szem előtt tartva – a hálózat- és információbiztonsági kultúra kialakításához. 2008-ban az Európai Parlament és a Tanács az 1007/2008/EK rendelettel[9] az Ügynökség megbízatását 2012 márciusáig meghosszabbította. Az 580/2011/EK rendelet[10] 2013. szeptember 13-ig újfent meghosszabbította az Ügynökség megbízatását. 2013-ban az Európai Parlament és a Tanács elfogadta az ENISA-ról és a 460/2004/EK rendelet hatályon kívül helyezéséről szóló 526/2013/EU rendeletet[11], amely az Ügynökség megbízatásának időtartamát 2020 júniusáig hosszabbította meg.

---

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

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

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

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

(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 keretében 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 energetika, 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 bizonytalanabbá és kevésbé biztonságossá vált globális környezet következtében is. Ennek fényében, illetve az új uniós kiberbiztonsági politika keretében felül kell vizsgálni az ENISA megbízatását a megváltozott kiberbiztonsági ökoszisztémában betöltött szerepének meghatározása és annak biztosítása érdekében, hogy hatékonyan hozzájáruljon a radikálisan új fenyegetettségi helyzetből 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 kiberbiztonsági uniós jogszabályokkal rá ruházott feladatokat kell ellátnia, többek között szakértelem rendelkezésre bocsátása és tanácsadás révén, valamint uniós információs és tudásközpontként működve. Feladata, hogy előmozdítsa a bevált gyakorlatok cseréjét a tagállamok és a magánszektor érdekelt felei között, szakpolitikai javaslatokat tegyen 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 intézmények, ügynökségek 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, valamint az Ügynökség személyzetének tagjait kísérő házastársaknak és gyermekeknek szükséges létesítmények állnak rendelkezésre. 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 **támogatnia kell** [...] a nemzeti **erőfeszítéseket, illetve proaktívan hozzá kell járulnia** az uniós erőfeszítésekhez, és feladatait az uniós intézményekkel, ügynökségekkel és szervekkel, valamint a tagállamokkal teljes körűen együttműködve 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 **– a kiberbiztonsági vonatkozású uniós politikák és jogszabályok relevanciájának növelése és a nemzeti szintű végrehajtás egységességének lehetővé tétele érdekében –** tanácsadással, véleményezéssel és elemzések készítésével kell segítenie a Bizottságot valamennyi olyan uniós kérdésben, amely a kiberbiztonságot [...] **és annak ágazatspecifikus vonatkozásait** érintő szakpolitikák és jogszabályok kidolgozásához, illetve azok aktualizálásához és felülvizsgálatához kapcsolódik. Az Ügynökségnek hivatkozási alapként kell szolgálnia az olyan uniós ágazatspecifikus szakpolitikai és jogalkotási kezdeményezésekkel kapcsolatos tanácsadás és szakértelem terén, 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 kiberreziliencia javításához. Tekintettel a kiberbiztonsági fenyegetettségi helyzet gyorsan változó jellegére, egyértelmű, hogy a tagállamokat több szakpolitikai területet is felölelő, átfogóbb megközelítéssel kell támogatni a kiberreziliencia kialakítása érdekében.

(15) Az Ügynökségnek segítenie kell a tagállamok és az uniós intézmények, ügynökségek és szervek arra irányuló munkáját, hogy kiépítsék, illetve fokozzák a kiber**veszély**[...] és a biztonsági események megelőzésével, észlelésével és az azokra való reagálással kapcsolatos képességeket és felkészültséget, 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 ENISA által a tagállamok operatív képességeivel kapcsolatban végzett tevékenységnek kizárólag arra kell irányulnia, hogy kiegészítse a tagállamok a célból hozott saját intézkedéseit, hogy megfeleljenek a kiberbiztonsági irányelvből eredő kötelezettségeiknek, és nem élvezhet elsőbbséget azokkal szemben** [...].

(15a) Az Ügynökségnek a hálózati és információs rendszerek biztonságára, kiváltképpen a kiberbiztonságra vonatkozó uniós és – kérésre – tagállami stratégiák kidolgozásához és aktualizálásához is hozzá kell járulnia, elő kell segítenie azok terjesztését, és nyomon kell követnie végrehajtásukat. 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 kapacitásuk kifejlesztésében.

(16) Az Ügynökségnek segítenie kell a kiberbiztonsági irányelvvel létrehozott együttműködési csoportot feladatai végrehajtásában, különösen szakértelmével, tanácsadással és a bevált gyakorlatok cseréjének megkönnyítésével, kiváltképpen ami az alapvető szolgáltatásokat nyújtó szereplők tagállamok általi azonosítását illeti, figyelembe véve többek között a biztonsági kockázatok és események terén fennálló, határokon átnyúló függőségeket.

(17) A köz- és a magánszektor közötti, valamint a magánszektoron belüli együttműködés ösztönzése céljából [...] **az Ügynökségnek** támogatnia **kell az ágazatok közötti és azokon belüli információmegosztást, különös tekintettel az (EU) 2016/1148 irányelv II. mellékletében felsorolt ágazatokra, azáltal, hogy bevált gyakorlatokat és iránymutatást kínál a rendelkezésre álló eszközökkel és az eljárásokkal kapcsolatban, továbbá útmutatással szolgál az információk megosztásával kapcsolatos szabályozási kérdésekben, például** előmozdítva az ágazati információmegosztási és elemző központok (ISAC-ok) létrehozását [...].

(18) Az Ügynökségnek összesítenie és elemeznie kell a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) és az európai intézmények, ügynökségek és szervek számítógépes vészhelyzeteket elhárító csoportja (CERT-EU) által készített **és önkéntesen megosztott** nemzeti jelentéseket **annak érdekében, hogy segítse a tagállamokat** az információcsere közös [...] **eljárásainak**, nyelvhasználatának és terminológiájának kialakításában. Munkájába a magánszektort is be kell vonnia a kiberbiztonsági irányelv keretében, amely [...] meghatározta a CSIRT-ek hálózatá**n belüli**, önkéntes alapon történő, operatív szintű technikai információcsere alapjait.

(19) Az Ügynökségnek nagy kiterjedésű, határokon átnyúló kiberbiztonsági esemény vagy válsághelyzet esetén hozzá kell járulnia az uniós szintű reagáláshoz. Ezt a feladatkört **az e rendelet szerinti megbízatásának, valamint a tagállamok által a nagy kiterjedésű kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló bizottsági ajánlás nyomán közösen elfogadandó megközelítésnek megfelelően kell ellátnia. Ide tartozhat** a megfelelő információk összegyűjtése, valamint a CSIRT-ek hálózata 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 információkkal szolgál a nyilvánosság tájékoztatása céljából. Az ilyen jellegű együttműködés módozatainak tesztelésére irányuló [...] **rendszeres** kiberbiztonsági gyakorlatok keretében az Ügynökségnek támogatnia kell ezt a folyamatot.

(20) **Az** operatív [...] **együttműködés támogatása céljából** az Ügynökségnek igénybe kell vennie a CERT-EU keretében rendelkezésre álló **technikai és operatív** szakértelmet, mégpedig [...] strukturált együttműködésen keresztül. [...]Adott esetben a két szervezet között külön megállapodást kell kialakítani az együttműködés gyakorlati megvalósításának meghatározása **és a párhuzamos munkavégzés elkerülése érdekében**.

(21) [...] **A CSIRT-ek hálózatán belüli operatív együttműködés támogatására irányuló** feladatainak megfelelően az Ügynökségnek képesnek kell lennie arra, hogy a tagállamokat **azok kérésére** támogassa, például tanácsot adjon **a biztonsági események megelőzésére, észlelésére és az azokra való reagálásra irányuló képességeik javításának lehetséges módjairól, megkönnyítse a jelentős vagy lényeges hatású biztonsági események** [...] technikai **kezelését** [...], illetve gondoskod**jon** a fenyegetések és biztonsági események elemzésének elkészítéséről. **A jelentős vagy lényeges hatású biztonsági események technikai kezelése megkönnyítésének feladatába bele kell tartoznia különösen annak, hogy az ENISA támogatja a technikai megoldások tagállamok közötti önkéntes megosztását, vagy összefoglaló jellegű technikai információkat állít elő például a tagállamok által önkéntesen megosztott technikai megoldásokról.** A Bizottság a nagy kiterjedésű 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 nagy kiterjedésű kiberbiztonsági eseményekkel és válsághelyzetekkel kapcsolatos információkat. Ezek az információk az ENISA segítségére lesznek [...] **az operatív együttműködés támogatása során**.

(22) Az uniós helyzetismeret támogatását célzó, rendes technikai szintű együttműködés részeként az Ügynökségnek **– a tagállamokkal szoros együttműködésben –** 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 [...] vagy a kiberbiztonsági irányelvvel létrehozott egyedüli kapcsolattartó pontok **(mindkettő önkéntes alapon)**, 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) vele megosztottak. A helyzetjelentést az érintett tanácsi és bizottsági szervek, az Unió külügyi és biztonságpolitikai főképviselője és a CSIRT-ek hálózata rendelkezésére kell bocsátani.

(23) A [...] jelentős hatású biztonsági eseményekre vonatkozóan [...] az **érintett** tagállamok [...] kérésére elvégzett utólagos technikai vizsgálatok**hoz az Ügynökség által nyújtott támogatásnak** a jövőbeli események megelőzésére kell összpontosítania [...]. **Az érintett tagállamoknak meg kell adniuk az ahhoz szükséges információkat, hogy az Ügynökség hatékony támogatást tudjon nyújtani a technikai vizsgálathoz.**

(24) [...]

(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 megismerése érdekében, valamint a tagállamoknak és az uniós intézményeknek nyújtandó hosszú távú stratégiai tanácsadás céljából az Ügynökségnek elemeznie kell mind a már ismert, mind az újonnan fellépő kockázatokat. E célból az Ügynökségnek a tagállamokkal és adott esetben a statisztikai hivatalokkal és más szervekkel együttműködésben össze kell gyűjtenie a **nyilvánosan elérhető és önkéntesen megosztott** releváns információkat, elemzéseket kell készítenie a kialakulóban lévő 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, ügynökségeket és szerveket az új tendenciák azonosításában és a kiberbiztonsági [...] **események** megelőzésében.

(27) Az Ügynökségnek – az Unió ellenálló képességének növelése érdekében – tanácsadással, iránymutatással és a bevált módszerek terjesztésével kiválóságra kell törekednie [...] **azon infrastruktúrák kiber**biztonságának témájában**, amelyek különösen a kiberbiztonsági irányelv II. mellékletében felsorolt ágazatokat támogatják, valamint amelyeket az ugyanazon irányelv III. mellékletében felsorolt digitális szolgáltatások nyújtói használnak**. 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, **ügynökségekkel és** szervekkel [...]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)**, az Európai GNSS Ügynökséggel (GNSS Ügynökség)** és a kiberbiztonságban érintett minden más uniós ügynökséggel. Kapcsolatot kell fenntartania továbbá az adatvédelmi hatóságokkal is a know-how és a bevált módszerek cseréje érdekében, valamint hogy tanácsot adjon a kiberbiztonság azon vonatkozásaival kapcsolatban, amelyek hatással lehetnek e hatóságok munkájára. A nemzeti és uniós bűnüldöző és adatvédelmi hatóságok képviselőinek lehetőséget kell biztosítani arra, hogy képviseltessék magukat az Ügynökséghez tartozó érdekeltek állandó csoportjában. Az Ügynökségnek a bűnüldözési szervekkel folytatott, a munkájukra esetlegesen hatást gyakorló hálózat- és információbiztonsági kérdésekkel kapcsolatos együttműködés során tiszteletben kell tartania a meglévő információs csatornákat és a létező hálózatokat.

(31) Az Ügynökségnek [...] a CSIRT-ek hálózatának titkársága **szerepében** támogatnia kell a tagállami CSIRT-ek és a CERT-EU operatív együttműködését, a CSIRT-ek hálózatának 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-ek hálózatának eljárási standardjait.

(32) A kiberbiztonsági eseményekre való reagálással kapcsolatos uniós felkészültség javítása érdekében az Ügynökségnek [...]**rendszeresen** kiberbiztonsági gyakorlatokat kell szerveznie uniós szinten, és, amennyiben erre igény van, támogatnia kell a tagállamokat és az uniós intézményeket, hivatalokat és szerveket ilyen gyakorlatok megszervezésében.

(33) Az Ügynökségnek a kiberbiztonsági tanúsítás terén kialakított szakértelmét tovább kell fejlesztenie és fenn kell tartania az arra vonatkozó 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 – a kellően kidolgozott kockázatértékelési módszereken kell alapulniuk. A kockázatértékelési módszereket különböző szinteken használják, és eredményes alkalmazásukat illetően nincs közös gyakorlat. A kockázatértékeléssel és az interoperábilis kockázatkezelési megoldásokkal kapcsolatban bevált módszereknek a köz- és a magánszektorbeli szervezetekben való ösztönzése, illetve kialakítása fokozni fogja az Unió kiberbiztonságát. E célból az Ügynökségnek uniós szinten támogatnia kell az érdekeltek együttműködését, azáltal, hogy előmozdítja az európai és nemzetközi szabványok kidolgozására és alkalmazására irányuló erőfeszítéseket egyfelől a kockázatkezeléssel, másfelől azon elektronikus termékek, rendszerek, hálózatok és szolgáltatások mérhető biztonságával kapcsolatban, amelyek a szoftverekkel együtt a hálózati és információs rendszereket alkotják.

(35) Az Ügynökségnek ösztönöznie kell a tagállamokat és a szolgáltatókat általános biztonsági előírásaik szigorítására, 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 – ezen belül kiberbiztonságának – a fokozására 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, **ügynökségek és** szervek [...], valamint adott esetben a tagállamok számára a [...] kiberbiztonság területét érintő kutatási igényekkel kapcsolatban. **A kutatási igények és prioritások meghatározása érdekében az Ügynökségnek konzultálnia kell az érintett felhasználói csoportokkal is.**

(37) A kiberbiztonsági [...]**fenyegetések** globális kérdést jelentenek. Szorosabb nemzetközi együttműködésre van szükség a **kiber**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 az 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, **ügynökségek és** szervek [...] 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 el kell készítenie az igazgatótanácshoz benyújtandó éves jelentést**, amely kiterjed az Ügynökség éves munkaprogramjának végrehajtására is**, 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 érdekeltekkel 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 összeférhetetlenségek megelőzésére és kezelésére. Alkalmaznia kell továbbá a dokumentumokhoz való nyilvános hozzáférésről szóló 1049/2001/EK európai parlamenti és tanácsi rendeletben[12] 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[13] 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.

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

[13] HL L 8., 2001.1.12., 1. o.

(46) Teljes mértékű autonómiájának és függetlenségének biztosítása érdekében, valamint hogy további és új feladatokat, többek között váratlan, sürgős feladatokat is teljesíteni tudjon, az Ügynökség számára elégséges és önálló költségvetést kell biztosítani, melynek bevételei elsősorban az Unió hozzájárulásából és az Ügynökség munkájában részt vevő harmadik országok hozzájárulásából származnak. Személyzete többségének közvetlenül az 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) [...]

(48) A kiberbiztonsági tanúsítás fontos szerepet játszik az ikt-termékek és -szolgáltatások iránti bizalomnak és azok biztonságosságának növelésében. A digitális egységes piac és különösen az adatgazdaság és a dolgok internete csak akkor lehet sikeres, ha a polgárok általában véve bízhatnak abban, hogy az ilyen termékek és szolgáltatások kiberbiztonsági megbízhatósága elér egy meghatározott szintet. A hálózatba kapcsolt és automatizált járművek, az elektronikus orvostechnikai 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 interoperábilis kiberbiztonsági termékekre és megoldásokra van szükség. Az ikt-termékek és -szolgáltatások kínálata az egységes piacon földrajzilag még mindig igen széttagolt. 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 interoperábilis 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 csökkenti a magánfelhasználók és a vállalkozások számára hozzáférhető, működőképes és használható kiberbiztonsági technológiák kínálatát. A digitális egységes piaci stratégia végrehajtásának félidős 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 széttagoltságára.

(50) Jelenleg az ikt-**folyamatok,** -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. Ennek fényében, ha egy nemzeti kiberbiztonsági hatóság tanúsítványt bocsát ki, azt a többi tagállam alapvetően nem ismeri el. Lehetséges ezért, hogy a vállalatoknak – 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 – nem látszik egységes és holisztikus megközelítés kirajzolódni. A meglévő rendszerek jelentős hiányosságokat és különbségeket mutatnak a lefedett termékek köre, a megbízhatósági szintek, az alapvető kritériumok és a gyakorlati felhasználás tekintetében.

(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 modell az együttműködésre és a kölcsönös elismerésre, [...], az SOG-IS csoportban csak az uniós tagállamok egy része vesz részt. 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 követelményeknek kell megfelelniük a kidolgozandó európai kiberbiztonsági tanúsítási rendszereknek, és lehetővé teszi az ikt-termékek és -szolgáltatások tanúsítványainak**, valamint EU-megfelelőségi nyilatkozatainak** 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 segítenie kell elkerülni, hogy egymásnak ellentmondó vagy egymást átfedő nemzeti kiberbiztonsági tanúsítványok létezzenek, csökkentve ezzel a digitális egységes piacon működő vállalkozások költségeit. A rendszereknek megkülönböztetésmenteseknek kell lenniük, és nemzetközi és/vagy [...]**európai** szabványokon kell alapulniuk, kivéve, ha ezek a szabványok nem hatékonyak vagy nem alkalmasak az EU e tekintetben kitűzött jogos céljainak teljesítésére.

(53) A Bizottságot fel kell hatalmazni arra, hogy európai kiberbiztonsági tanúsítási rendszereket fogadjon el az ikt**-folyamatok,** -termékek és -szolgáltatások meghatározott csoportjaira vonatkozóan. Ezeket a rendszereket a nemzeti **kiberbiztonsági** tanúsító [...] 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 esetében nem indokolt, hogy a rendelet hatálya alá tartozzanak. Az ilyen rendszereket működtető szervezetek azonban javasolhatják a Bizottságnak annak mérlegelését, hogy saját rendszereik alapul vehetők-e európai rendszerként való jóváhagyás céljából.

(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. Ez a rendelet nem érinti az adatkezelési műveletek általános adatvédelmi rendelet szerinti tanúsítását, még akkor sem, ha az ilyen műveletek termékekbe és szolgáltatásokba vannak beágyazva.

(55) Az európai kiberbiztonsági tanúsítási rendszerek rendeltetése annak biztosítása, hogy az ilyen rendszerek keretében tanúsított ikt**-folyamatok,** -termékek és -szolgáltatások megfeleljenek a meghatározott követelményeknek [...] **abból a célból,** hogy [...] **védjék** az e rendelet szerinti termékek, eljárások, szolgáltatások és rendszerek által tárolt vagy továbbított vagy kezelt adatok, illetve az említett termékek, eljárások, szolgáltatások és rendszerek által biztosított vagy elérhetővé tett kapcsolódó funkciók vagy szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét és titkosságát **azok teljes életciklusa alatt**. Lehetetlen ebben a rendeletben az összes ikt**-folyamat,** -termék és -szolgáltatás vonatkozásában részletesen meghatározni a kiberbiztonsági követelményeket. Az ikt**-folyamatok,** -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. Azt, hogy ezeket a célkitűzéseket egyes ikt**-folyamatok,** -termékek és -szolgáltatások esetében hogyan kell elérni, részleteiben a Bizottság által elfogadott egyedi tanúsítási rendszerek szintjén kell meghatározni, például szabványokra vagy műszaki előírásokra való hivatkozás révén **olyan esetekben, ahol nem áll rendelkezésre megfelelő szabvány**.

(55a) Az európai kiberbiztonsági tanúsítási rendszerek keretében alkalmazandó műszaki előírásokat az 1025/2012/EU rendelet II. mellékletében rögzített elvek szerint kell meghatározni. Kellően indokolt esetekben azonban, amikor a műszaki előírások olyan európai kiberbiztonsági tanúsítási rendszer keretében alkalmazandók, amely „magas" megbízhatósági szintre vonatkozik, szükségessé válhat az ezen elvektől való kis mértékű eltérés. Az ilyen eltérés indokait nyilvánossá kell tenni.

(55b) A tanúsított megfelelőségértékelés olyan eljárás, amelynek során értékelik, hogy egy adott ikt-eljárás, -termék vagy -szolgáltatás megfelel-e az előírt követelményeknek. Ezt az eljárást egy független harmadik fél folytatja le, aki nem egyezhet meg a termék gyártójával vagy a szolgáltatóval. Tanúsítványt az ikt-folyamat, -termék vagy -szolgáltatás sikeres értékelésének folyamatát követően lehet kiállítani. A tanúsítvány igazolásnak tekintendő arra nézve, hogy a vonatkozó értékelést előírásszerűen elvégezték. Az európai kiberbiztonsági rendszerben elő kell írni, hogy a megbízhatósági szinttől függően magánjogi vagy közjogi szerv állítja-e ki a tanúsítványt. A megfelelőségértékelés és a tanúsítás önmagában nem garantálja, hogy a tanúsított ikt-termékek és -szolgáltatások kiberbiztonsági szempontból megbízhatóak. 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 műszaki szabványokban meghatározott – kiberbiztonsági követelményeknek.

(55c) A tanúsítvány felhasználójának az adott ikt-folyamat, -termék vagy -szolgáltatás használatának kockázatelemzése alapján kell megválasztania a tanúsításnak és az ahhoz kapcsolódó biztonsági követelményeknek a megfelelő szintjét. A megbízhatósági szintnek tehát arányban kell állnia az adott ikt-folyamat, -termék vagy -szolgáltatás rendeltetés szerinti használatához fűződő kockázat szintjével.

(55d) Az európai kiberbiztonsági tanúsítási rendszerek keretében lehetővé lehetne tenni, hogy a megfelelőségértékelésre az ikt-termékek, illetve -szolgáltatások gyártójának, illetve nyújtójának kizárólagos felelőssége mellett kerüljön sor (megfelelőségi önértékelés). Ilyen esetekben elegendő, ha a gyártó, illetve szolgáltató maga végzi el az összes ahhoz szükséges vizsgálatot, hogy az adott ikt-folyamat, -termék vagy -szolgáltatás megfeleljen a tanúsítási rendszer követelményeinek. Az ilyen típusú megfelelőségértékelés az olyan, kevésbé összetett ikt-termékek és szolgáltatások esetében tekinthető megfelelőnek, amelyek alacsony kockázatot jelentenek a közérdekre nézve. Ezenkívül, kizárólag az „alacsony" megbízhatósági szintnek megfelelő ikt-termékek és szolgáltatások esetében alkalmazható a megfelelőségi önértékelés .

(55e) Az európai kiberbiztonsági tanúsítási rendszerek keretében lehetővé lehetne tenni az ikt-termékeknek és -szolgáltatásoknak mind a tanúsítását, mind e termékekre, illetve szolgáltatásokra vonatkozóan megfelelőségi önértékelés végzését. Ebben az esetben a rendszernek világos, közérthető módszerekkel kell szolgálnia a célból, hogy a fogyasztók vagy más felhasználók különbséget tudjanak tenni az olyan termékek és szolgáltatások között, amelyeket a gyártó vagy a szolgáltató felelősségi körében értékeltek, illetve amelyeket harmadik fél tanúsított.

(55f) Az ikt-termékek és szolgáltatások azon gyártójának, illetve szolgáltatójának, aki megfelelőségi önértékelést végez, a megfelelőségértékelési eljárás részeként uniós megfelelőségi nyilatkozatot kell készítenie, és azt alá kell írnia. Az uniós megfelelőségi nyilatkozat olyan dokumentum, amely egy adott ikt-terméket vagy -szolgáltatást a tanúsítási rendszerben előírt követelményeknek megfelelőnek minősít. Az uniós megfelelőségi nyilatkozat elkészítésével és aláírásával a gyártó vagy szolgáltató felelősséget vállal azért, hogy az adott ikt-termék vagy -szolgáltatás megfelel a tanúsítási rendszerben előírt jogi követelményeknek. Az uniós megfelelőségi nyilatkozat egy-egy példányát meg kell küldeni a nemzeti kiberbiztonsági tanúsító hatóságnak és az ENISA-nak.

(55g) Az ikt-termékek és -szolgáltatások gyártójának, illetve nyújtójának gondoskodnia kell arról, hogy az alkalmazandó európai kiberbiztonsági tanúsítási rendszerben meghatározott ideig az illetékes nemzeti kiberbiztonsági tanúsító hatóság rendelkezésére álljon mind az uniós megfelelőségi nyilatkozat, mind az ikt-termékek, illetve -szolgáltatások tanúsítási rendszernek való megfelelésével kapcsolatos összes releváns információt tartalmazó műszaki dokumentáció. A műszaki dokumentációnak tartalmaznia kell az alkalmazandó követelményeket, és – az értékelés szempontjából szükséges mértékben – ismertetnie kell az adott ikt-termék, illetve -szolgáltatás tervét, gyártását és működését. A műszaki dokumentációt úgy kell összeállítani, hogy az alapján értékelni lehessen, hogy az adott ikt-termék vagy -szolgáltatás megfelel-e a vonatkozó követelményeknek.

(55h) A tagállamokat és az érintett érdekelt szervezeteket fel kell jogosítani arra, hogy az európai kiberbiztonsági tanúsítási csoporthoz forduljanak egy javasolt rendszer kidolgozása érdekében. Érintett érdekelt szervezetnek minősülnek az ágazatot vagy a fogyasztókat képviselő szervezetek, ideértve az olyan kkv-k érdekképviseleti szervezeteit is, amelyeknek jogos érdeke fűződik egy adott európai kiberbiztonsági tanúsítási rendszer kidolgozásához. Az európai kiberbiztonsági tanúsítási csoportnak az általa meghatározott kritériumok alapján, az átláthatóság, nyitottság, pártatlanság, konszenzus, eredményesség, relevancia és koherencia elvein nyugvó iránymutatásoknak megfelelően kell megvizsgálnia e javaslatokat.

(56) A Bizottságot **és a csoportot** fel kell hatalmazni arra, hogy felkérhesse az ENISA-t meghatározott ikt-**folyamatokra,** -termékekre vagy -szolgáltatásokra vonatkozó javasolt rendszerek **indokolatlan késedelem nélküli** 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 e rendelet általános céljára és a benne megállapított biztonsági célkitűzésekre, a Bizottság által elfogadott európai kiberbiztonsági tanúsítási rendszereknek bizonyos elemeket legalább meg kell határozniuk az egyes rendszerek tárgya, alkalmazási köre és működése vonatkozásában. Ezeknek többek között a következőkre kell kiterjedniük: a kiberbiztonsági tanúsítás hatálya és tárgya, ideértve a hatálya alá tartozó ikt-**folyamatok,** -termékek és -szolgáltatások kategóriáit, a kiberbiztonsági követelmények részletes leírását, például szabványokra vagy műszaki előírásokra való hivatkozások révén, az egyedi értékelési kritériumokat és értékelési módszereket, a rendeltetés szerinti megbízhatósági szintet (alacsony, közepes és/vagy magas)**, valamint adott esetben az értékelési szinteket**.

(56a) Az európai tanúsítási rendszerek megbízhatósága alapozza meg a bizalmat az iránt, hogy valamely ikt-folyamat, -termék vagy -szolgáltatás teljesíti egy adott európai kiberbiztonsági tanúsítási rendszer biztonsági követelményeit. A tanúsított ikt-folyamatokra, -termékekre és -szolgáltatásokra vonatkozó keretrendszer következetessége érdekében az európai kiberbiztonsági tanúsítási rendszerek meghatározhatnák az adott rendszer szerint kibocsátott európai kiberbiztonsági tanúsítványokban és uniós megfelelőségi nyilatkozatokban feltüntetendő megbízhatósági szinteket. A tanúsítványokban az „alacsony”, „közepes” vagy „magas” megbízhatósági szintek egyike szerepelhetne, míg az uniós megfelelőségi nyilatkozat csak az „alacsony” megbízhatósági szintre utalhatna. A megbízhatósági szintekkel összhangban áll az értékelés érdekében tett erőfeszítés szintje [...], és leírása az adott szinttel kapcsolatos műszaki előírásokra, szabványokra és eljárásokra, többek között a műszaki ellenőrzésekre való hivatkozással történik, melyek rendeltetése a kiberbiztonsági események hatásainak mérséklése, illetve azok megelőzése. Az egyes megbízhatósági szinteket a tanúsítást alkalmazó különböző ágazati területek között következetesen kell alkalmazni.

(56b) Az európai kiberbiztonsági tanúsítási rendszerekben az alkalmazott értékelési módszertan szigorúságától és mélységétől függően több értékelési szint is meghatározható, melyek mindegyike meg kell, hogy feleljen egy-egy megbízhatósági szintnek, és melyek mindegyikéhez társítani kell a megbízhatósági komponensek egy bizonyos, megfelelő kombinációját. Minden megbízhatósági szint esetében meg kell határozni, hogy az ikt-termékek vagy -szolgáltatások a tanúsítási rendszer szerint meghatározott mely biztonságos funkciókkal kell, hogy rendelkezzenek: ilyen lehet például az alapértelmezésben biztonságos konfiguráció, az aláírt kód, a biztonságos frissítés, a sebezhetőségek kihasználhatóságának csökkentése, valamint a veremmemória/halommemória teljes körű védelme. Ezeket a funkciókat biztonságorientált fejlesztési megközelítésmódot, illetve társított eszközöket alkalmazva kell kifejleszteni, illetve fenntartani annak érdekében, hogy (mind a szoftver, mind a hardver szintjén) hatékony mechanizmusok kerüljenek beépítésre, megbízható módon. Az „alacsony" megbízhatósági szint esetében az értékelésnek legalább a következő megbízhatósági elemeken kell nyugodnia: az ikt-termék vagy -szolgáltatás műszaki dokumentációjának a megfelelőségértékelő szervezet általi áttekintése. Amennyiben a tanúsítás ikt-folyamatokra is kiterjed, az ikt-termék vagy -szolgáltatás tervezésére, fejlesztésére és karbantartására szolgáló folyamatot is műszaki felülvizsgálatnak kell alávetni. Azokban az esetekben, amikor egy európai kiberbiztonsági tanúsítási rendszer megfelelőségi önértékelést ír elő, elegendőnek kell tekinteni, ha a gyártó vagy a szolgáltató elvégezte az ikt-folyamatnak, -termékeknek vagy -szolgáltatásoknak a tanúsítási rendszer követelményeinek való megfelelésére vonatkozó önértékelést. A „közepes" megbízhatósági szint esetében az értékelésnek – az „alacsony" megbízhatósági szintnél leírtakon felül – legalább annak ellenőrzésén kell nyugodnia, hogy az ikt-termék vagy -szolgáltatás biztonsági funkciói megfelelnek-e a műszaki dokumentációnak. A „magas" megbízhatósági szint esetében az értékelésnek – a „közepes" megbízhatósági szintnél leírtakon felül – legalább egy olyan hatékonysági teszten kell nyugodnia, amely felméri, hogy az ikt-termék vagy -szolgáltatás biztonsági funkciói ellenállóak-e a jelentős szakértelemmel és erőforrásokkal rendelkező elkövetők által végrehajtott kifinomult kibertámadásokkal szemben.

(56c) Az ENISA-nak a javasolt rendszerek kidolgozása során célszerű konzultálnia minden érdekelt féllel, így például az európai szabványügyi szervezetekkel, az érintett nemzeti hatóságokkal, a kölcsönös elismerési megállapodásokon alapuló szervezetekkel (mint például az SOG-IS MRA), a kkv-kkal, a fogyasztói szervezetekkel, valamint a környezetvédelmi és társadalmi érdekvédő szervezetekkel.

(56d) Az ENISA-nak honlapot kell fenntartania, amelyen tájékoztatást kell nyújtania az európai kiberbiztonsági tanúsítási rendszerekről, illetve népszerűsítenie kell azokat, és a honlapon szerepelniük kell többek között a javasolt európai kiberbiztonsági tanúsítási rendszerek kidolgozása iránti kérelmeknek, valamint a kidolgozási szakaszban az ENISA által folytatott konzultációk során kapott visszajelzéseknek is. A honlapon az e rendelet szerint kiadott tanúsítványokról és uniós megfelelőségi nyilatkozatokról is tájékoztatást kell nyújtani.

(57) Az európai kiberbiztonsági tanúsítás **és az uniós megfelelőségi nyilatkozat** igénybevételének továbbra is önkéntes alapon kell történnie, kivéve ha uniós jogszabályok **vagy az uniós joggal összhangban elfogadott** nemzeti jogszabályok ettől eltérően rendelkeznek. **Harmonizált jogi szabályozás hiányában a tagállamok elfogadhatnak olyan, az (EU) 2015/1535 irányelvnek megfelelő nemzeti műszaki szabályokat, amelyekben előírják a valamely európai kiberbiztonsági tanúsítási rendszer szerinti kötelező tanúsítást. A tagállamok a közbeszerzésekkel és a 2014/24/EU irányelvvel összefüggésben is igénybe vehetik az európai kiberbiztonsági tanúsítást.**[...]

(57a) E rendelet céljainak elérése és a belső piac széttagoltságának elkerülése érdekében az európai kiberbiztonsági tanúsítási rendszer hatálya alá tartozó ikt-termékekre és -szolgáltatásokra vonatkozó nemzeti kiberbiztonsági tanúsítási rendszerek és eljárások a Bizottság által végrehajtási jogi aktusban meghatározott időponttól kezdve nem keletkeztethetnek joghatást. Emellett a tagállamok nem vezethetnek be olyan új nemzeti tanúsítási rendszereket, amelyek már valamely meglévő európai kiberbiztonsági tanúsítási rendszer hatálya alá tartozó ikt-termékek és -szolgáltatások tekintetében szolgálnak kiberbiztonsági tanúsítási rendszerként. A tagállamokat ugyanakkor semmi nem akadályozhatja abban, hogy nemzetbiztonsági célokra nemzeti tanúsítási rendszert vezessenek be vagy tartsanak fenn.

(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 szólhat, és azonos feltételek mellett megújítható, feltéve hogy az adott megfelelőségértékelő szervezet teljesíti a követelményeket. Az akkreditáló testületeknek **korlátozniuk kell, fel kell függeszteniük vagy** 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) [...]A tagállamoknak [...] ki **kell** jelölniük egy **vagy több** kiberbiztonsági tanúsító [...] hatóságot, amely(ek) felügyeli(k) [...] **az e rendeletből eredő követelményeknek** való megfelelést. **Ha valamely tagállam megfelelőnek ítéli, erre a feladatra már meglévő hatóságokat is kijelölhet. A tagállamok számára lehetővé kell tenni továbbá, hogy egy másik tagállammal kötött kölcsönös megállapodás alapján egy vagy több, az adott másik tagállam területén működő felügyeleti hatóságot jelöljenek ki. A hatóság feladata különösen, hogy nyomon kövesse és betartassa az ikt-termékek és -szolgáltatások területükön letelepedett gyártóinak, illetve -nyújtóinak az uniós megfelelőségi nyilatkozathoz kapcsolódó kötelezettségeit, segítse – szakértelmével és megfelelő információkkal – a nemzeti akkreditáló szervezeteket a megfelelőségértékelő szervezetek tevékenységeinek nyomon követésében és felügyeletében, engedélyezze a megfelelőségértékelő szervezeteknek, hogy ellássák a hatóság feladatait, amennyiben teljesítik a valamely rendszerben meghatározott kiegészítő követelményeket, továbbá figyelemmel kísérje a kiberbiztonsági tanúsítás területén zajló releváns fejleményeket** [...]. A nemzeti **kiberbiztonsági** tanúsító [...] hatóságok feladata, hogy kezeljék [...] **az általuk vagy** a megfelelőségértékelő szervezetek által kiadott**, „magas" megbízhatósági szintre vonatkozó** tanúsítványokkal kapcsolatban természetes vagy jogi személyek által 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 **kiberbiztonsági** tanúsító[...] 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 kiberbiztonsági rendszerek követelményeinek.

(60) Az európai kiberbiztonsági tanúsítási keretrendszer következetes alkalmazása érdekében létre kell hozni a nemzeti **kiberbiztonsági** tanúsító[...] hatóságok **vagy egyéb megfelelő nemzeti hatóságok képviselőiből** 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 Ügynökséget és szorosan együttműködjön vele a javasolt kiberbiztonsági tanúsítási rendszerek kidolgozásában; ajánlásokat fogalmazzon meg arra vonatkozóan, hogy a Bizottság kérje fel az Ügynökséget a javasolt európai kiberbiztonsági tanúsítási rendszerek kidolgozására; valamint fogadjon el **az Ügynökségnek címzett véleményeket a javasolt rendszerekről, illetve a** Bizottságnak címzett véleményeket a meglévő európai kiberbiztonsági tanúsítási rendszerek fenntartásával és felülvizsgálatával kapcsolatban.

(60a) A csoportnak elő kell segítenie a bevált gyakorlatok és a szakismeretek cseréjét a megfelelőségértékelő szervezetek engedélyezéséért és a tanúsítványok kiadásáért felelős nemzeti kiberbiztonsági tanúsító hatóságok között. A csoportnak – a javasolt rendszerek kidolgozása tekintetében – támogatást kell nyújtania a „magas" megbízhatósági szintre vonatkozó európai kiberbiztonsági tanúsítványt kiadó szervezetek között alkalmazandó kölcsönös felülvizsgálati mechanizmus kialakításához. A kölcsönös felülvizsgálat során elsősorban azt kell értékelni, hogy az érintett szervezetek rendelkeznek-e a kellő szakértelemmel, és harmonizált módon végzik-e feladataikat. A kölcsönös felülvizsgálat eredményét nyilvánosan hozzáférhetővé kell tenni. Az említett szervek intézkedéseket hozhatnak annak érdekében, hogy kiigazítsák gyakorlataikat és szakismereteiket.

(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 gyakorlatokról vagy a felelős kiberbiztonsági magatartásról, kiemelve a tanúsított ikt-termékek és -szolgáltatások használatának kedvező hatását.

(61a) A kereskedelem további megkönnyítése érdekében, továbbá tudatában az ikt-ellátási láncok globális dimenziójának, az Unió az EUMSZ 218. cikkével összhangban kölcsönös elismerési megállapodásokat köthet az európai kiberbiztonsági tanúsítási keretrendszer szerint létrehozott rendszerek által kiadott tanúsítványokra vonatkozóan. A Bizottság az ENISA és az európai kiberbiztonsági tanúsítási csoport tanácsának figyelembevételével ajánlást tehet ilyen irányú tárgyalások megkezdésére. Minden egyes rendszeren belül egyedi feltételeket kell meghatározni a harmadik országok viszonylatában alkalmazandó kölcsönös elismerésre vonatkozóan.

(62) [...]

(63) [...]

(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, az Ügynökség általi **vizsgálatlefolytatás** módszereire, valamint arra vonatkoznak, hogy a nemzeti **kiberbiztonsági** tanúsító [...] hatóságok milyen körülmények esetén, 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 ezért azok uniós szinten jobban megvalósíthatók, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritási elvnek megfelelően. Az említett cikkben foglalt arányossági elvnek megfelelően ez a rendelet nem lépi túl a e célok eléréséhez szükséges mértéket,

ELFOGADTA EZT A RENDELETET:

I. CÍM
ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy és hatály

(1) A belső piac megfelelő működésének biztosítása és ezzel egyidejűleg az Unión belül a kiberbiztonság, a kiberreziliencia és a kiberbiztonságba vetett bizalom magas szintjének elérése érdekében e rendelet:

a) megállapítja az ENISA, az „Európai Uniós Kiberbiztonsági Ügynökség” (a továbbiakban: az Ügynökség) célkitűzéseit, feladatait és szervezeti felépítését; valamint

b) meghatározza az európai kiberbiztonsági tanúsítási rendszerek létrehozásának keretrendszerét annak érdekében, hogy az Unión belül biztosítsa az ikt-**folyamatok,** -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) **Ez a rendelet nem sérti a kiberbiztonsággal kapcsolatos tagállami hatásköröket, továbbá semmilyen esetben sem sérti a közbiztonsággal, a honvédelemmel és a nemzetbiztonsággal kapcsolatos tevékenységeket, valamint az államnak a büntetőjog egyes területein folytatott tevékenységeit.**

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”: bármely, az (EU) 2016/1148 irányelv 4. cikkének 6. pontjában szereplő fogalommeghatározás szerinti olyan jogi személy, amely digitális szolgáltatást nyújt;

6. „biztonsági esemény”: bármely, az (EU) 2016/1148 irányelv 4. cikkének 7. pontjában szereplő fogalommeghatározás szerinti esemény;

7. „biztonsági esemény kezelése”: bármely, az (EU) 2016/1148 irányelv 4. cikkének 8. pontjában szereplő fogalommeghatározás szerinti eljárás;

8. „kiberfenyegetés”: bármely olyan lehetséges körülmény vagy esemény, amely **károsíthatja vagy megzavarhatja** a hálózati és információs rendszereket, azok felhasználóit és az érintett személyeket, **vagy egyéb** kedvezőtlen hatást gyakorolhat rájuk;

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) **folyamatok,** termékek és szolgáltatások tanúsítására **vagy megfelelőségértékelésére** vonatkoznak;

9a. „nemzeti kiberbiztonsági tanúsítási rendszer”: valamely nemzeti hatóság által kidolgozott és elfogadott átfogó szabályok, műszaki követelmények, szabványok és eljárások összessége, melyek az adott tanúsítási rendszer hatálya alá tartozó ikt-folyamatok, -termékek és -szolgáltatások tanúsítására vagy megfelelőségértékelésére vonatkoznak;

10. „európai kiberbiztonsági tanúsítvány”: olyan dokumentum, [...] amely tanúsítja, hogy egy adott ikt-**folyamat,** -termék vagy -szolgáltatás [...] esetében **értékelték azt, hogy megfelel-e** valamely európai kiberbiztonsági tanúsítási rendszer szerinti specifikus **biztonsági** követelményeknek;

11. „ikt-termék [...]”: a hálózati és információs rendszerek bármely eleme vagy elemeinek csoportja;

11a. „ikt-szolgáltatás”: bármely olyan szolgáltatás, amely teljes mértékben vagy legnagyobb részben információ hálózati és információs rendszerek felhasználásával történő továbbításából, tárolásából, lekérdezéséből vagy kezeléséből áll;

11b. „ikt-eljárás”: valamely ikt-termék vagy -szolgáltatás tervezése, fejlesztése, szállítása vagy nyújtása és karbantartása céljából végzett tevékenységek összessége;

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 szerinti szabvány**;**

16a. „műszaki előírás”: olyan dokumentum, amely megszabja, hogy az ikt-folyamatoknak, termékeknek vagy szolgáltatásoknak milyen műszaki követelményeket kell teljesíteniük;

16b. „megbízhatósági szint”: amire alapozva bízni lehet abban, hogy valamely ikt-folyamat, -termék vagy -szolgáltatás teljesíti egy adott európai kiberbiztonsági tanúsítási rendszernek a biztonsági követelményeit, és feltünteti, hogy az értékelést milyen szinten végezték el; a megbízhatósági szint nem méri maguknak az ikt-folyamatoknak, -termékeknek vagy -szolgáltatásoknak a biztonságát.

II. CÍM

ENISA – „*Európai Uniós Kiberbiztonsági Ügynökség*”

I. FEJEZET

MEGBÍZATÁS ÉS CÉLKITŰZÉSEK */.../*

3. cikk

Megbízatás

(1) Az Ügynökségnek el kell végeznie az e rendelet által ráruházott feladatokat, ezzel hozzájárulva a magas szintű kiberbiztonsághoz [...] **az egész** Unióban, **különösen annak révén, hogy támogatást biztosít a tagállamoknak, valamint az uniós intézményeknek, ügynökségeknek és szerveknek a kiberbiztonság javításához**. **Az Ügynökségnek az uniós intézmények, ügynökségek és szervek számára a kiberbiztonsággal kapcsolatos tanácsadás és szakértelem referenciapontjának szerepét kell betöltenie.**

(2) Az Ügynökségnek el kell látnia a kiberbiztonsággal kapcsolatos tagállami törvényi, rendeleti és közigazgatási rendelkezések közelítésére vonatkozó intézkedéseket meghatározó uniós jogi aktusok által ráruházott feladatokat.

(2a) Feladatainak ellátása során az Ügynökségnek függetlenül kell eljárnia és a lehető legnagyobb mértékben figyelembe kell vennie a releváns tagállami hatóságok nemzeti szinten meglévő szakértelmét, tevékenységei során elkerülve ugyanakkor a nemzeti szintű tevékenységekkel való párhuzamosságokat.

(3) [...]

4. cikk

Célkitűzések

(1) Az Ügynökségnek kiberbiztonsági szakértői központként kell működnie, amit függetlensége, az általa biztosított tanácsadás, segítségnyújtás és információk tudományos és technikai minősége, működési eljárásainak és módszereinek átláthatósága, valamint a feladatai ellátásában tanúsított gondosság révén tud megvalósítani.

(2) Az Ügynökségnek segítséget kell nyújtania az uniós intézmények, ügynökségek és szervek, valamint a tagállamok számára a kiberbiztonsággal kapcsolatos **uniós** szakpolitikák, **beleértve a kiberbiztonsággal kapcsolatos ágazati szakpolitikákat is,** kidolgozásában és végrehajtásában.

(3) Az Ügynökségnek támogatnia kell az Unión belüli kapacitásépítést és felkészültséget azáltal, hogy segítséget nyújt az uniós **intézmények, ügynökségek és szervek** számára, **valamint** a tagállamok és az állami érdekeltek és a magánszereplők számára is a hálózati és információs rendszereik védelmének fokozásához, **a kiberreziliencia és a kiberbiztonsági eseményekre való reagálási kapacitások** fejlesztéséhez **és javításához, valamint** a kiberbiztonsági készségek és kompetenciák **fejlesztéséhez**[...].

(4) Az Ügynökségnek a kiberbiztonsággal kapcsolatos kérdésekben elő kell mozdítania az uniós szintű együttműködést és koordinációt a tagállamok, az uniós intézmények, ügynökségek és szervek, valamint a releváns **magánszereplők és állami** érdekeltek között[...].

(5) Az Ügynökségnek **hozzá** kell **járulnia** [...] az uniós szintű kiberbiztonsági képességek **növeléséhez** annak érdekében, hogy [...] **segítséget lehessen nyújtani** a tagállamoknak a kiberfenyegetések megelőzéséhez és az azokra való reagáláshoz, különösen a határokon átnyúló biztonsági események esetében.

(6) Az Ügynökségnek elő kell mozdítania a tanúsítás használatát **annak érdekében, hogy el lehessen kerülni a tanúsítási rendszerek szétaprózódását az Unión belül. Az Ügynökségnek különösen hozzá kell járulnia** [...] egy uniós szintű kiberbiztonsági tanúsítási keretrendszernek az e rendelet III. címével összhangban történő létrehozásához és fenntartásához annak érdekében, hogy átláthatóbbá váljon, hogy a kiberbiztonság tekintetében mennyire megbízhatóak az ikt-termékek és -szolgáltatások, megerősítve ezzel a digitális belső piacba vetett bizalmat.

(7) Az Ügynökségnek elő kell segítenie azt, hogy a polgárok és a vállalkozások a kiberbiztonsághoz kapcsolódó kérdések tekintetében nagy fokú tudatossággal járjanak el.

IA. FEJEZET
FELADATOK

5. cikk

*[...]**Az uniós szakpolitika és jogszabályok kidolgozása és végrehajtása***

Az Ügynökségnek az alábbi tevékenységekkel kell hozzájárulnia 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 jogalkotási kezdeményezésekkel kapcsolatban is;

(2) segítségnyújtás a tagállamok számára a kiberbiztonsággal kapcsolatos uniós szakpolitika és jogszabályok következetes végrehajtásában, nevezetesen az (EU) 2016/1148 irányelv vonatkozásában, többek között a kockázatkezelés, a biztonsági események bejelentése és az információk megosztása tekintetében véleményekkel, iránymutatásokkal, tanácsadással és bevált gyakorlatokkal, valamint az ezzel a területtel kapcsolatos bevált gyakorlatok illetékes hatóságok közötti cseréjének elősegítésével;

(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 gyakorlatok illetékes hatóságok közötti cseréjének elősegítésével;

2. az elektronikus hírközlés magasabb biztonsági szintjének előmozdítása, többek között szakértelem rendelkezésre bocsátása és tanácsadás révén, valamint a bevált gyakorlatok illetékes hatóságok közötti cseréjének elősegítésével;

(5) az uniós szakpolitikai tevékenységek rendszeres felülvizsgálatához nyújtott támogatás a vonatkozó jogi keretrendszer végrehajtásának állásáról szóló éves jelentés formájában, a következők tekintetében:

a) azok a tagállami biztonságiesemény-bejelentések, amelyekről az (EU) 2016/1148 irányelv 10. cikkének (3) bekezdése alapján az egyedüli kapcsolattartó pontok tájékoztatják az együttműködési csoportot;

b) azok a bejelentések, amelyeket a felügyeleti szervek a 910/2014/EU rendelet 19. cikke (3) bekezdésének megfelelően juttatnak el az Ügynökséghez a bizalmi szolgáltatóknál bekövetkezett, a biztonság megsértésével és az adatok sértetlenségének megszűnésével járó esetekről;

c) azok a nyilvános hírközlő hálózatokat vagy nyilvánosan hozzáférhető elektronikus hírközlési szolgáltatásokat biztosító vállalkozások által tett [...] biztonsági**esemény**-bejelentések, amelyekről [az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló irányelv] 40. cikkének megfelelően az illetékes hatóságok tájékoztatják az Ügynökséget.

6. cikk

*[...]**Kapacitásépítés***

(1) Az Ügynökségnek támogatnia kell:

a) a tagállamokat a kiber[...]**fenyegetések**[...] és biztonsági események megelőzésének, észlelésének és elemzésének, valamint az ezekre való reagálási képességnek a javítására irányuló erőfeszítéseikben, biztosítva számukra a szükséges ismereteket és szaktudást;

b) az uniós intézményeket, [...] ügynökségeket **és szerveket** a kiber[...]**fenyegetések**[...] és biztonsági események megelőzésének, észlelésének és elemzésének, valamint az ezekre való reagálási képességnek a javítására irányuló erőfeszítéseikben, **különösen** annak révén, hogy megfelelő támogatást biztosít az uniós intézmények, ügynökségek és szervek számítógépes vészhelyzeteket elhárító csoportjának (CERT-EU);

c) azok kérése alapján a tagállamokat a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) továbbfejlesztésében az (EU) 2016/1148 irányelv 9. cikke (5) bekezdésének megfelelően;

d) azok kérése alapján a tagállamokat a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia kidolgozásában az (EU) 2016/1148 irányelv 7. cikke (2) bekezdésének megfelelően; az Ügynökségnek ezen túlmenően az egész Unióban elő kell mozdítania a kapcsolódó információk terjesztését és [...]**nyomon kell követnie** e stratégiák végrehajtását a bevált gyakorlatok előmozdítása érdekében;

e) az uniós intézményeket a kiberbiztonsággal kapcsolatos uniós stratégiák kidolgozásában és felülvizsgálatában, elősegítve azok terjesztését és végrehajtásuk előrehaladásának nyomon követését;

f) a tagállami és az uniós CSIRT-eket képességeik fejlesztésében, többek között a párbeszéd és az információcsere előmozdítása révén annak biztosítása érdekében, hogy a legkorszerűbbnek számító megoldások tekintetében minden CSIRT rendelkezzen egy sor közösen megállapított minimumképességgel, és a bevált gyakorlatok szerint működjön;

g) a tagállamokat a 7. cikk (6) bekezdésében említett, uniós szintű **rendszeres**[...] 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 gyakorlatok megosztás**ában**[...], különösen az alapvető szolgáltatásokat nyújtó szereplők tagállamok általi meghatározása tekintetében, beleértve a határokon átnyúló függőségeket, a biztonsági kockázatokra és biztonsági eseményekre vonatkozóan is, az (EU) 2016/1148 irányelv 11. cikke (3) bekezdése l) pontjának megfelelően.

(2) Az Ügynökségnek **támogatnia** kell **az ágazatokon belüli és az azok közötti információmegosztást**[...], különösen az (EU) 2016/1148 irányelv II. mellékletében felsorolt ágazatokban azáltal, hogy megosztja a rendelkezésre álló eszközökkel és az eljárásokkal kapcsolatban bevált gyakorlatokat, illetve iránymutatást nyújt e téren, továbbá útmutatással szolgál az információk megosztásával kapcsolatos szabályozási kérdések kezelését illetően.

7. cikk

*[...]**Uniós szintű operatív együttműködés**[...]*

(1) Az Ügynökségnek támogatnia kell **a tagállamok, az uniós intézmények, ügynökségek és**[...] szervek, valamint az érdekeltek közötti operatív együttműködést.

(2) Az Ügynökségnek operatív szintű együttműködést és szinergiákat kell kialakítania az uniós intézményekkel, [...] ügynökségekkel **és szervekkel**, köztük a CERT-EU-val, a kiberbűnözés elleni szolgálatokkal, valamint a magánélet és a személyes adatok védelmével foglalkozó felügyeleti hatóságokkal a közös problémák kezelése érdekében, többek között a következők által:

a) a szakismeretek és a bevált gyakorlatok 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 Ügynökségnek kell biztosítania a CSIRT-ek hálózatának titkárságát, és **ebben a minőségében** [...] elő kell segítenie a hálózat tagjai közötti információmegosztást és együttműködést.

(4) Az Ügynökségnek **támogatnia** kell [...] a CSIRT-ek hálózatán belüli operatív együttműködést, **kérésük alapján** 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) [...]a jelentős vagy lényeges hatású biztonsági események technikai **kezelésének megkönnyítése, többek között különösen a technikai megoldások tagállamok közötti önkéntes megosztásának támogatása révén**;

c) a sebezhetőségek[...] és biztonsági események elemzése**;**

ca) támogatás az (EU) 2016/1148 irányelv szerint jelentős vagy lényeges hatású biztonsági események utólagos technikai vizsgálatához.

E feladatok ellátása során az Ügynökségnek és a CERT-EU-nak strukturált együttműködést kell folytatnia a szinergiák kihasználása **és a tevékenységek párhuzamos végzésének elkerülése** érdekében[...].

(5) [...]

[...]

(6) Az Ügynökségnek **rendszeresen**[...] kiberbiztonsági gyakorlatokat kell szerveznie uniós szinten, és kérésre támogatást kell biztosítania a tagállamoknak, valamint az uniós intézményeknek, ügynökségeknek és szerveknek gyakorlatok szervezéséhez. **Az ilyen uniós szintű gyakorlatok tartalmazhatnak műszaki, operatív vagy stratégiai elemeket**[...]. **Kétévente egyszer szervezni kell egy olyan nagyobb szabású gyakorlatot, amely az összes fenti elemet tartalmazza.** Az Ügynökségnek emellett hozzá kell járulnia és adott esetben segítséget kell nyújtania az ágazati kiberbiztonsági gyakorlatok megszervezéséhez a releváns [...]**szervezetekkel** együtt, **mely utóbbiak** részt vehetnek az uniós szintű kiberbiztonsági gyakorlatok**ban** is[...].

(7) Az Ügynökségnek **a tagállamokkal szoros együttműködésben** rendszeresen uniós kiberbiztonsági technikai helyzetjelentést kell készítenie a biztonsági eseményekről és a fenyegetésekről, a nyilvánosan hozzáférhető információk, az Ügynökség saját elemzése, valamint többek között a következő szervezetek által rendelkezésre bocsátott jelentések alapján: a tagállamok CSIRT-jei [...] vagy a kiberbiztonsági irányelv szerinti egyedüli kapcsolattartó pontok (**mindkettő esetében önkéntes alapon**[...]); az Europol keretében működő Számítástechnikai Bűnözés Elleni Európai Központ (EC3), CERT-EU.

(8) Az Ügynökségnek hozzá kell járulnia ahhoz, hogy a kiberbiztonsággal kapcsolatos nagy kiterjedésű, határokon átnyúló biztonsági eseményekre vagy válságokra uniós és tagállami szinten együttműködésen alapuló válasz kerüljön kidolgozásra, elsősorban az alábbiak révén:

a) **az önkéntes alapon megosztott,** tagállami forrásokból származó jelentések összesítése a közös helyzetismeret kialakításához való hozzájárulás céljából;

b) a CSIRT-ek hálózata és az uniós szintű technikai és politikai döntéshozók közötti hatékony információcsere és eszkalációs eljárások biztosítása;

c) [...] **a tagállamok kérése alapján** a biztonsági események vagy válságok technikai kezelésének **elősegítése**, többek között **különösen** a technikai megoldások tagállamok közötti **önkéntes** megosztásának [...] **támogatása révén**;

d) **az uniós intézmények, ügynökségek és szervek, valamint kérésre a tagállamok** támogatása a biztonsági eseményekkel vagy válságokkal kapcsolatos nyilvános kommunikációban;

e) **kérésre a tagállamok támogatása abban, hogy** teszteljék[...] az ilyen biztonsági eseményekre vagy válságokra való reagálást célzó együttműködési terveket.

8. cikk

[...]Piac, kiberbiztonsági tanúsítás, valamint szabványosítás

Az Ügynökségnek:

a) támogatnia kell és elő kell mozdítania az ikt**-folyamatok,** -termékek és -szolgáltatások – e rendelet III. címében meghatározott – kiberbiztonsági tanúsítására vonatkozó uniós szakpolitika kidolgozását és végrehajtását, az alábbiak révén:

1. európai kiberbiztonsági tanúsítási rendszerek javaslati szintű kidolgozása az ikt**-folyamatokra,** -termékekre és -szolgáltatásokra vonatkozóan **az iparággal történő együttműködés révén,** 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 gyakorlatok kialakítása a nemzeti **kiberbiztonsági** tanúsítást végző [...]hatóságokkal és az ágazattal együttműködve;

3a. ajánlás készítése az európai kiberbiztonsági tanúsítási rendszerek fejlesztéséhez használható megfelelő műszaki előírásokra a 47. cikk (1) bekezdésének b) pontjában említetteknek megfelelően az olyan esetekre, amikor nem állnak rendelkezésre szabványok;

3b. hozzájárulás az értékelési és tanúsítási folyamattal kapcsolatos megfelelő kapacitásépítéshez iránymutatások kidolgozásával és közzétételével, valamint kérésre a tagállamoknak nyújtott támogatással;

b) elő kell segítenie a kockázatkezelésre és az ikt**-folyamatok,** -termékek és szolgáltatások[...] biztonságára vonatkozó európai és nemzetközi szabványok kidolgozását és alkalmazását**;**

ba) a tagállamokkal együttműködésben tanácsot kell adnia és iránymutatásokat kell készítenie 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 elemeznie kell a kiberbiztonsági piac keresleti és kínálati oldalára jellemző főbb tendenciákat, és gondoskodnia kell ezen elemzések terjesztéséről az Unió kiberbiztonsági piacának megerősítése céljából.

9. cikk

*[...]**Ismeretek* és *tájékoztatás***[...]

Az Ügynökségnek:

a) elemzéseket kell készítenie a kialakulóban lévő technológiákról, és tematikus értékeléseket kell végeznie a technológiai innovációknak a kiberbiztonságra gyakorolt várható társadalmi, jogi, gazdasági és szabályozási hatásairól;

b) el kell végeznie a kiberbiztonsági fenyegetések és események hosszú távú stratégiai elemzését az új tendenciák azonosítása és a kiberbiztonsági [...]**események** megelőzésének elősegítése érdekében;

c) a tagállami hatóságok szakértőivel együttműködésben tanácsot és útmutatást kell adnia, illetve bevált gyakorlatokat kell rendelkezésre bocsátania a hálózati és információs rendszerek biztonságával, különösen [...] az (EU) 2016/1148 irányelv II. mellékletében felsorolt ágazatokat támogató infrastruktúrák, **valamint az említett irányelv III. mellékletében felsorolt digitális szolgáltatók által használt infrastruktúrák** biztonságával kapcsolatban;

d) össze kell gyűjtenie, rendszereznie kell és a nyilvánosság számára elérhetővé kell tennie egy külön erre a célra létrehozott portálon az uniós intézmények, ügynökségek és szervek által, **valamint az önkéntes alapon a tagállamok, illetve a magánszereplők és az állami érdekeltek által** a kiberbiztonsággal kapcsolatban rendelkezésre bocsátott információkat;

e) [...]

f) össze kell gyűjtenie és elemeznie kell a jelentős biztonsági eseményekkel kapcsolatos nyilvánosan hozzáférhető információkat, valamint jelentéseket kell készítenie annak érdekében, hogy azok révén Unió-szerte iránymutatást lehessen nyújtani a vállalkozások és a magánszemélyek számára;

g) [...].

9a. cikk

Tudatosságnövelés és oktatás

Az Ügynökségnek:

a) növelnie kell a közvélemény kiberbiztonsági kockázatokkal kapcsolatos tudatosságát, és a bevált gyakorlatokról szóló, az egyedi felhasználóknak szánt iránymutatást kell eljuttatnia a polgárokhoz és a szervezetekhez;

b) rendszeres tájékoztató kampányokat kell szerveznie a tagállamokkal, valamint az uniós intézményekkel, szervekkel, ügynökségekkel és az ágazati szereplőkkel együttműködésben annak érdekében, hogy az Unión belül fokozódjon a kiberbiztonság és annak láthatósága;

c) segítséget kell nyújtania a tagállamoknak a kiberbiztonsággal kapcsolatos tudatosság növelése és a kiberbiztonsággal kapcsolatos oktatás előmozdítása érdekében tett erőfeszítéseikhez;

d) támogatnia kell a kiberbiztonsággal kapcsolatos oktatás és tudatosság területén kialakult bevált gyakorlatokra vonatkozó, a tagállamok közötti szorosabb koordinációt és információcserét, elősegítve egy olyan hálózat létrehozását és fenntartását, amelyben nemzeti oktatási kapcsolattartó pontok vesznek részt.

10. cikk

*[...]**Kutatás és innováció***

A kutatás és az innováció tekintetében az Ügynökségnek:

a) tanácsokkal kell ellátnia 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 kockázatokat és fenyegetéseket is, másrészt pedig ahhoz, hogy eredményesen lehessen alkalmazni a kockázatmegelőző technológiákat;

b) részt kell vennie a kutatás és az innováció finanszírozását célzó programok megvalósítási szakaszában, amennyiben a Bizottság az erre vonatkozó hatásköröket rá ruházta, vagy kedvezményezettként.

11. cikk

*[...]**Nemzetközi együttműködés***

Az Ügynökségnek a kiberbiztonsággal kapcsolatos kérdésekre vonatkozó nemzetközi együttműködés elősegítése érdekében hozzá kell járulnia 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 [...]**releváns nemzetközi együttműködési keretek között** elősegíti a bevált gyakorlatok cseréjét [...];

c) kérésre szakértelemmel támogatja a Bizottságot**;**

ca) az 53. cikkel létrehozott európai kiberbiztonsági tanúsítási csoporttal együttműködésben tanácsadást és támogatást biztosít a Bizottságnak a kiberbiztonsági tanúsítványok harmadik országok esetében történő kölcsönös elismerését célzó megállapodások tekintetében.

II. FEJEZET
AZ ÜGYNÖKSÉG FELÉPÍTÉSE

12. cikk

Struktúra

Az Ügynökség igazgatási és irányítási struktúrájának a következőkből kell állnia:

a) az igazgatótanács, amelynek a 14. cikkben meghatározott feladatokat kell ellátnia;

b) a felügyelőtestület, amelynek a 18. cikkben meghatározott feladatokat kell ellátnia;

c) az ügyvezető igazgató, akinek a 19. cikkben meghatározott feladatokat kell ellátnia;[...]

d) az érdekeltek állandó csoportja, amelynek a 20. cikkben meghatározott feladatokat kell ellátnia**;**

da) a nemzeti összekötő tisztviselők hálózata, amelynek a 20a. cikkben meghatározott feladatokat kell ellátnia.

1. SZAKASZ
IGAZGATÓTANÁCS

13. cikk

Az igazgatótanács összetétele

(1) Az igazgatótanácsnak tagállamonként egy-egy képviselőből és a Bizottság által kijelölt két képviselőből kell állnia. Valamennyi képviselőnek rendelkeznie kell szavazati joggal.

(2) Az igazgatótanács minden egyes tagjának rendelkeznie kell egy póttaggal, aki képviseli őt távollétében.

(3) Az igazgatótanács tagjait és a póttagokat a kiberbiztonság terén meglévő tudásuk alapján kell kinevezni, a megfelelő vezetői, igazgatási és költségvetési készségek figyelembevételével. Az igazgatótanács munkájának folytonosságát biztosítandó, a Bizottságnak és a tagállamoknak törekedniük kell arra, hogy képviselőik ne cserélődjenek túl gyakran az igazgatótanácsban. A Bizottságnak és a tagállamoknak arra kell törekedniük, 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 feladatköre

(1) Az igazgatótanácsnak:

a) meg kell határoznia az Ügynökség működésének általános irányát, és gondoskodnia kell arról, hogy az Ügynökség az e rendeletben megállapított szabályoknak és elveknek megfelelően végezze tevékenységét. Biztosítania kell továbbá, hogy az Ügynökség munkája összhangban legyen a tagállamok által és az Unió szintjén folytatott tevékenységekkel;

b) el kell fogadnia az Ügynökség 21. cikkben említett egységes programozási dokumentumának tervezetét, mielőtt a dokumentumot benyújtanák a Bizottsághoz véleményezésre;

c) a Bizottság véleményének figyelembevételével, a tagok szavazatainak kétharmados többségével, a 17. cikknek megfelelően el kell fogadnia az Ügynökség egységes programozási dokumentumát;

ca) felügyelnie kell az egységes programozási dokumentumban szereplő többéves és éves programozás végrehajtását;

d) a tagok szavazatainak kétharmados többségével el kell fogadnia az Ügynökség éves költségvetését, és el kell látnia az Ügynökség költségvetéséhez kapcsolódó, a III. fejezet szerinti egyéb feladatokat;

e) értékelnie kell, majd pedig el kell fogadnia az Ügynökség tevékenységéről szóló összevont éves jelentést, és a következő év július 1-jéig meg kell küldenie 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) el kell fogadnia az Ügynökségre vonatkozó pénzügyi szabályzatot a 29. cikknek megfelelően;

g) olyan, csalás elleni stratégiát kell elfogadnia, amely – figyelemmel a végrehajtandó intézkedések költség-haszon elemzésére – arányos a csalási kockázatokkal;

h) az összeférhetetlenségek megelőzésére és kezelésére vonatkozó szabályokat kell elfogadnia az igazgatótanács tagjai tekintetében;

i) biztosítania kell 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) el kell fogadnia eljárási szabályzatát;

k) a (2) bekezdésnek megfelelően az Ügynökség személyzete vonatkozásában gyakorolnia kell 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 kell elfogadnia a személyzeti szabályzat és az egyéb alkalmazottakra vonatkozó alkalmazási feltételek végrehajtásával kapcsolatban;

m) e rendelet 33. cikkének megfelelően ki kell neveznie az ügyvezető igazgatót, és adott esetben meg kell hosszabbítania hivatali idejét, vagy fel kell mentenie hivatalából;

n) ki kell neveznie egy számvitelért felelős tisztviselőt, aki lehet a Bizottság számvitelért felelős tisztviselője is, és akinek feladatai ellátása során teljes mértékben függetlenül kell eljárnia;

o) meg kell hoznia az Ügynökség belső struktúráinak kialakításával és szükség szerint 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 engedélyeznie kell munkamegállapodások megkötését.

(2) Az igazgatótanácsnak a személyzeti szabályzat 110. cikkével összhangban, a személyzeti szabályzat 2. cikkének (1) bekezdése és az egyéb alkalmazottakra vonatkozó alkalmazási feltételek 6. cikke alapján határozatot kell elfogadnia, amelyben kinevezésre jogosult hatósági hatásköröket kell ruháznia az ügyvezető igazgatóra, és meg kell határoznia 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, illetve valamelyik tagjára vagy a személyzetnek az ügyvezető igazgatótól eltérő tagjára ruházhatja.

15. cikk

Az igazgatótanács elnöke

Az igazgatótanácsnak a tagok szavazatainak kétharmados többségével négy évre elnököt és elnökhelyettest kell választania tagjai közül; e személyek hivatali ideje egy alkalommal megújítható. Ha azonban igazgatótanácsi tagságuk hivatali idejük alatt bármikor megszűnik, ugyanezen a napon hivatali idejüknek is automatikusan meg kell szűnnie. Az elnökhelyettesnek hivatalból helyettesítenie kell az elnököt abban az esetben, ha az elnök nem tudja ellátni feladatait.

16. cikk

Az igazgatótanács ülései

(1) Az igazgatótanács üléseit az elnöknek kell összehívnia.

(2) Az igazgatótanácsnak évente legalább két rendes ülést kell tartania. Az igazgatótanácsnak az elnök kérésére, a Bizottság kérésére vagy tagjai legalább egyharmadának kérésére rendkívüli ülést is kell tartania.

(3) Az ügyvezető igazgatónak – szavazati jog nélkül – részt kell vennie 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 Ügynökségnek kell biztosítania a titkárságot.

17. cikk

Az igazgatótanács szavazási szabályai

(1) Az igazgatótanácsnak tagjai többségi szavazatával kell határozatot hoznia.

(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 elnöknek részt kell vennie a szavazásban.

(5) Az ügyvezető igazgató nem vehet részt a szavazásban.

(6) Az igazgatótanács eljárási szabályzatának még részletesebben kell rendelkeznie a szavazás szabályairól, és különösen arról, hogy egy tag milyen feltételek mellett járhat el egy másik tag nevében.

2. SZAKASZ
FELÜGYELŐTESTÜLET

18. cikk

A felügyelőtestület

(1) Az igazgatótanács munkáját felügyelőtestületnek kell támogatnia.

(2) A felügyelőtestületnek:

a) elő kell készítenie az igazgatótanács által elfogadandó határozatokat;

b) az igazgatótanáccsal együtt gondoskodnia kell 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 kell nyújtania és tanácsot kell adnia az ügyvezető igazgató számára az igazgatótanács adminisztratív és költségvetési ügyekben hozott határozatainak a 19. cikk szerinti végrehajtásában.

(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 igazgatónak részt kell vennie a felügyelőtestület ülésein, de szavazati joggal nem rendelkezik.

(4) A felügyelőtestület tagjainak hivatali ideje négy év. A hivatali idő megújítható.

(5) A felügyelőtestületnek legalább háromhavonta üléseznie kell. A felügyelőtestület elnökének a tagok kérésére további üléseket kell összehívnia.

(6) A felügyelőtestület eljárási szabályzatát az igazgatótanácsnak kell megállapítania.

(7) [...]

3. SZAKASZ
ÜGYVEZETŐ IGAZGATÓ

19. cikk

Az ügyvezető igazgató feladatköre

(1) Az Ügynökséget az ügyvezető igazgató vezeti, akinek feladatai ellátása során függetlenül kell eljárnia. Az ügyvezető igazgató a tevékenységéért az igazgatótanácsnak tartozik felelősséggel.

(2) Az ügyvezető igazgató, amennyiben erre felkérést kap, köteles beszámolni 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**, az éves munkaprogram végrehajtását is beleértve**, és annak benyújtása az igazgatótanácshoz értékelésre és elfogadásra;

f) a visszamenőleges értékelések megállapításain alapuló cselekvési terv elkészítése és kétévente 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 jogtalanul kifizetett összegek visszatérítésével, valamint szükség esetén hatékony, arányos és visszatartó erejű közigazgatási vagy pénzügyi szankciókkal;

k) az Ügynökség csalás elleni stratégiájának elkészítése és az igazgatótanács elé terjesztése jóváhagyatás céljából;

l) kapcsolat kialakítása és fenntartása az üzleti élet szereplőivel és a fogyasztói szervezetekkel, az érdekeltekkel folytatott rendszeres párbeszéd biztosítása érdekében;

la) az uniós szakpolitika következetes alakításának és végrehajtásának biztosítása érdekében rendszeres információcsere az uniós intézményekkel, ügynökségekkel és szervekkel azok kiberbiztonsági tevékenységeire vonatkozóan;

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 **szükség esetén az ügynökség feladatainak hatékony és eredményes ellátása céljából, megfelelő költség-haszon-elemzés alapján** [...] **dönthet egy vagy több helyi irodának egy vagy több tagállamban történő létrehozásáról**. A helyi irodára vonatkozó döntést megelőzően az ügyvezető igazgatónak **ki kell kérnie az érintett tagállamok véleményét, azt a tagállamot is beleértve, amelyben az ügynökség székhelye található, és** meg kell szereznie a Bizottság **és** az igazgatótanács [...] előzetes hozzájárulását. **Ha az ügyvezető igazgató és az érintett tagállamok közötti konzultációs folyamat során nem alakul ki egyetértés, az ügyet a Tanács elé kell terjeszteni megvitatásra.** 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.[...]**A helyi irodák teljes személyzetének létszámát a szükséges minimumra kell korlátozni, és az <u>összességében</u> nem haladhatja meg az <u>abban a tagállamban alkalmazott</u> <u>[...]</u> személyzet létszámának 40 %-át, <u>amelyben az Ügynökség székhelye található</u>. Az egyes helyi irodák személyzetének létszáma nem haladhatja meg az <u>abban a tagállamban alkalmazott</u> <u>[...]</u> személyzet létszámának 10 %-át, <u>amelyben az Ügynökség székhelye található</u>.**

4. SZAKASZ
AZ ÉRDEKELTEK ÁLLANDÓ CSOPORTJA

20. cikk

Az érdekeltek állandó csoportja

(1) Az igazgatótanácsnak az ügyvezető igazgató javaslatára létre kell hoznia 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, **az alapvető szolgáltatásokat nyújtó szereplők,** 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 az adatvédelmi 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 igazgatónak vagy az általa eseti alapon kinevezett személynek kell ellátnia.

(4) Az érdekeltek állandó csoportja tagjainak hivatali ideje két és fél év. 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 csoportjának tanácsadással kell segítenie az Ügynökséget tevékenységeinek ellátásában. A csoport különösen az Ügynökség munkaprogramjára vonatkozó javaslat elkészítéséhez és a releváns érdekeltekkel a munkaprogramot érintő valamennyi kérdésről folytatandó párbeszéd biztosításához köteles tanácsot adni az ügyvezető igazgatónak.

(5a) Az érdekeltek állandó csoportja köteles rendszeresen tájékoztatni tevékenységeiről az igazgatótanácsot.

4A. SZAKASZ
A NEMZETI ÖSSZEKÖTŐ TISZTVISELŐK HÁLÓZATA

20a. cikk

A nemzeti összekötő tisztviselők hálózata

(1) Az igazgatótanácsnak az ügyvezető igazgató javaslata alapján létre kell hoznia a nemzeti összekötő tisztviselőknek a tagállamok képviselőiből álló hálózatát.

(2) A nemzeti összekötő tisztviselők hálózatában minden tagállamnak képviseltetnie kell magát. Minden tagállam egy-egy képviselőt jelöl ki. A hálózat üléseire többféle szakértői felállásban kerülhet sor.

(3) A nemzeti összekötő tisztviselők hálózatának feladata elsősorban az ENISA és a tagállamok közötti információcsere elősegítése. Támogatnia kell az ENISA arra irányuló munkáját, hogy tevékenységeit, megállapításait és ajánlásait az Unió egészében eljuttassa az érintett érdekeltekhez.

(4) **A nemzeti összekötő tisztviselőknek tagállami szinten központi kapcsolattartó pontként kell működniük annak érdekében, hogy az ENISA munkaprogramjának végrehajtásával összefüggésben megkönnyítsék az ENISA és a tagállami szakértők közötti együttműködést.**

(5) **Míg a nemzeti összekötő tisztviselőknek szorosan együtt kell működniük az igazgatótanács országukat képviselői tagjával, magának a hálózatnak el kell kerülnie a párhuzamos munkavégzést mind az igazgatótanáccsal, mind a többi uniós fórummal.**

(6) **A nemzeti összekötő tisztviselők hálózatának feladatait és eljárásait az Ügynökség belső működési szabályzatában kell meghatározni, és azokat nyilvánosságra kell hozni.**

5. SZAKASZ
MŰKÖDÉS

21. cikk

Egységes programozási dokumentum

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

(2) Az ügyvezető igazgató – az 1271/2013/EU felhatalmazáson alapuló bizottsági rendelet[14] 32. cikkével összhangban és a Bizottság által meghatározott iránymutatások figyelembevételével – minden évben köteles elkészíteni a többéves és éves programozást tartalmazó egységes programozási dokumentum tervezetét, amely a megfelelő humán- és pénzügyi erőforrások tervezésére is kiterjed.

(3) Az igazgatótanácsnak minden évben november 30-ig el kell fogadnia az (1) bekezdésben említett egységes programozási dokumentumot, és a rákövetkező évben legkésőbb január 31-ig továbbítania kell azt az Európai Parlamentnek, a Tanácsnak és a Bizottságnak; hasonlóképpen gondoskodnia kell 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 tevékenységalapú költségvetés-tervezés és irányítás elveivel összhangban – ismertetni kell benne a finanszírozandó fellépéseket, és meg kell jelölni az egyes fellépésekhez rendelt pénzügyi és humánerőforrásokat. 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.

[14] A Bizottság 2013. szeptember 30-i 1271/2013/EU felhatalmazáson alapuló rendelete 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.).

(6) Amikor az Ügynökség új feladatot kap, az igazgatótanácsnak módosítania kell 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 köteles kötelezettségvállalási nyilatkozatot tenni, továbbá nyilatkozni arról, hogy van-e olyan közvetlen vagy közvetett érdeke, amelyről feltehető, hogy függetlenségét befolyásolhatja. A nyilatkozatnak pontosnak és teljes 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 köteles legkésőbb az adott ülés kezdetén pontosan és teljeskörűen nyilatkozni az egyes napirendi pontokkal kapcsolatos minden olyan érdekéről, amelyről feltehető, hogy függetlenségét befolyásolhatja, az ilyen napirendi pontok megvitatásában való részvételtől és az azokról való szavazástól pedig köteles tartózkodni.

(3) Az Ügynökségnek belső működési szabályzatában meg kell állapítania az (1) és a (2) bekezdésben említett érdekeltségi nyilatkozatokkal kapcsolatos szabályokra vonatkozó gyakorlati rendelkezéseket.

23. cikk

Átláthatóság

(1) Az Ügynökség köteles tevékenységét magas fokú átláthatóság mellett, a 25. cikknek megfelelően végezni.

(2) Az Ügynökségnek biztosítania kell, 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 érdekelt felek az Ügynökség egyes tevékenységeiben megfigyelőként részt vegyenek.

(4) Az Ügynökségnek belső működési szabályzatában meg kell állapítania 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 Ügynökségnek belső működési szabályzatában meg kell állapítania az (1) és (2) bekezdésben említett titoktartási szabályok végrehajtására vonatkozó gyakorlati rendelkezéseket.

(4) Amennyiben az Ügynökség feladatainak ellátásához szükséges, az igazgatótanácsnak lehetővé kell tennie az Ügynökség számára, hogy minősített adatokat is kezeljen. Ebben az esetben az igazgatótanácsnak a Bizottság szolgálataival egyetértésben belső működési szabályzatot kell elfogadnia az (EU, Euratom) 2015/443[15] és az (EU, Euratom) 2015/444 bizottsági határozatban[16] megállapított biztonsági elvek alkalmazásáról. Ennek a szabályzatnak a minősített adatok cseréjére, kezelésére és tárolására vonatkozó rendelkezéseket kell tartalmaznia.

---

15 A Bizottság 2015. március 13-i (EU, Euratom) 2015/443 határozata a Bizottságon belüli biztonságról (HL L 72., 2015.3.17., 41. o.).

16 A Bizottság 2015. március 13-i (EU, Euratom) 2015/444 határozata az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (HL L 72., 2015.3.17., 53. o.).

25. cikk

Dokumentumokhoz való hozzáférés

(1) Az 1049/2001/EK rendelet az Ügynökség birtokában lévő dokumentumokra is vonatkozik.

(2) Az igazgatótanácsnak az Ügynökség létrejöttét követő hat hónapon belül el kell fogadnia 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 igazgatónak minden évben el kell készítenie és a létszámterv tervezetével együtt továbbítania kell az igazgatótanácsnak az Ügynökség következő pénzügyi évre tervezett bevételeire és kiadásaira vonatkozó kimutatás tervezetét. A bevételeknek és a kiadásoknak egyensúlyban kell lenniük.

(2) Az igazgatótanácsnak a tervezett bevételekről és kiadásokról szóló kimutatás (1) bekezdésben említett tervezete alapján minden évben el kell készítenie az Ügynökség következő költségvetési évre vonatkozó tervezett bevételeiről és kiadásairól szóló kimutatást.

(3) Az igazgatótanácsnak minden évben január 31-ig meg kell küldenie 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.

(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 igazgatótanácsnak az egységes programozási dokumentummal együtt el kell fogadnia az Ügynökség költségvetését. A költségvetés az Unió általános költségvetésének végleges elfogadását követően válik véglegessé. Az igazgatótanácsnak az Ügynökség költségvetését és egységes programozási dokumentumát szükség szerint az Unió általános költségvetéséhez kell igazítania.

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 mindenkori pénzügyi évet követő év március 1-jéig (N+1. év március 1.) az Ügynökség számvitelért felelős tisztviselőjének meg kell küldenie 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 tisztviselőjének saját felelősségi körében el kell készítenie az Ügynökség végleges beszámolóját.

(5) Az ügyvezető igazgató köteles a végleges beszámolót véleményezésre benyújtani az igazgatótanácshoz.

(6) Az ügyvezető igazgató köteles N+1. év március 31-ig megküldeni az Európai Parlamentnek, a Tanácsnak, a Bizottságnak és a Számvevőszéknek a költségvetési és pénzügyi gazdálkodásról szóló jelentést.

(7) A számvitelért felelős tisztviselőnek N+1. év július 1-jéig meg kell küldenie 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 köteles az e végleges beszámolóra vonatkozó teljességi nyilatkozatot is benyújtani a Számvevőszéknek, egy másolati példányt pedig a Bizottság számvitelért felelős tisztviselőjének.

(9) Az ügyvezető igazgatónak a következő év november 15-ig közzé kell tennie a végleges beszámolót.

(10) Az ügyvezető igazgató köteles N+1. év szeptember 30-ig válaszolni a Számvevőszéknek az észrevételekre, és e válaszról másolatot küldeni az igazgatótanácsnak és a Bizottságnak.

(11) Az ügyvezető igazgató köteles az Európai Parlament kérésére a költségvetési rendelet 165. cikke (3) bekezdésének megfelelően benyújtani az Európai Parlamentnek 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 szabályok

Az Ügynökségre vonatkozó pénzügyi szabályokat a Bizottsággal folytatott konzultációt követően az igazgatótanácsnak kell elfogadnia. Ezek a szabályok nem térhetnek el az 1271/2013/EU rendelettől, 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[17] értelmében folytatott küzdelem elősegítése érdekében az Ügynökség köteles, legkésőbb hat hónappal működésének megkezdése után csatlakozni az Európai Csalás Elleni Hivatal (OLAF) belső vizsgálatairól szóló, 1999. május 25-i intézményközi megállapodáshoz, és a megállapodás mellékletében szereplő minta alapján el kell fogadnia az Ügynökség személyzetének valamennyi tagjára alkalmazandó megfelelő rendelkezéseket.

(2) A Számvevőszék jogosult dokumentumalapú és helyszíni ellenőrzést végezni a támogatások összes kedvezményezettjénél, valamint az Ügynökségtől uniós forrásokban részesülő vállalkozóknál és alvállalkozóknál.

[17] Az Európai Parlament és a Tanács 2013. szeptember 11-i 883/2013/EU, Euratom rendelete 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.).

(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[18] 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.

---

18 A Tanács 1996. november 11-i 2185/96/Euratom, EK rendelete 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.).

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

Az ügyvezető igazgató

(1) Az Ügynökségnek az ügyvezető igazgatót az egyéb alkalmazottakra vonatkozó alkalmazási feltételek 2. cikkének a) pontja értelmében ideiglenes alkalmazottként kell foglalkoztatnia.

(2) Az ügyvezető igazgatót nyílt és átlátható kiválasztási eljárást követően az igazgatótanácsnak kell kineveznie a Bizottság által javasolt jelöltek listájáról.

(3) Az ügyvezető igazgató szerződésének megkötése céljából az Ügynökséget az igazgatótanács elnökének kell képviselnie.

(4) Kinevezése előtt az igazgatótanács által kiválasztott jelöltet fel kell kérni arra, hogy tegyen nyilatkozatot az Európai Parlament illetékes bizottsága előtt, és válaszoljon a képviselők kérdéseire.

(5) Az ügyvezető igazgató hivatali ideje **négy**[...] év. Ezen időszak lejárta előtt a Bizottság értékelést készít, amely figyelembe veszi az ügyvezető igazgató teljesítményét, valamint az Ügynökség jövőbeni feladatait és az előtte álló kihívásokat.

(6) Az igazgatótanácsnak az ügyvezető igazgató kinevezéséről, hivatali idejének meghosszabbításáról és felmentéséről a szavazásra jogosult tagok kétharmadának szavazatával kell döntenie.

(7) Az igazgatótanács az (5) bekezdésben említett értékelést figyelembe vevő bizottsági javaslat alapján eljárva az ügyvezető igazgató hivatali idejét egy alkalommal, legfeljebb **négy**[...] évre meghosszabbíthatja.

(8) Amennyiben az igazgatótanács meg kívánja hosszabbítani az ügyvezető igazgató hivatali idejét, erről tájékoztatnia kell az Európai Parlamentet. Legfeljebb három hónappal hivatali idejének meghosszabbítása előtt az ügyvezető igazgatónak – amennyiben felkérik – az Európai Parlament illetékes bizottsága előtt nyilatkozatot kell tennie, és válaszolnia kell 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 csak az igazgatóság határozata alapján hívható vissza hivatalából [...].

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 igazgatótanácsnak határozatot kell elfogadnia 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 ingatlanvagyont szerezhet, illetve idegeníthet el, és/vagy perképességgel 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 választottbírósági 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 köteles megtéríteni 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

Nyelvhasználati szabályok

(1) Az 1. tanácsi rendeletben megállapított rendelkezések az Ügynökségre is vonatkoznak[19]. 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 köteles biztosítani.

38. cikk

A személyes adatok védelme

(1) A személyes adatoknak az Ügynökség általi feldolgozására a 45/2001/EK európai parlamenti és tanácsi rendelet[20] vonatkozik.

(2) A 45/2001/EK rendelet 24. cikkének (8) bekezdésében említett végrehajtási intézkedéseket az igazgatótanácsnak kell elfogadnia. Az igazgatótanács további intézkedéseket fogadhat el, amennyiben azok szükségesek a 45/2001/EK rendeletnek az Ügynökség általi alkalmazásához.

---

19 1. rendelet az Európai Atomenergia-közösség által használt nyelvek meghatározásáról (HL 17., 1958.10.6., 401. o.).

20 Az Európai Parlament és a Tanács 2000. december 18-i 45/2001/EK rendelete 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.).

39. cikk

Együttműködés harmadik országokkal és nemzetközi szervezetekkel

(1) Amennyiben az az e rendeletben meghatározott célkitűzések eléréséhez szükséges, az Ügynökség harmadik országok illetékes hatóságaival és/vagy nemzetközi 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 Ügynökségnek nyitottnak kell lennie azon harmadik országok részvételére, amelyek ebből a célból megállapodást kötöttek az Unióval. Ezen megállapodások vonatkozó rendelkezései alapján részletes szabályokat kell hozni, meghatározva 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 igazgatótanácsnak az Ügynökség hatáskörébe tartozó kérdések tekintetében stratégiát kell elfogadnia 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 érzékeny adatok védelmére

A Bizottsággal folytatott konzultáció alapján az Ügynökségnek saját biztonsági szabályokat kell elfogadnia 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 szabályoknak többek között az ilyen adatok cseréjére, feldolgozására és tárolására vonatkozó rendelkezésekre kell kiterjedniük.

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 [...] biztosítja az Ügynökség megfelelő működéséhez szükséges feltételeket, 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

Az európai kiberbiztonsági tanúsítási **keretrendszer** […]

(1) **Annak érdekében, hogy a kiberbiztonság szintjének az Európai Unión belüli megemelésének köszönhetően jobb feltételek között működhessen a belső piac, létrejön az európai kiberbiztonsági tanúsítási keretrendszer. E keretrendszer olyan irányítási szabályokat tartalmaz, amelyek – az ikt-folyamatok, -termékek és szolgáltatások digitális egységes piacának a létrehozása céljából – uniós szinten harmonizált megközelítés alkalmazását teszik lehetővé az európai kiberbiztonsági tanúsítási rendszerek tekintetében.**

(2) **Az európai kiberbiztonsági tanúsítási keretrendszer meghatároz egy mechanizmust** az európai kiberbiztonsági tanúsítási rendszerek **létrehozása**, [...] **valamint** annak tanúsítása **céljára**, hogy az e rendszereknek megfelelően [...] **értékelt** ikt**-folyamatok, -** termékek és szolgáltatások megfelelnek adott **biztonsági** követelményeknek, [...] **hogy ezáltal biztosítsa** az e termékek, folyamatok **és** szolgáltatások [...] által tárolt, továbbított vagy kezelt adatok, illetve az általuk ellátott funkciók vagy kínált szolgáltatások rendelkezésre állásának, hitelességének, sértetlenségének vagy titkosságának **a védelmét**, [...] **azok teljes életciklusa alatt.**

44. cikk

Európai kiberbiztonsági tanúsítási rendszerek kidolgozása és elfogadása

(1) Az ENISA-nak a Bizottság **vagy az 53. cikkel létrehozott európai kiberbiztonsági tanúsítási csoport (a továbbiakban: a csoport)** felkérése alapján javaslati szinten ki kell dolgoznia egy, az e rendelet 45., 46. és 47. cikkében meghatározott követelményeknek megfelelő európai kiberbiztonsági tanúsítási rendszert.[...]

(1a) Európai kiberbiztonsági tanúsítási rendszer kidolgozására a tagállamok vagy az érintett érdekelt szervezetek is javaslatot tehetnek a csoportnak. E javaslatok értékelése céljából a csoportnak az 53. cikk (3) bekezdésének ca) pontja szerinti iránymutatások segítségével kritériumokat kell kidolgoznia, és a javaslatokat ezek alapján értékelnie kell, valamint felkérheti az ENISA-t adott európai kiberbiztonsági tanúsítási rendszer javaslati szintű kidolgozására.

(2) Az e cikk (1) bekezdésében említett rendszerek javaslati szintű kidolgozása során az ENISA valamennyi érdekelt féllel – **átlátható konzultációs folyamatok útján** – köteles konzultálni, és szorosan együtt kell működnie a csoporttal. A csoportnak segítséget és szakértői tanácsadást kell biztosítania az ENISA számára a rendszer javaslati szintű kidolgozásához [...], **és a Bizottságnak történő benyújtása előtt véleményt kell elfogadnia a javasolt rendszerről [...]. Az ENISA-nak biztosítania kell, hogy a javasolt rendszerek összhangban álljanak a megfelelőségértékelő szervezet akkreditálása céljára használt, vonatkozó harmonizált szabványnak.**

(3) Az ENISA-nak az e cikk (2) bekezdésével összhangban kidolgozott rendszerjavaslat [...] **továbbítása** [...]**előtt a lehető legkörültekintőbben figyelembe kell vennie a csoport véleményét**.

(4) A Bizottság az ENISA által javasolt rendszer alapján az 55. cikk (2) bekezdésének megfelelően végrehajtási jogi aktusokat fogadhat el, amelyekben az ikt-**folyamatokra,** -termékekre és -szolgáltatásokra vonatkozó, az e rendelet 45., 46. és 47. cikkében foglalt követelményeknek megfelelő európai kiberbiztonsági tanúsítási rendszerekről rendelkezik.

(5) [...]

44a. cikk

Az európai kiberbiztonsági tanúsítási rendszerek gondozása

(1) Az európai kiberbiztonsági tanúsítási rendszerekről, a tanúsítványokról és a 47a. cikk alapján kiadott uniós megfelelőségi nyilatkozatokról való tájékoztatás, illetve az azokkal kapcsolatos publicitás biztosítása céljából az Ügynökségnek egy külön e célra szolgáló weboldalt kell fenntartania.

(2) Az Ügynökségnek a csoporttal szoros együttműködésben legalább ötévente felül kell vizsgálnia az elfogadott európai kiberbiztonsági tanúsítási rendszereket, az érdekelt felektől kapott visszajelzések figyelembevételével. Ha szükséges, a Bizottság vagy a csoport felkérheti az Ügynökséget, hogy a 44. cikk (2) és (3) bekezdésével összhangban indítsa be a módosított rendszer javaslati szintű kidolgozására irányuló folyamatot.

45. cikk

Az európai kiberbiztonsági tanúsítási rendszerek biztonsági célkitűzései

Az európai kiberbiztonsági tanúsítási rendszereket úgy kell kialakítani, hogy – értelemszerűen – [...] **teljesítsék legalább** az alábbi biztonsági célkitűzéseket:

a) a tárolt, továbbított vagy egyéb módon kezelt adatok védelme a véletlen vagy jogosulatlan tárolással, kezeléssel, hozzáféréssel és közléssel szemben, **a folyamat, termék vagy szolgáltatás teljes életciklusa alatt**;

b) a tárolt, továbbított vagy egyéb módon kezelt adatok védelme a véletlen vagy illetéktelen megsemmisítéssel, [...] elvesztéssel vagy megváltoztatással**, vagy a hozzáférhetetlenséggel szemben, a folyamat, termék vagy szolgáltatás teljes életciklusa alatt**;

c) [...] a feljogosított személyek, programok vagy gépek kizárólag a hozzáférési jogaik tárgyát képező adatokhoz, szolgáltatásokhoz vagy funkciókhoz férhetnek hozzá;

d) annak rögzítése, hogy ki mikor mely adatokat, funkciókat és szolgáltatásokat [...] **vette igénybe, használta vagy kezelte egyéb módon**;

e) [...] ellenőrizni lehet, hogy ki mikor mely adatokat, szolgáltatásokat vagy funkciókat vette igénybe, [...] használta **vagy kezelte egyéb módon**;

f) fizikai vagy műszaki biztonsági esemény bekövetkeztekor az adatok, szolgáltatások és funkciók elérhetőségének, illetve az adatokhoz, a szolgáltatásokhoz és a funkciókhoz való hozzáférésnek a mihamarabbi helyreállítása;

g) [...] az ikt**-folyamatok,** -termékek és -szolgáltatások szoftvere **és hardvere** naprakész, esetükben nem állnak fenn **[...] közismert** sebezhetőségek, és rendelkezésre állnak a biztonságos frissítésükre szolgáló [...] mechanizmusok**;**

ga) az ikt-folyamatok, -termékek és -szolgáltatások fejlesztése, gyártása és rendelkezésre bocsátása az adott rendszerben előírt biztonsági követelményeknek megfelelően történik.

46. cikk

Az európai kiberbiztonsági tanúsítási rendszerek megbízhatósági szintjei

(1) Az európai kiberbiztonsági tanúsítási rendszer az „alacsony”, „közepes” és/vagy „magas” megbízhatósági szintek közül egy vagy több szintet határozhat meg az ikt**-folyamatok,** -termékek és -szolgáltatások vonatkozásában[...]. **A megbízhatósági szintnek arányban kell állnia az adott ikt-folyamat, -termék vagy -szolgáltatás rendeltetés szerinti használatához fűződő kockázat szintjével.**

(2) Az alacsony, közepes, illetve magas megbízhatósági szintek egy-egy európai kiberbiztonsági tanúsítási rendszer keretében kibocsátott tanúsítványra vagy uniós megfelelőségi nyilatkozatra **utalnak, amely [...] az egyes megbízhatósági szintek esetében meghatározza a vonatkozó biztonsági követelményeket – így többek között a biztonsági funkciókat is –, valamint az ikt-folyamat, -termék vagy -szolgáltatás értékeléséhez szükséges, ezzel összhangban lévő erőfeszítés szintjét. A tanúsítvány, illetve az uniós megfelelőségi nyilatkozat minősítésének alapját a nekik megfelelő műszaki előírásokra, szabványokra és eljárásokra, többek között műszaki ellenőrzésekre való hivatkozás képezi – melyek célja a kiberbiztonsági események kockázatának csökkentése, illetve azok megelőzése –, az alábbiak szerint:**

a) az „alacsony” megbízhatósági szintet **feltüntető európai kiberbiztonsági tanúsítvány vagy uniós [...] megfelelőségi nyilatkozat arra vonatkozóan szolgál biztosítékkal, hogy az adott ikt-folyamatok, -termékek és -szolgáltatások teljesítik a vonatkozó biztonsági követelményeket – így többek között a biztonsági funkciókat is –, és olyan szintű értékelésen estek át, amelynek célja a kiberbiztonsági eseményekkel és kibertámadásokkal kapcsolatos alapvető, ismert kockázatok minimalizálása. Az értékelési tevékenységeknek magukban kell foglalniuk legalább a műszaki dokumentáció áttekintését, vagy ha ez nem releváns, az ezzel egyenlő hatású helyettesítő tevékenységeket**[...];

b) a „közepes” megbízhatósági szintet **feltüntető európai kiberbiztonsági tanúsítványarra vonatkozóan** szolgál **biztosítékkal, hogy az ikt-folyamatok, -termékek és -szolgáltatások teljesítik a vonatkozó biztonsági követelményeket – így többek között a biztonsági funkciókat is –, és olyan szintű értékelésen estek át, amelynek célja az ismert kiberbiztonsági kockázatok és kiberbiztonsági események, valamint a korlátozott szakértelemmel és erőforrásokkal rendelkező elkövetők által végrehajtott kiberbiztonsági támadások minimalizálása. Az értékelési tevékenységeknek magukban kell foglalniuk legalább az alábbiakat: a közismert sebezhetőségek hiányának felülvizsgálata és annak tesztelése, hogy az ikt-folyamatok, -termékek vagy -szolgáltatások megfelelően működtetik-e a szükséges biztonsági funkciókat; ha ez nem releváns, ezzel egyenlő hatású helyettesítő tevékenységeket kell magukban foglalniuk[...];**

c) a „magas” megbízhatósági szintet **feltüntető európai kiberbiztonsági tanúsítvány arra vonatkozóan** szolgál **biztosítékkal, hogy az ikt-folyamatok, -termékek és -szolgáltatások teljesítik a vonatkozó biztonsági követelményeket – így többek között a biztonsági funkciókat is –, és olyan szintű értékelésen estek át, amelynek célja a jelentős szakértelemmel és erőforrásokkal rendelkező elkövetők által végrehajtott, kifinomult kiberbiztonsági támadások minimalizálása. Az értékelési tevékenységeknek magukban kell foglalniuk legalább a következőket: a közismert sebezhetőségek hiányának felülvizsgálata, annak tesztelése, hogy az ikt-folyamatok, -termékek vagy -szolgáltatások megfelelően, a legmagasabb színvonalon működtetik-e a szükséges biztonsági funkciókat, valamint behatolásvizsgálatok révén annak értékelése, hogy mennyire ellenállóak a jól képzett elkövetők által végrehajtott támadásokkal szemben; vagy ha ez nem releváns, ezzel egyenlő hatású helyettesítő tevékenységeket kell magukban foglalniuk**[...].

(2a) Az európai kiberbiztonsági tanúsítási rendszerekben az értékelési módszerek szigorúságától és mélységétől függően több értékelési szint is meghatározható. Az értékelési szintek mindegyikének egy-egy megbízhatósági szintnek kell megfelelnie, és mindegyik értékelési szint a megbízhatósági komponensek megfelelő kombinációjának megadásával határozandó meg.

47. cikk

Az európai kiberbiztonsági tanúsítási rendszerek elemei

(1) Az európai kiberbiztonsági tanúsítási rendszereknek tartalmazniuk kell **legalább** a következő elemeket:

a) a tanúsítási **rendszer** tárgya és hatálya, ideértve az érintett ikt-folyamatok, -termékek és -szolgáltatások típusát vagy kategóriáit, valamint annak **kifejtése**, **hogy a tanúsítási rendszer hogyan felel meg a várt célcsoport igényeinek**;

b) hivatkozás **az értékelésben követett** [...] nemzetközi, **európai vagy nemzeti szintű** szabványokra. **Amennyiben nem állnak rendelkezésre szabványok, hivatkozást kell beilleszteni az 1025/2012/EU rendelet II. mellékletében foglalt követelményeket teljesítő** [...]műszaki előírásokra, **illetve ha ilyen nem áll rendelkezésre, a rendszerben meghatározott műszaki előírásra vagy egyéb kiberbiztonsági követelményekre;**

c) adott esetben egy vagy több megbízhatósági szint;

ca) adott esetben a megfelelőségértékelő szervezetekre vonatkozó külön követelmények vagy kiegészítő követelmények, amelyek e szervezeteknek a kiberbiztonsági követelmények értékeléséére való szakmai felkészültségét hivatottak garantálni;

d) konkrét értékelési kritériumok és módszerek, ideértve az értékelés típusait is, amelyeket a 45. cikkben említett konkrét célkitűzések elérésének bizonyítása érdekében alkalmaznak;

e) **adott esetben** a kérelmező által a megfelelőségértékelő szervezetek részére benyújtandó **vagy egyéb úton a rendelkezésükre bocsátandó**, a tanúsításhoz szükséges információk;

f) amennyiben a rendszer jelölésekről vagy címkékről rendelkezik, e jelölések vagy címkék használati feltételei;

g) [...] a tanúsítványokban **vagy az uniós megfelelőségi nyilatkozatban** foglalt követelményeknek való megfelelés nyomon követésére vonatkozó szabályok, ideértve a meghatározott kiberbiztonsági követelményeknek való folyamatos megfelelés bizonyítására szolgáló mechanizmusokat is;

h) **adott esetben a tanúsítás** megadására **és megújítására, illetve** a hatályának fenntartására, folytatódására, kiterjesztésére, **illetve** csökkentésére vonatkozó feltételek;

i) az annak következményeire vonatkozó szabályok, ha a tanúsított **vagy önértékelés keretében ellenőrzött** ikt-termékek és -szolgáltatások nem felelnek meg **a rendszer** [...] követelményeinek;

j) az ikt**-folyamatok**, -termékek és -szolgáltatások terén korábban nem észlelt kiberbiztonsági sebezhetőségek bejelentésének és kezelésének módjára vonatkozó szabályok;

k) **adott esetben** a megfelelőségértékelő szervezetek nyilvántartásainak megőrzésére vonatkozó szabályok;

l) az azonos típusú vagy kategóriájú ikt**-folyamatokra,** -termékekre és -szolgáltatásokra kiterjedő nemzeti **vagy nemzetközi** kiberbiztonsági tanúsítási rendszerek, **illetve biztonsági követelmények, valamint értékelési kritériumok és módszerek** azonosítása;

m) a kiadott tanúsítvány **vagy uniós megfelelőségi nyilatkozat** tartalma;

ma) az uniós megfelelőségi nyilatkozatnak, valamint az összes releváns információt tartalmazó műszaki dokumentációnak az ikt-termékek, illetve szolgáltatások gyártója, illetve nyújtója általi megőrzési időtartama;

mb[...]) a tanúsítványok maximális érvényességi ideje;

mc[...]) a megadott, módosított vagy visszavont tanúsítványokkal kapcsolatos közzétételi szabályok;

md[...]) a tanúsítási rendszerek harmadik országokkal való kölcsönös elismerésének feltételei;

me[...]) adott esetben a 48. cikk (4a) bekezdésével összhangban „magas" megbízhatósági szintű európai kiberbiztonsági tanúsítványokat kiállító szervek között alkalmazandó kölcsönös felülvizsgálati mechanizmusra vonatkozó szabályok.

(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, **illetve uniós megfelelőségi nyilatkozat kiállításával** 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 az adott jogi követelményeknek való megfelelés vélelmezésére is használható.

47a. cikk

Megfelelőségi önértékelés

(1) Egy európai kiberbiztonsági tanúsítási rendszer adott esetben lehetővé teheti, hogy a megfelelőségértékelésre az ikt-termékek, illetve -szolgáltatások gyártójának, illetve nyújtójának kizárólagos felelőssége mellett kerüljön sor. Ilyen megfelelőségértékelés csak az „alacsony” megbízhatósági szintnek megfelelő alacsony kockázati szintű ikt-termékek és -szolgáltatások esetében alkalmazható.

(2) Az ikt-termékek, illetve -szolgáltatások gyártója, illetve nyújtója uniós megfelelőségi nyilatkozatot állíthat ki arról, hogy megtörtént annak bizonyítása, hogy a tanúsítási rendszer követelményei teljesülnek. E nyilatkozat kiállításával az ikt-termékek, illetve -szolgáltatások gyártója, illetve nyújtója felelősséget vállal azért, hogy az ikt-termék vagy -szolgáltatás megfelel a tanúsítási rendszer követelményeinek.

(3) Az ikt-termékek, illetve -szolgáltatások gyártójának, illetve nyújtójának gondoskodnia kell arról, hogy az alkalmazandó európai kiberbiztonsági tanúsítási rendszerben meghatározott ideig az 50. cikk (1) bekezdésében említett nemzeti kiberbiztonsági tanúsító hatóság rendelkezésére álljon mind az uniós megfelelőségi nyilatkozat, mind az ikt-termékek, illetve -szolgáltatások tanúsítási rendszernek való megfelelésével kapcsolatos összes releváns információt tartalmazó műszaki dokumentáció. Az uniós megfelelőségi nyilatkozat egy-egy példányát meg kell küldeni a nemzeti kiberbiztonsági tanúsító hatóságnak és az ENISA-nak.

(4) Az uniós megfelelőségi nyilatkozat kiállítása az uniós, illetve a tagállami jog eltérő rendelkezése hiányában önkéntes.

(5) Az e cikk alapján kiadott uniós megfelelőségi nyilatkozatot minden tagállamban el kell ismerni.

48. cikk

Kiberbiztonsági tanúsítás

(1) A 44. cikk alapján elfogadott európai kiberbiztonsági tanúsítási rendszer keretében tanúsított ikt**-folyamatokról**, -termékekről és -szolgáltatásokról vélelmezni kell, hogy megfelelnek az e rendszer által támasztott követelményeinek.

(2) Amennyiben az uniós jog **vagy a tagállamok joga** másként nem rendelkezik, a tanúsítás önkéntes.

(3) Az e cikk szerinti, **„alacsony" vagy „közepes" megbízhatósági szintre vonatkozó** európai kiberbiztonsági tanúsítványt az 51. cikkben említett megfelelőségértékelő szervezetek a 44. cikk alapján elfogadott európai kiberbiztonsági tanúsítási rendszerben foglalt kritériumok alapján adhatják ki.

(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. E [...] szervnek a következők valamelyikének kell lennie:

a) az 50. cikk (1) bekezdésében említett nemzeti **kiberbiztonsági** [...] tanúsító hatóság;

b) az 51. cikk (1) bekezdése szerinti megfelelőségértékelő szervezetként akkreditált **közjogi** szerv [...]

c) [...].

(4a) Azokban az esetekben, ha a 44. cikk szerinti európai kiberbiztonsági tanúsítási rendszer „magas" megbízhatósági szintet ír elő, a tanúsítványt csakis az 50. cikk (1) bekezdésében említett nemzeti kiberbiztonsági tanúsító hatóság állíthatja ki, vagy az 51. cikkben említett megfelelőségértékelő szervezet abban az esetben,

a) ha az egyes, megfelelőségértékelő szervezet által kiállított tanúsítványokra vonatkozóan a nemzeti kiberbiztonsági tanúsító hatóság külön-külön előzőleg a jóváhagyását adta; vagy

b) ha e feladatát a nemzeti kiberbiztonsági tanúsító hatóság előzőleg általános jelleggel átruházta az adott megfelelőségértékelő szervezetre.

(5) Az ikt-**folyamataikat,** -termékeiket vagy -szolgáltatásaikat a tanúsítási mechanizmusnak alávető természetes vagy jogi személyek kötelesek **hozzáférhetővé tenni** az 51. cikkben említett megfelelőségértékelő szervezet **vagy az 50. cikkben említett nemzeti kiberbiztonsági tanúsító hatóság** [...] **számára <u>– amennyiben a tanúsítványt e hatóság állította ki –</u>** a tanúsítási eljárás lefolytatásához szükséges összes információt.

(5a) A tanúsítvány jogosultjának tájékoztatnia kell a tanúsítványt kiállító szervezetet minden olyan, a tanúsított ikt-folyamat, -termék, illetve -szolgáltatás biztonságát érintő, utólag észlelt sebezhetőségről vagy rendellenességről, amely hatással lehet a tanúsítással összefüggő követelmények teljesülésére. Ez a szervezet a szóban forgó információt köteles indokolatlan késedelem nélkül továbbítani a nemzeti kiberbiztonsági tanúsító hatóságnak.

(6) A tanúsítványokat [...] **az adott tanúsítási rendszerben meghatározott időtartamra** kell kiállítani, és [...] megújíthatók, feltéve hogy a vonatkozó 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 rendszerek hatálya alá tartozó ikt-**folyamatokra**, -termékekre és -szolgáltatásokra vonatkozó idevágó eljárások a 44. cikk (4) bekezdése alapján elfogadott végrehajtási jogi aktusban meghatározott időponttól kezdve nem keletkeztetnek joghatást. A nemzeti kiberbiztonsági tanúsítási rendszerek, valamint az európai kiberbiztonsági tanúsítási rendszerek hatálya alá nem tartozó ikt-**folyamatokra,** -termékekre és -szolgáltatásokra vonatkozó idevágó eljárások azonban továbbra is fennmaradnak.

(2) A tagállamok a valamely hatályos európai kiberbiztonsági tanúsítási rendszer hatálya alá tartozó ikt-**folyamatokra**, -termékekre és -szolgáltatásokra vonatkozóan nem vezethetnek be új nemzeti kiberbiztonsági tanúsítási rendszereket.

(3) A nemzeti kiberbiztonsági tanúsítási rendszerek alapján kiadott, **valamely európai kiberbiztonsági tanúsítási rendszer hatálya alá tartozó** meglévő tanúsítványok lejáratuk napjáig érvényben maradnak.

50. cikk

Nemzeti* kiberbiztonsági *tanúsító [...] hatóságok

(1) Minden tagállam **a saját területén** [...] **kijelöl egy vagy több** nemzeti **kiberbiztonsági** tanúsító [...] **hatóságot**, **vagy amennyiben erről egy másik tagállammal kölcsönös megállapodás születik, egy vagy több ezen másik tagállambeli hatóságot jelöl ki a kijelölő tagállam felügyeleti feladatainak ellátásáért felelős hatóságként.**

(2) Minden tagállam közli a Bizottsággal, hogy mely **hatóságokat jelölte ki [...], és milyen feladatokkal bízta meg őket.**

(3) **A 48. cikk (4) bekezdése a) pontjának, valamint a 48. cikk (4a) bekezdésének sérelme nélkül,** minden nemzeti [...] **kiberbiztonsági** tanúsító hatóságnak – szerkezetét, a finanszírozási határozatokat, jogi felépítését és a döntéshozatalt illetően – függetlennek kell lennie az általa felügyelt szervezetektől.

(3a) A tagállamok gondoskodnak arról, hogy a nemzeti kiberbiztonsági tanúsító hatóság azon tevékenységei, amelyek a tanúsítványoknak a 48. cikk (4) bekezdésének a) pontja, valamint a 48. cikk (4a) bekezdése szerinti kiállításával kapcsolatosak, szigorúan el legyenek választva az e cikk szerinti szerepektől és feladatoktól, és e kétféle tevékenység ellátása egymástól függetlenül történjen.

(4) A tagállamok biztosítják, hogy a nemzeti **kiberbiztonsági** tanúsító [...] hatóságok rendelkezzenek a hatáskörük gyakorlásához, valamint a rájuk bízott feladatok hatékony és eredményes elvégzéséhez szükséges forrásokkal.

(5) A rendelet hatékony végrehajtása érdekében célszerű, hogy ezek a hatóságok – aktív, hatékony, eredményes és biztonságos módon – részt vegyenek az 53. cikk alapján létrehozott európai kiberbiztonsági tanúsítási csoportban.

(6) A nemzeti **kiberbiztonsági** tanúsító [...] hatóságok feladatai:

a) [...]

aa) nyomon követik és betartatják az ikt-termékek, illetve -szolgáltatások azon gyártóinak, illetve -nyújtóinak a 47a. cikk (2) és (3) bekezdésében, valamint az alkalmazandó európai kiberbiztonsági tanúsítási rendszerben foglalt kötelezettségeit, amely gyártók, illetve szolgáltatók székhelye a területükön található;

b) [...] **az 51. cikk (1b) bekezdésének sérelme nélkül, segítik a nemzeti akkreditáló szerveket** a megfelelőségértékelő szervezetek e rendelet alkalmazása céljából [...] ellátott tevékenységeinek **a nyomon követésében és felügyeletében;**

ba) nyomon követik és felügyelik a 48. cikk (4) bekezdésében említett szervek tevékenységeit;

bb) ellátják az 51. cikk (1b) bekezdésében említett megfelelőségértékelő szervezetek engedélyezésének feladatát, valamint az e rendeletben foglalt követelmények nem teljesítése esetén korlátozzák, felfüggesztik vagy visszavonják a kiadott engedélyeket;

c) kezelik a természetes vagy jogi személyeknek **[...] a nemzeti kiberbiztonsági tanúsító hatóság vagy – a 48. cikk (4a) bekezdésével összhangban – megfelelőségértékelő szervezetek által kiadott** tanúsítványokkal kapcsolatban benyújtott panaszait, megfelelő mértékben kivizsgálják a panasz tárgyát, és észszerű időn belül tájékoztatják a panaszost a vizsgálat előrehaladásáról és eredményéről;

d) együttműködnek a többi nemzeti **kiberbiztonsági** tanúsító [...] hatósággal és más hatóságokkal, többek között azáltal, hogy megosztják az azzal kapcsolatos információkat, ha bizonyos ikt-**folyamatok,** -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 **kiberbiztonsági** tanúsító [...] hatóság legalább a következő hatáskörökkel rendelkezik:

a) felszólíthatja a megfelelőségértékelő szervezeteket, [...] az európai kiberbiztonsági tanúsítványok jogosultjait **és az uniós megfelelőségi nyilatkozatok kibocsátóit,** hogy bocsássák rendelkezésére a feladata ellátásához szükséges információkat;

b) a III. cím rendelkezéseinek való megfelelés ellenőrzése céljából vizsgálatokat végezhet a megfelelőségértékelő szervezeteknél, [...] az európai kiberbiztonsági tanúsítványok jogosultjainál **és az uniós megfelelőségi nyilatkozatok kibocsátóinál** tett ellenőrzések formájában;

c) a nemzeti joggal összhangban meghozhatja a megfelelő intézkedéseket annak biztosítása érdekében, hogy a megfelelőségértékelő szervezetek, [...] a tanúsítványok jogosultjai **és az uniós megfelelőségi nyilatkozatok kibocsátói** 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 **a nemzeti kiberbiztonsági tanúsító hatóság vagy – a 48. cikk (4a) bekezdésével összhangban – megfelelőségértékelő szervezetek által kiadott**, 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 **kiberbiztonsági** tanúsító [...] hatóságoknak együtt kell működniük egymással és a Bizottsággal, azaz meg kell osztaniuk egymással az ikt**-folyamatok,** -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 akkreditálhatja a megfelelőségértékelő szervezeteket, ha azok megfelelnek az e rendelet mellékletében meghatározott követelményeknek.

(1a) Azokban az esetekben, ha egy európai kiberbiztonsági tanúsítványt egy nemzeti kiberbiztonsági tanúsító hatóság állít ki a 48. cikk (4) cikkének a) pontja, illetve 48. cikkének (4a) bekezdése alapján, a nemzeti kiberbiztonsági tanúsító hatóság tanúsító szervének e cikk (1) bekezdésével összhangban megfelelőségértékelő szervezetként akkreditált szervnek kell lennie.

(1b) A megfelelőségértékelő szervezeteknek adott esetben a feladataik ellátására vonatkozóan engedélyt kell kapniuk a nemzeti kiberbiztonsági tanúsító hatóságtól, amennyiben teljesítik az európai tanúsítási rendszerben a 47. cikk (1) bekezdésének ca) pontja alapján meghatározott egyedi vagy kiegészítő követelményeket.

(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 testületeknek **észszerű időkereten belül minden, e célra megfelelő intézkedést meg kell tenniük** a megfelelőségértékelő szervezet e cikk (1) bekezdése szerinti akkreditációjának a **korlátozása, felfüggesztése vagy** visszavonása érdekében, 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 **kiberbiztonsági** tanúsító [...] hatóságoknak a 44. cikk alapján elfogadott minden egyes európai kiberbiztonsági tanúsítási rendszer vonatkozásában be kell jelenteniük a Bizottságnak, hogy mely megfelelőségértékelő szervezeteket akkreditálták, **illetve – adott esetben – látták el engedéllyel az 51. cikk (1b) bekezdése alapján** a 46. cikkben említett, meghatározott megbízhatósági 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 lejárta 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 **kiberbiztonsági** tanúsító [...] 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 **kiberbiztonsági** tanúsító [...] 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 csoportnak a nemzeti **kiberbiztonsági** tanúsító [...] hatóságok **képviselőiből** vagy adott esetben **az egyéb illetékes nemzeti hatóságok képviselőiből** kell állnia. [...]**A csoport mindegyik tagja legfeljebb egy másik tagállamot képviselhet.**

(3) A csoportnak a következő feladatokat kell ellátnia:

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 javasolt tanúsítási rendszerek e rendelet 44. cikkének megfelelően történő kidolgozásával kapcsolatban;

ba) e rendelet 44. cikkével összhangban véleményt fogad el a javasolt tanúsítási rendszerekről;

c) [...] **felkéri** az Ügynökséget, hogy e rendelet 44. cikkének megfelelően javaslati szinten dolgozzon ki európai kiberbiztonsági tanúsítási rendszert;

ca) iránymutatásokat dolgoz ki és fogad el a csoporthoz a 44. cikk (1a) bekezdésével összhangban benyújtott, kidolgozásra javasolt tanúsítási rendszerek értékelésének a kritériumaira vonatkozóan;

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) **kapacitásépítés és** információcsere útján előmozdítja a nemzeti **kiberbiztonsági** tanúsító [...] hatóságok közötti, e cím rendelkezései szerinti együttműködést, különösen a kiberbiztonsági tanúsítással kapcsolatos valamennyi kérdésre vonatkozó hatékony információcserére szolgáló módszerek kialakítása révén**;**

fa) támogatást biztosít az e rendelet 47. cikke (1) bekezdésének md) pontja alapján valamely európai kiberbiztonsági tanúsítási rendszer erre vonatkozó szabályai szerint végezhető kölcsönös felülvizsgálati mechanizmus végrehajtásához.

(4) A csoportban a Bizottság látja el az elnökséget **közvetítői minőségben,** és a 8. cikk a) pontjának megfelelően az ENISA segítségével biztosítja a titkárságot.

53a. cikk

A nemzeti* kiberbiztonsági *tanúsító [...] hatóságnál való panasztétel joga

(1) Természetes vagy jogi személyeknek jogában áll panasszal élni a nemzeti kiberbiztonsági tanúsító hatóságnál az ugyanazon hatóság vagy a 48. cikk (4a) bekezdése alapján valamely megfelelőségértékelő szervezet által kibocsátott tanúsítvánnyal kapcsolatban.

(2) Az a nemzeti kiberbiztonsági tanúsító hatóság, amelyhez a panaszt benyújtották, köteles tájékoztatni a panaszost a panasszal kapcsolatos eljárási fejleményekről és annak eredményéről, ideértve azt is, hogy az 53b. cikk szerint a panaszosnak jogában áll bírósági jogorvoslattal élni.

53b. cikk

A hatékony bírósági jogorvoslathoz való jog

(1) A természetes, illetve jogi személyeknek a nemzeti kiberbiztonsági tanúsító hatóság őket érintő, kötelező jogi erővel bíró határozatával szemben jogában áll hatékony bírósági jogorvoslattal élni.

(2) A természetes, illetve jogi személyeknek jogában áll hatékony bírósági jogorvoslattal élni, amennyiben a nemzeti kiberbiztonsági tanúsító hatóság nem jár el panaszuk ügyében.

(3) A nemzeti kiberbiztonsági tanúsító hatósággal szemben annak a tagállamnak a bírósága előtt lehet eljárást kezdeményezni, amelyben az adott hatóság székhelye található.

54. cikk

Szankciók

A tagállamok megállapítják az e címben 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 hatékonynak, arányosnak 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 eljárás

(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 **5. cikke (4) bekezdésének b) pontját** 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

Hatálybalépés

(1) Ez a rendelet az Európai Unió Hivatalos Lapjában való kihirdetését követő huszadik napon lép hatályba.

(1a) Ezt a rendeletet […]-tól/-től kell alkalmazni, az 50., az 51., az 52., az 53a., az 53b. és az 54. cikk kivételével, amelyek [24 months after the date of its publication in the Official Journal of the European Union]-tól/-től alkalmazandók.

(2) Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben,

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*

A MEGFELELŐSÉGÉRTÉKELŐ SZERVEZETEK ÁLTAL TELJESÍTENDŐ KÖVETELMÉNYEK

Az akkreditációt igénylő megfelelőségértékelő szervezeteknek meg kell felelniük az alábbi követelményeknek:

1. A megfelelőségértékelő szervezetet nemzeti jogszabályok szerint kell létrehozni, és annak jogi személyiséggel kell rendelkeznie.

2. A megfelelőségértékelő szervezetnek az általa értékelt szervezettől, illetve ikt-termékektől vagy -szolgáltatásoktól független harmadik félnek kell lennie.

3. Megfelelőségértékelő szervezetnek tekinthető az a szervezet is, amely az általa értékelt ikt-termékek vagy -szolgáltatások tervezésében, gyártásában, szállításában, összeszerelésében, használatában vagy karbantartásában részt vevő vállalkozásokat képviselő vállalkozói szövetséghez vagy szakmai egyesüléshez tartozik, feltéve hogy bizonyítottan független és összeférhetetlenségektől mentes.

4. A megfelelőségértékelő szervezet, valamint annak felső vezetése és a megfelelőségértékelési feladatok elvégzéséért felelős személyzet nem lehet tervezője, gyártója, szállítója, üzembe helyezője, vásárlója, tulajdonosa, felhasználója és karbantartója az értékelés tárgyát képező ikt-terméknek vagy -szolgáltatásnak, valamint nem lehet a felsorolt felek meghatalmazott képviselője sem. Ez nem zárja ki a megfelelőségértékelő szervezet működéséhez szükséges, értékelt termékek használatát, sem az értékelt termékek személyes célra történő használatát.

5. A megfelelőségértékelő szervezet, valamint annak felső vezetése és a megfelelőségértékelési feladatok elvégzéséért felelős személyzet nem vehet részt közvetlenül a szóban forgó ikt-termékek vagy -szolgáltatások tervezésében, gyártásában és kivitelezésében, értékesítésében, üzembe helyezésében, használatában és karbantartásában, továbbá nem képviselhet ilyen tevékenységben részt vevő feleket. Nem vehet részt továbbá olyan tevékenységben sem, amely veszélyeztetné döntéshozói függetlenségét vagy feddhetetlenségét azon megfelelőségértékelési tevékenységek tekintetében, amelyek elvégzésére bejelentették. Ez a szaktanácsadási szolgáltatásokra különösen érvényes.

6. A megfelelőségértékelő szervezetnek gondoskodnia kell arról, hogy leányvállalatainak és alvállalkozóinak tevékenysége ne befolyásolja megfelelőségértékelési tevékenységei bizalmas jellegét, objektivitását és pártatlanságát.

7. A megfelelőségértékelő szervezetnek és személyzetének a legmagasabb szintű szakmai feddhetetlenséggel és az adott szakterületen elvárható műszaki felkészültséggel kell megfelelőségértékelési tevékenységét végezni, és függetlennek kell lennie minden olyan – többek között pénzügyi – nyomásgyakorlástól és ösztönzéstől, amely befolyásolhatná ítélőképességét vagy megfelelőségértékelési tevékenysége eredményeit; különösen érvényes ez a tevékenysége eredményeiben érdekelt személyek vagy azok csoportjának viszonylatában.

8. A megfelelőségértékelő szervezetnek képesnek kell lennie az e rendelet alapján rá ruházott valamennyi megfelelőségértékelési feladat elvégzésére, függetlenül attól, hogy ezeket a feladatokat a megfelelőségértékelő szervezet maga, vagy az ő nevében és felelősségi körében valaki más végzi el.

9. A megfelelőségértékelő szervezetnek minden megfelelőségértékelési eljárás és az ikt-termékek és -szolgáltatások minden fajtája, kategóriája és alkategóriája tekintetében mindenkor rendelkeznie kell a következőkkel:

a) olyan személyzet, amely műszaki ismeretekkel, valamint elegendő és megfelelő tapasztalattal rendelkezik a megfelelőségértékelési feladatok elvégzéséhez;

b) azon eljárások leírása, amelyek szerint a megfelelőségértékelést végzik, és amelyek biztosítják ezen eljárások átláthatóságát és megismételhetőségét. Rendelkeznie kell megfelelő szabályokkal és eljárásokkal, amelyek segítségével a bejelentett szervezetként végzett feladatai és az egyéb tevékenységei elkülönülnek egymástól;

c) olyan eljárások, amelyek segítségével tevékenysége során képes megfelelően figyelembe venni az adott vállalkozás méretét, az ágazatot, amelyben a vállalkozás a tevékenységét folytatja, a vállalkozás szerkezetét, az érintett ikt-termék vagy -szolgáltatás technológiai összetettségének fokát, valamint azt, hogy tömeg- vagy sorozatgyártásról van-e szó.

10. A megfelelőségértékelő szervezetnek rendelkeznie kell a megfelelőségértékelési tevékenységekhez kapcsolódó műszaki és adminisztrációs feladatok megfelelő ellátásához szükséges eszközökkel, és hozzá kell férnie minden szükséges felszereléshez, illetve létesítményhez.

11. A megfelelőségértékelési tevékenységek elvégzéséért felelős személyzetnek rendelkeznie kell a következőkkel:

a) valamennyi megfelelőségértékelési tevékenységre kiterjedő, alapos műszaki és szakképzettség;

b) az általa végzett értékelésekre vonatkozó követelmények kellő ismerete és megfelelő hatáskör a szóban forgó értékelések elvégzésére;

c) a vonatkozó követelmények és vizsgálati előírások megfelelő szintű ismerete és megértése;

d) az értékelések elvégzését igazoló tanúsítványok, nyilvántartások és jelentések elkészítésének képessége.

12. Biztosítani kell a megfelelőségértékelő szervezet, annak felső vezetése és az értékelést végző személyzet pártatlanságát.

13. A megfelelőségértékelő szervezet felső vezetésének és az értékelést végző személyzetének javadalmazása nem függhet az elvégzett értékelések számától és az értékelések eredményétől.

14. A megfelelőségértékelő szervezeteknek felelősségbiztosítást kell kötniük, kivéve, ha a felelősséget a nemzeti joggal összhangban az állam vállalja át, vagy ha a tagállam közvetlenül felel a megfelelőségértékelésért.

15. A megfelelőségértékelő szervezet személyzetének minden olyan információ tekintetében, amely e rendelet vagy az e rendeletből fakadó joghatások érvényesülését biztosító nemzeti jogszabályok rendelkezései alapján ellátott feladatainak végrehajtása során jutott birtokába, be kell tartania a szakmai titoktartás követelményeit, kivéve azon tagállamok illetékes hatóságainak viszonylatában, ahol a szervezet a tevékenységét gyakorolja.

16. A megfelelőségértékelő szervezeteknek teljesíteniük kell **a vonatkozó, a folyamatok, termékek vagy szolgáltatások tanúsításáért felelős megfelelőségértékelő szervezetek akkreditálása tekintetében a 765/2008/EK rendelettel harmonizált** szabványban foglalt követelményeket [...].

17. A megfelelőségértékelő szervezetnek gondoskodnia kell arról, hogy a megfelelőségértékelések céljára használt vizsgálati laboratóriumok megfeleljenek **a vizsgálatokat végző laboratóriumok akkreditálása tekintetében a 765/2008/EK rendelettel harmonizált, vonatkozó** szabványban foglalt követelményeknek [...].